SIL Determination Techniques Report

White Paper provided courtesty of:

A Division of ACM Automation Inc

Copyright - Intellectual Property

Disclaimer and Limited Liability

What is a "White Paper"?

A white paper is a document that high lights a problem or situation common to a constituency (the process industry) and offers the reader an approach as to how to arrive at a solution. The term white paper is an offshoot of the phrase "white book", which is often used in government circles.

ACM provides this white paper without cost. It is for informational purposes only.

How to Contact ACM

Murray J. Macza MBA
VP – Sales & Marketing
ACM Automation Inc.
#825, 906 – 12th Avenue SW
Calgary, Alberta, Canada
T2R 1K7
Ph: 403 264 9637 Cell: 403 862 6914
Email: murray.macza@acm.ab.ca
Web: http://www.acm.ab.ca

Table of Contents

Appendix

1.0 SIL DETERMINATION & THE SAFETY LIFE CYCLE

SIL Determination

While the Hazard and Operability (HAZOP) study identifies and risk ranks hazards, Safety Integrity Level (SIL) Determination focuses on the adequacy of safeguards to mitigate hazards. Furthermore, SIL adds another dimension to safety analysis. Within the framework of a HAZOP, analysts are restricted to the limits of the governing risk matrix (i.e. specific range limits on frequencies of occurrence). In contrast, SIL analysis enables analysts to refine the estimates of frequencies of occurrence to obtain more realistic estimates of risk.

SIL Determination is the process of determining the amount of risk mitigation required to reduce the risk put forth by a process to a tolerable level. SIL Determination is the first step in the development, design, commission and operation of a Safety Instrumented System (SIS).

SIL Determination involves the determination of the safety integrity level (SIL) for each Safety Instrumented Function (SIF) in a Safety Instrumented System and is dependent on the following factors:

- Corporate standards for the tolerable risk after applying all the layers of protection
- The overall risk from the unprotected hazards that can occur
- The risk reduction provided by all of the non-SIS protection layers

The SIL Determination exercise occurs during Phases 1 and 2 of the SIS Safety Life Cycle. See Appendix A for a graphical depiction, as taken from IEC 61511 Functional safety - Safety instrumented systems for the process industry sector. SIL Determination can also determine if a SIS, or specific SIFs, are really necessary. If a SIF is not needed, there is no benefit in installing it. In fact, there would be an economic penalty in both capital and maintenance costs if it were installed.

The ideal time for SIL Determination to be done is during the front-end engineering design (FEED) and project definition stages and, typically, as a supplement to the HAZOP. An effective risk reduction and protection layer design draws on the same information and personnel involved in the initial hazard study (HAZOP). Nevertheless, SIL Determination may also be used effectively during the plant's life to determine if improvements are needed and to provide guidance as to the form of the improvements.

The initial protection layer design may need to be reviewed and changed soon after the HAZOP has been completed. If the protection layer design and SIL Determination is delayed for some considerable time after the HAZOP, there is the risk that the SIS will have the feel of a "bolted on" solution and the capability of being able to integrate SIS and non-SIS protection layers may be compromised.

Careful planning and management is needed in the lifecycle of a SIS. However, while the SIS Safety Life Cycle model provides guidance on the steps necessary for a successful SIS project, the actual step-by-step directions to perform all the steps are not explicitly contained in the IEC 61511 standard.

The determination of SIL is driven by company decision criteria such as Tolerable Frequencies, ALARP and corporate risk tolerance philosophy. Standards such as IEC 61511 and OSHA's Process Safety Management legislation require the process industry to use good engineering practice in the design and operation of their facilities. This means that the determination of safety integrity levels must be competently performed and properly documented.

SIL Concept Validation

SIL Concept Validation can be performed immediately following SIL Determination. It starts with situations where unmitigated risk exists and involves the design of one or more "conceptual solutions" that would mitigate the residual risk. Various types of Independent Protection Layers (IPLs) can be proposed to do this.

Most often, all the non-instrumented IPLs have already been applied. See Appendix B for an overview of IPLs. Once an instrumented solution is created using various types of components (i.e. logic solvers, final elements, sensors) in the SIF, such a conceptual design that mitigates risk to a tolerable level is referred to as a Concept Validation solution. It shows that the specified safeguards will indeed mitigate all risk according to corporate risk targets.

It is also called "Concept Validation" because when the actual plant is built, the components (i.e. logic solvers, final elements, sensors) incorporated into the SIF need to be validated so the user confirms that the plant is properly protected. In this "Final Validation" process, the actual variables for the exact components, including the maintenance testing frequencies, are used to validate the SIF.

Safety Requirement Specification

The Safety Requirements Specification (SRS) develops specifications for safety functions, including a Safety Instrumented System (SIS) design, and includes tags, functionality, performance and physical requirements. It is developed following SIL Determination and SIL Concept Validation to ensure that the critical control and safety system is designed to meet the necessary technical requirements to prevent or minimize injury to personnel, damage to equipment (asset loss) and loss of production. The SRS defines the functional and integrity requirements of the critical control system and serves as the basis to begin detailed engineering and programming of the SIS hardware and software.

The SRS is developed during the execution of a project involving a SIS and provides a key measure by which the SIS design is compared to and judged throughout its life cycle. So, while the SRS serves as the basis for the SIS design, it is more than a "specification" for the SIS design. It acts as a living document for the life of the facility.

Typically, Functional Specification sheets are developed for each safety function. These data sheets are then combined into an overall Safety Requirements Specification for the SIS. Also included are non-SIF functions that maybe found in the SIS (i.e. eyewash stations).

SilCore™ Software

SilCore™ is a field proven, IEC compliant SIL Life Cycle tool that gives high integrity and critical control systems designers, engineers, operators and maintainers the information and power to conduct SIL Determination, SIL Validation and SIL Optimization exercises. It is used in the execution of the all ACM SIL studies.

1. Download a free trial copy at: http://acm.ab.ca/sd/
2. Experience a personalized web cast by calling 403 264 9637
3. View our online SilCore™ tutorials at http://acm.ab.ca

2.0 SIL DETERMINATION TECHNIQUES

The IEC 61511 standard refers to six SIL Determination techniques specified in Annex A – F:

- ALARP and Tolerable Risk Concepts (Annex A)
- Semi-Quantitative Method – Event Tree Analysis (Annex B)
- Safety Layer Matrix Method (Annex C)
- Calibrated Risk Graph (Annex D)
- Risk Graph (Annex E)
- Layer of Protection Analysis or LOPA (Annex F)

Companies potentially can apply four of the six IEC 61511 listed SIL Determination techniques. The ALARP (As Low As Reasonably Practicable) principle sets the stage for doing SIL Determination and is not used to actually determine SIL levels. Risk Graph (Annex E) is not considered a reasonable technique due to its generic nature and the predominant use of the Calibrated Risk Graph in the process industry.

A seventh potential technique, which might be called the Corporately Mandated SIL, is not seriously considered either. This is the least time consuming approach and is essentially based on the premise that "a safety system is a safety system and therefore should be SIL 3". Such a broad-brush approach minimizes the time and effort of SIL analysis, but is inherently imprecise in economically mitigating risk. Substantial over-instrumentation, with the resulting significantly increased SIS life cycle costs, would be the result of such an approach.

All SIL Determination methods require a thorough analysis be completed to identify the hazards of concern. For the process industry, the preferred analysis method is the hazards and operability (HAZOP) study. The HAZOP can be done either prior to the SIL Determination or as part of the SIL Determination. If the HAZOP is done separately from the SIL Determination, specific information is required including the frequency of initiating events and the risk ranking of the consequence without safeguards.

SIL Determination techniques are similar in the following ways:

- focus on a specific hazardous event
- identify initiating causes and frequencies
- identify protective measures
- assess the level of risk and the contribution to risk reduction required (if any) from a SIF to meet the required risk target(s)
- evaluate whether the risk is reduced to ALARP

The following five SIL Determination techniques are listed in Part 3, IEC Standard 61511, first edition 2003.

2.1 ALARP and Tolerable Risk Concept

The ALARP (As Low As Reasonably Practicable) principle sets the stage for doing a SIL Determination and is not used to actually determine SIL levels. The ALARP principle helps to define the tolerable risk target for a facility in terms of the social, political and economic factors and predefined consequences relevant to the company. This principle is also used by many companies to define the tolerable risk target for safety, environmental impact and asset/production loss.

ALARP is a fundamental requirement for the management of industrial risks. The risk interpretation from ALARP is developed into several other forms. These include Risk Matrix (for HAZOP) as well as SIL Risk Matrix (Safety Layer Matrix), Calibrated Risk Graph and Layer of Protection Analysis (LOPA) definitions for SIL Determination.

2.2 Semi-Quantitative Method – Fault Tree and Event Tree Analysis

Fault trees and event trees are quantitative methods used to determine the frequencies of hazardous events. These frequencies may then be compared to a pre-defined Tolerable Frequency (TF). Any inadequacy is expressed in terms of SIL and this value is normally assigned to the development of a new safeguard. The event tree displays the demand rate of all the initiating events resulting in the same consequence. Calling fault tree and event tree methods "semi-quantitative" could be perceived as a misnomer. Both methods are quantitative and the combination of the two is a powerful and rigorous method for determining SIL. Fault tree and event tree analysis often requires the use of specialized, quantitative risk assessment software.

Advantages

- Objective
- Graphically easy to understand
- Very powerful
- Mathematically rigorous

Disadvantages

- Requires skill in probabilistic methods to apply properly

2.3 Safety Layer Matrix

The Safety Layer Matrix method identifies the risk reduction or SIL required. It is often referred to as the "SIL risk matrix" approach. The user selects on the Matrix: the frequency of the initiating event; the consequence without safeguards; and the safeguards. The safeguards are evaluated using Independent Protection Layer (IPL) rules defined by the company.

The Safety Layer Matrix is applied to the most frequent initiating event resulting in the same consequence. This results in a qualitative analysis on which initiating event has the highest frequency of occurrence. It is occasionally used in the process industry and can be used for integrated HAZOP/SIL Determination sessions.

This method can also be used as a screening method to identify the high end Safeguards (SIL 2 & 3), which can be further evaluated in separate risk evaluation sessions. This screening process suggested

helps identify the high-end safeguards quickly, but the user still needs to perform the validation. Note that to complete the due diligence required by the standards, all instrument loops with SIL ratings need mathematical validation.

Advantages

- Non numerical
- HAZOP/ SIL matrix at same session
- Easy to understand

Disadvantages

- Somewhat simplistic approach
- High effort on Management of Change
- Not integrated to SIL Life Cycle (if used alone)
- Less discriminating
- Credit for multiple low end safeguards not achieved

2.4 Calibrated Risk Graph

The Calibrated Risk Graph is set by the company to meet the intent of ALARP and the related tolerable frequencies. Calibration of the risk graph is the process of assigning numerical values to the risk graph variables. This forms the basis of assessment of the risk and determination of the required integrity of the SIF under consideration.

The Calibrated Risk Graph is applied to the most frequent initiating event resulting in the same consequence. This may result in some qualitative analysis to determine which initiating event has the highest frequency of occurrence for a specific consequence. The Calibrated Risk Graph approach normally involves three graphs - Safety, Environmental Impact, and Asset/Production Loss.

This SIL Determination method often requires more time than others because of the multiple evaluations of consequence categories.

Advantages

- Non numerical approach
- Easy to apply
- Commonly used when SIL first applied

Disadvantages

- Qualitative, does not yield well-defined numerical estimates of risk
- Time consuming on ranking the risk
- Credits for low end safeguards not achieved
- Subjective when evaluating the initiating events and which frequency to use

2.5 Layer of Protection Analysis (LOPA)

The LOPA technique is more quantitative and results in more defensible conclusions. The LOPA process requires more precise information on the initiating event frequencies, the probabilities of failures of all safeguards, and more mathematical evaluation. The process requires more user defined risk criteria and statistical data but produces more objective results.

LOPA is applied to a set of individual initiating events resulting in the same consequence. This is more

rigorous than other techniques, except fault tree/event tree, which normally take the worst-case scenario and use the most frequent initiating event. LOPA results in a quantitative analysis on the set of initiating events.

The LOPA process also evaluates an initiating event against the safeguards which can mitigate that event or reduce the post-hazardous event frequency. This is done by determining the probability of failure on demand (PFD) for each safeguard. The PFD ranges may be modeled directly into the LOPA evaluation from SIL validations of the safeguards. Where the validated value of the PFD is already known, this allows for objective results and allows the user to determine which safeguards are most economical to apply. The user can quickly assess a scenario that is demanding SIL 2 or SIL 3 solutions and determine potential SIS and non-SIS options.

The LOPA approach typically involves establishing unique tolerable frequencies for Safety, Environmental Impact and Asset/Production Loss. In cases where Asset/Production Loss, not Safety, is the primary driver for the consequences under consideration, the user has the option to select a tolerable frequency more closely associated with Asset/Production Loss rather than relying on a tolerable frequency based on Safety (injury or fatality).

LOPA gives the users a much clearer picture than Calibrated Risk Graph and Safety Layer Matrix, but less so than Fault Tree/Event Tree, of which safeguards contribute to what level of risk reduction.

Advantages

- Numerical approach
- Considers all low end safeguards for credit to achieve maximum risk reduction
- Clear picture of safeguards and initiating events
- Results more rigorous than risk matrix or risk graph but less rigorous than fault tree/event tree.

Disadvantages

- Requires numerous calibrated tools to assess safeguards, and initiating events
- Can involve more effort and time in SIL Determination stage
- More items for Management of Change

3.0 EVALUATING THE SIL DETERMINATION OPTIONS

In general, all SIL Determination techniques identified in IEC 61511 accomplish the same objective in similar ways. To compare and contrast the SIL Determination options, the following parameters are suggested:

- Rigour and Effort
- Fit with SIL Life Cycle
- Inputs Required

3.1 Comparison Based on Rigor and Effort

The rigor of the study refers to the completeness of safeguards evaluation. The IEC standards state all SIL rated safeguards that are instrument based need mathematical validation to confirm that the SIL rating of the safeguard can be met given the reliability and architecture of elements making up the safeguard. The IEC standards also say that the other non-instrument safeguards need to be evaluated and maintained to ensure the SIL rating of the instrument safeguard does not change. This is part of the complexity of evaluating the SIL remaining or the Target SIL. The number of safeguards where this rigor is applied also affects the time and effort to complete the validation step. The rigor of the study is also a measure of how quantitative the process is. Some techniques use specific values for initiating events, consequences, probability of failures, and consider specific values for human error and common cause. Others do not.

The effort required to complete the SIL Determination is influenced by such factors as whether the SIL Determination was separate from the HAZOP or was completed at the same session as the HAZOP and the effort involved in establishing and/or confirming specific values like initiating events, consequences, probability of failures, human error and common cause.

3.2 Comparison Based on Fit with SIL Life Cycle

A major oversight when selecting SIL Determination techniques is not considering the remaining steps in the SIL Life Cycle. Understanding the remaining effort involved can highlight shortcomings of the SIL Determination technique. SIL Determination techniques are not equal. Some get the SIS designer further "down the path" than others.

As well, the software tools used to document and perform SIL Determination and SIL Validation have a significant impact. Some create more work, making change management difficult if not almost impossible.

3.3 Comparison Based on Inputs Required

Depending on the type of SIL Determination to be done, the following company supplied inputs may need to be supplied:

- IPL table and rules
- Initiating event frequencies
- Risk matrix & tolerable frequencies
- Method for human error rate determination
- Risk graphs
- Method for determining the probability of failure on demand (PFD) for layers of protection
- Fault Tree/Event Tree practices

Except for fault trees and event trees, these inputs or "tools" need to be calibrated. Calibrating these tools will ensure consistent approaches within a corporation to SIL Determination.

For example, calibration of the risk graph is the process of assigning numerical values to risk graph parameters. When considering the calibration of risk graphs, it is important to consider requirements relating to risk arising from both corporate expectations and regulatory authorities.

It is critical that the chosen risk interpretation method and calibrated risk tool is agreed to at the senior level within the company. Calibration decisions made pertaining to Safety, Environmental Impact and Asset/Production Loss drive the overall safety and economic performance of the company. It is important to note that risk tools can be calibrated more specifically to a type of facility should the company wish to do so.

4.0 PROCESS INDUSTRY OBSERVATIONS

In our 12 years in the "SIL business", ACM has seen a wide variety of approaches taken by the Canadian and International process industry. Generally speaking, here are some of the trends we have noticed pertaining to SIL Determination:

- Early enthusiasm for the Calibrated Risk Graph method has ebbed somewhat and the more rigorous Layer of Protection Analysis method is becoming more popular.

- The popularity of LOPA is due to a variety of factors, including the adoption of SIL software tools, like SilCore™, that simplify the mathematical calculations, and the growing need for Operating Companies to use a defensible numerical approach that serves to satisfy both internal (senior management) and external (regulators, investment bankers) stakeholders.

- Many Operating Companies still do not have formalized SIL Standards and Practices as part of their Risk Assessment or Loss Management guidelines. Consequently, companies are "flying blind" to some degree and often either over or under protecting their assets, people and the environment.

- Many engineering contractors, who assist Operating Companies in new plant design and/or expansion of existing plants do not have formalized SIL Standards and Practices.

- Insufficient attention has been placed on the eventual operation and maintenance of SIL rated systems. Engineering is only the beginning of the SIL Life Cycle.

- Improper calibration of corporate Tolerable Frequency tables and the confusion about the suitability of failure rate data can undermine the enthusiasm of participants in the SIL Determination and SIL Validation process.

- Insufficient understanding of the probabilistic methods underlying SIL lead to doubts about the efficacy of the results.

- A significant proportion of high SIL values for SIFs are driven by economic loss, not safety.

5.0 SIL PROGRAM BENEFITS

A well designed and executed SIL Program will:

1. Potentially reduce the number of SIF loops in a safety instrumented system.

   ACM's experience has shown that SIF loops that were expected to be required during the initial design process can be eliminated, because sufficient protection layers already existed and were shown to exist by the SIL Determination.

2. Standardize an approach to all projects, so Engineering, Operations & Maintenance will be on the same page.

3. Provides a basis for due diligence.

   All possible efforts have been taken to confirm that the plant systems are capable of providing the appropriate level of protection against known hazards to people, loss of production and the environment.

4. Determine if a dedicated SIS is necessary.

5. Provide a choice of safeguarding methods.

   Designers have a variety of risk reduction methods to choose from and can do a cost-benefit calculation to support their choices.

6. Evaluate maintenance, testing and operation of safeguarding systems decisions at the design stage.
   Since minimum testing is considered, over testing non-related SIL equipment is avoided.

7. Enable clients to develop the capacity to generate their own specific failure rate data, so they can fine tune testing and maintenance activities.

Appendix A – SIS Safety Life Cycle from IEC 61511

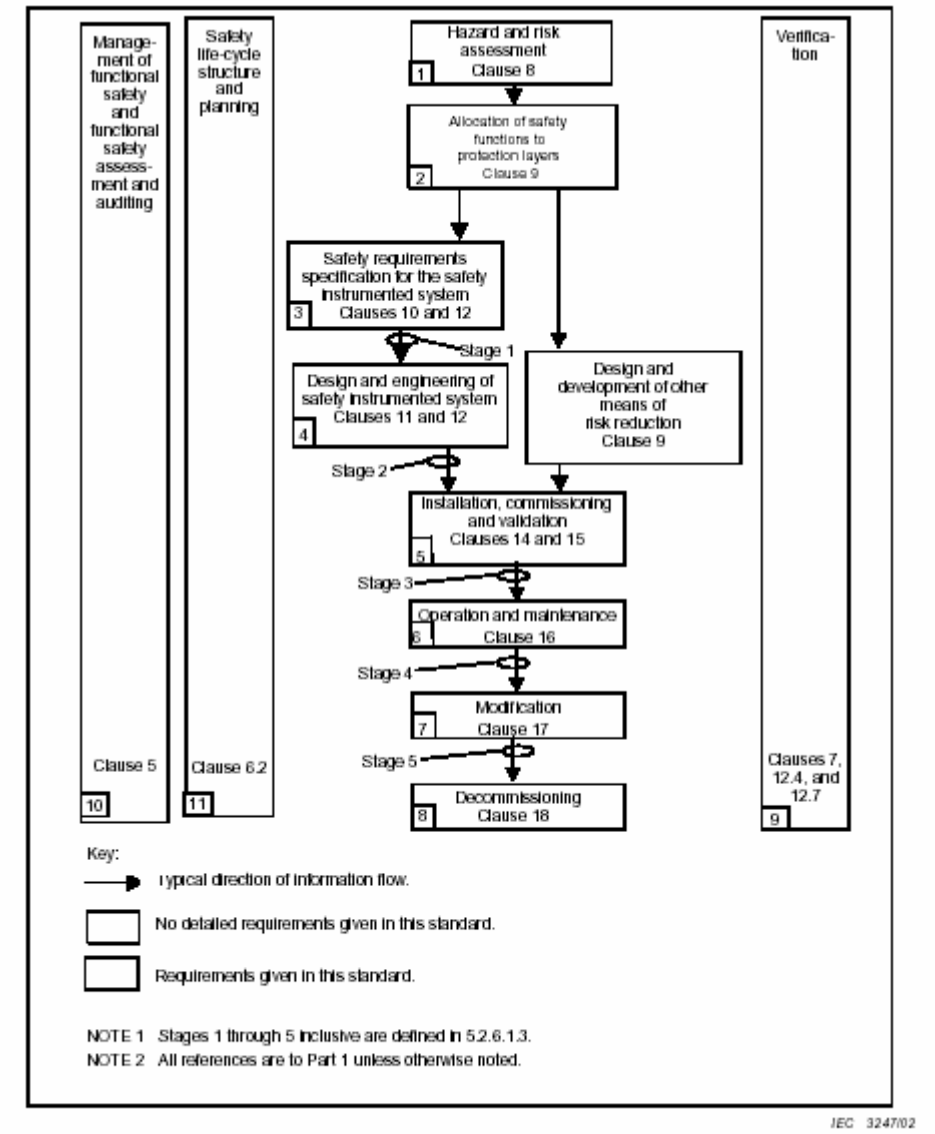

Figure 8 – SIS safety life-cycle phases and functional safety assessment stages

The Safety Life Cycle is defined in IEC 61511 as:

"necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use."

Appendix B - Overview of Independent Protection Layers (IPL)

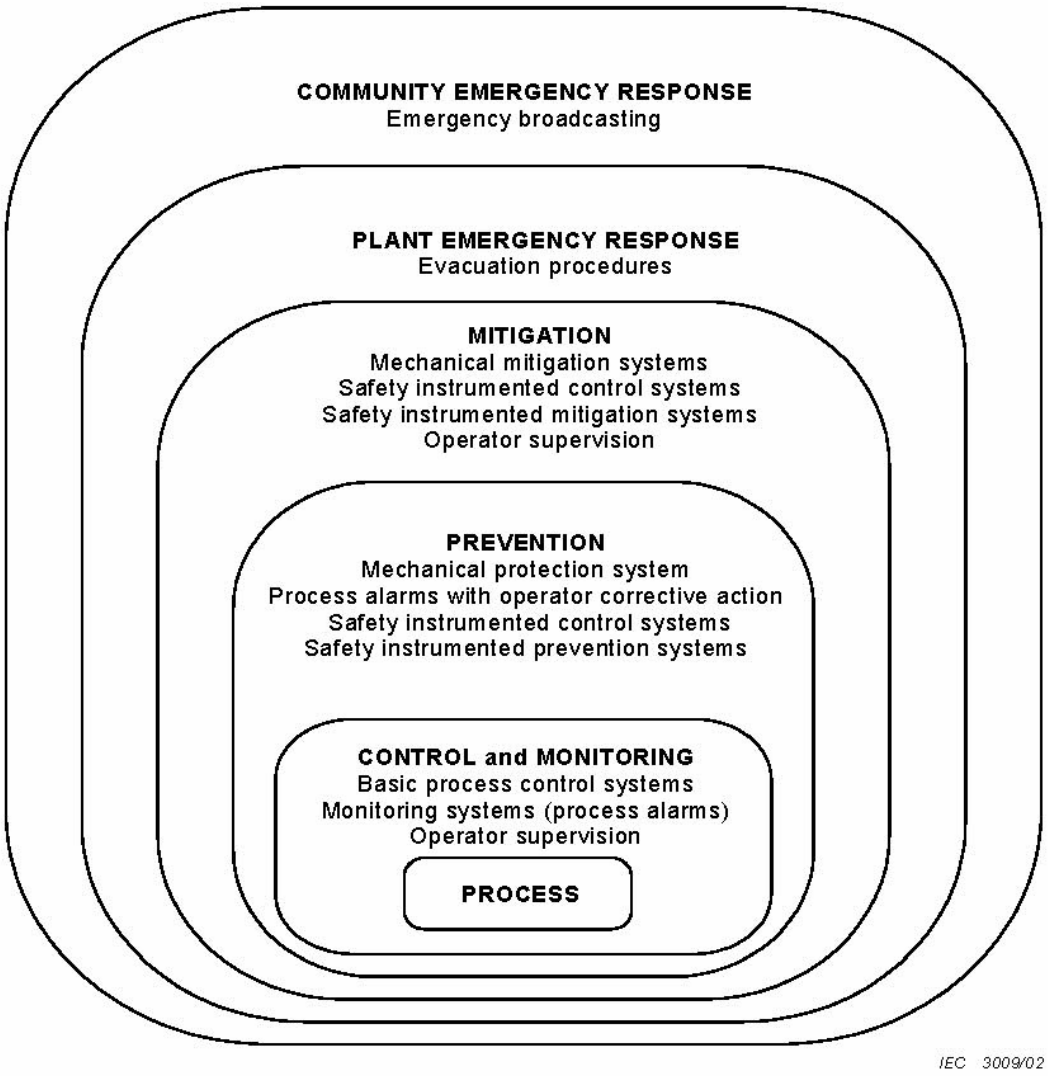

Figure 2 – Typical risk reduction methods found in process plants (for example, protection layer model)