A framework for optimizing cross-company prevention in case of adding equipment to a chemical cluster.

Authors: G. Reniers[1], W. Dullaert[2], K. Soudan[1]
[1]University of Antwerp, Prinsstraat 13, 2000 Antwerp; tel: +32 (0)3 220 41 82;
fax: +32 (0)3 220 49 01; e-mail address: genserik.reniers@ua.ac.be
[2]Institute of Transport and Maritime Management Antwerp (ITMMA), Keizerstraat 64,
2000 Antwerp

Abstract

Adding new equipment (e.g. an installation) to an existing network of chemical installations alters the existing danger equilibrium of the chemical surrounding complex. Therefore, precaution measures for preventing external domino effects have to be updated. The Hazwim framework, based on the Process Hazards Analysis (PHA) techniques of Hazop, What-if analysis and the Risk Matrix has been developed to prevent knock-on effects for an existing cluster of chemical plants. However, preventive safety measures for new installations based on PHA implementation in the design phase are preferred to the use of protection- and mitigation measures derived from non-design PHAs. The risk analysis techniques suggested by the authors allowing for the design of inherently safe installations are then evaluated based on Belgian government recommendations and Belgian Seveso plant practices. Next, based on the proposed techniques this paper presents a framework called 'Installation Plus' for redesigning external domino accident prevention when adding an installation to an existing chemical facility. Installation Plus integrates enhanced cross-company cooperation on process hazards and risk assessment activities with the selection of Safety Instrumented Functions offering the appropriate integrity requirements.

1. Introduction

The best way to achieve safe plant operation is to have inherently safe processes, and to operate in correctly designed, controlled and maintained installations equipment.

However, it seems inevitable that once process and plant designs have been engineered to optimize processing safety, a spectrum of operating risks remain in many chemical operations. To deal with these risks, the European Seveso regulation mandates the development of a comprehensive Safety Management System that integrates technologies, procedures and management practices. The Directive addresses process hazard assessment, specification of risk control measures, evaluation of the consequence of failures of these controls, documentation of engineering controls, and scheduled maintenance to assure the ongoing integrity of the protective equipment. Basic process control and Safety Instrumented Functions (SIF) must be considered in each of these segments. Christou & Porter (1999) indicate that Article 10 of the Directive, which apply to lower tier as well as top tier Seveso establishments, covers modifications of an establishment, a storage facility, an installation or process or of the nature and quantity of dangerous substances which could have significant repercussions on major-accident hazards. In case of major modification, the facility operator is required *to review, and where necessary revise, the major-accident prevention policy and the management systems and procedures as well as the safety report, and inform the competent authority of the details of such revision in advance of such modification.* Moreover, Article 12 of the Directive requires *taking account of the need for additional technical measures so as not to increase the risks to people*. Hence, the Directive requires the operator to take all technical and meta-technical measures necessary to prevent major accidents and to limit their consequences.

By consequence, introducing a new installation into an existing chemical cluster is subject to reviewing or revising safety measures for the whole chemical cluster of which the new installation will be part of. An assessment of the implications on proactive safety measures will include a choice of Process Hazard Analysis (PHA) techniques intended to prevent any increase of internal or cross-company domino risks. However, plants subject to Seveso legislation remain responsible for setting their own safety criteria, selecting the risk analysis procedure(s) to use and basically defining how safe is safe enough.

Therefore, designing an optimizing framework for preventing cross-company domino effects in a situation where an installation is added to an existing facility needs to consider the following conditions:

- ***(a)*** an inherently safe process design approach for the new installation;
- ***(b)*** additional technical safety measures for the new installation, if necessary;
- ***(c)*** updating the safety precaution measures of all chemical installations in the existing cluster.

For preventing external domino accidents in an existing industrial area, Reniers *et al.* (2005b) suggest a standardized framework called Hazwim, based on the risk analysis procedures of Hazop, What-if analysis and the Risk Matrix. In the next section, this framework is evaluated against the prevention requirements for a modified industrial area. Section 3 suggests some PHA techniques capable of improving the selection of precaution measures to achieve inherent safety in case a major modification is made to an existing chemical cluster. For optimizing the choice of technical measures applied as last resort preventive tools, a Safety Integrity Level (SIL) upgrading selection is proposed. The possibility of implementing the proposed techniques is examined for Belgium, having the second largest cluster of chemical companies worldwide in the Antwerp harbor port area. So far, conditions ***(a)*** and ***(b)*** are satisfied. Section 4 integrates the proposed analysis techniques into an external domino accident prevention framework in case of adding equipment to an existing cluster of chemical industries, called *Installation Plus*, hereby fulfilling the last condition ***(c)***. The final section summarizes the most important conclusions.

2. A framework for preventing external domino risks in an existing installations network

In practice, the Hazop and What-if risk identification techniques have much in common (Reniers *et al.*, 2005b). Therefore, a meta-technical synergetic combination of these two Process Hazards Assessment identification techniques with a complementary risk evaluation method offers cooperation opportunities for all the participating companies to tackle external domino risks. Hence, in the Hazwim framework, the three complementary risk analysis techniques of Hazop, What-if analysis and the Risk Matrix are integrated.

In the first step of Hazwim, an extended Hazop risk identification technique is proposed to verify for external domino effects hazards. The next stage performs a Domino Hazard and Operability analysis. In the Hazop method as well as in the What-if technique, the multidisciplinary team examines the process conditions of each subsection of the system under investigation. In case of deviations from normal processing conditions possibly leading to one or more unwanted events, protection and mitigation safeguards are suggested.

The well-known risk evaluation technique of the Risk Matrix is used to evaluate Hazop results as well as What-if results. This evaluation method is a simplification with respect to confronting the results of a societal risk calculation with risk criteria in the shape of limit lines in an FN diagram. In this simple form levels rather than numbers are evaluated for the likelihood and the consequence of a given process hazard. A two-dimensional matrix is used to evaluate the likelihood/consequence levels to determine whether the safety measures proposed are sufficient. Based on this evaluation, a judgment is made as to whether the safety provided is adequate.

The benefits of these approaches (i.e. Hazop, What-if analysis and the Risk Matrix) are their relative simplicity and the requirement of limited resources. Moreover, these approaches are excellent for identifying loss scenarios. This makes them very popular and thus the associated know-how and expertise is widespread and readily available. They can be effectively used to qualitatively or semi-qualitatively analyze risks.

Therefore, Hazwim, an acronym for ***Haz***op, ***W***hat-***i***f analysis and the Risk ***M***atrix, seems to be a very powerful framework for enhancing cross-company cooperation on major hazards possibly leading to knock-on effects for an existing cluster of chemical plants or chemical installations.

However, these methodologies analyze scenarios only from initiating events (causes), to loss events and their impacts (consequences). They do not investigate the underlying physical and chemical hazards that must be contained and controlled for the process to operate safely, and thus they do not integrate inherent safety into the PHA. Hence, most action items that result from such PHA studies refer to existing safety procedures or refer to technical safeguards or require the addition of new levels of protection around the same underlying hazards.

The following risk identification methodology drawbacks can be mentioned:

(a) Hazop and What-if analysis rely heavily on the expertise of a team to identify potential accident scenarios and their perceptions on likelihood and losses associated with a hazardous event, thus may produce inconsistent results;

(b) it is difficult to document all thought processes that have led to the stated outcome;

(c) these methods do not provide the possibility to take preventive measures in the conceptual design phase.

Hazwim uses the Risk Matrix as a complementary risk evaluation procedure. Reniers *et al.* (2005a) point out that it is the most used industrial risk evaluation method at present day. Although very popular in industrial practice, Marszal *et al.* (1999) indicate that the Risk Matrix evaluation method has some important drawbacks:

(a) the qualitative approach does not provide enough resolution between layers of protection;

(b) the lowest frequencies assigned by teams of experts for many risk matrix applications are about 1 in 100 years. The selection of a Safety Integrity Level (e.g. SIL2 or an equivalent risk reduction factor of 1,000) is performed partially by estimating the likelihood of an impact event. Therefore, using the risk matrix does not always suffice to justify choosing for the use or not of a Safety Instrumented Function for reducing the likelihood e.g. from SIL1 to SIL2 (1 in 100 to 1 in 1,000 years).

(c) subjectivity can be high and variable.

These risk identification and -evaluation drawbacks indicate that the Hazwim framework is not suitable for the design of inherently safe process and taking additional technical prevention measures in the design phase of process equipment development. In other words, it is not recommended to use the Hazwim risk analysis procedures in case an existing establishment is modified by adding new equipment. Therefore, the next section proposes some risk analysis methods taking inherent safety into account.

3. Risk analysis procedures for achieving inherently safe equipment

3.1. Achieving inherent safety for new chemical equipment

If an installation is added to an existing chemical cluster, the most desirable requirement is that it is *inherently safe*. Achieving such inherent safety starts in the process design phase of the installation. An inherently safe process design approach includes the selection of the process itself, site selection and decisions on dangerous substances inventories and plant layout. Complete inherent safety is rarely achievable within economic constraints. Therefore potential hazards remaining after applying such an approach should be addressed by further specifying independent protection layers to reduce the operating risks to an acceptable level.

In current industry practice, chemical facilities processing dangerous substances are designed with multiple layers of protection, each designed to prevent or mitigate an undesirable event (Thurston, 1994). Multiple, Independent Protection Layers (IPL) addressing the same event are often necessary to achieve sufficiently high levels of certainty that protection will be available when needed. Powell (1994) defines an IPL as having the following characteristics:

(a) *Specific* – designed to prevent or to mitigate specific, potentially hazardous events, such as a runaway reaction, release of toxic materials, loss of containment or fire.

(b) *Independent* – independent of the other protective layers associated with the identified hazard.

(c) *Dependable* – can be counted on to operate in a prescribed manner with an acceptable reliability. Both random and systematic failure modes are addressed in the assessment of dependability.

(d) *Auditable* – designed to facilitate regular validation (including testing) and maintenance of the protective functions.

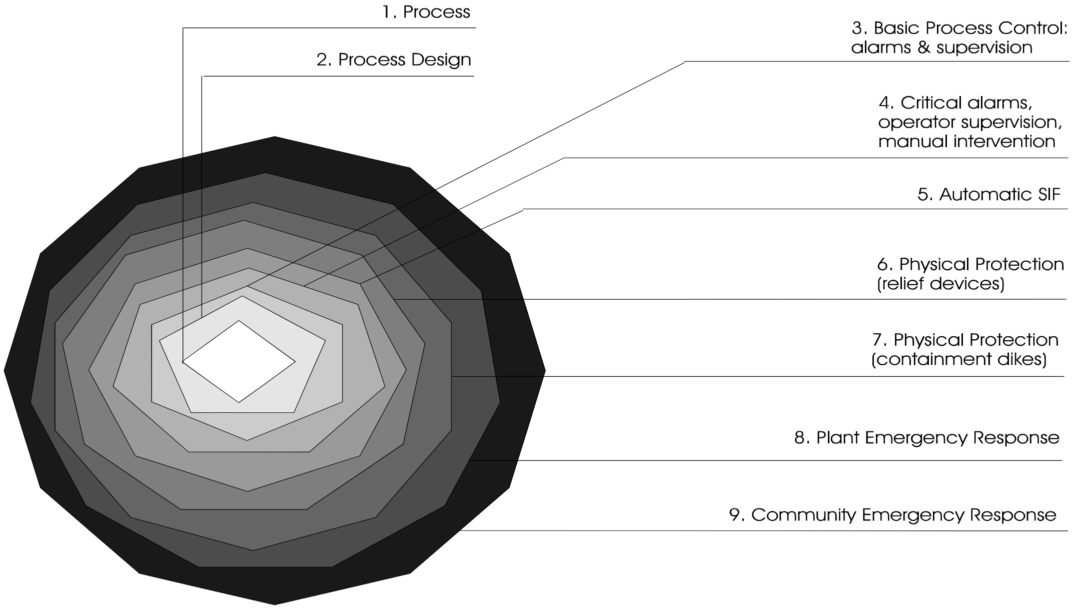
(e) *Reducing* – the likelihood of the identified hazardous event must be reduced by a factor of at least 100.

An IPL can thus be defined as a device, system or action that is capable of preventing a scenario from proceeding to its undesired consequence independent of the initiating event or the action of any other layer of protection associated with the scenario. The effectiveness and independence of an IPL must be auditable (Center of Chemical Process Safety, 2001).

Figure 1 illustrates safety layers of protection used in chemical process industry. Detailed process design provides the first layer of protection. Next come the automatic regulation of the process heat and material flows and the providing of sufficient data for operator supervision, together called the ‘basic process control systems’ (BPCS). A further layer of protection is provided by a high-priority alarm system and instrumentation that facilitates operator-initiated corrective actions. A Safety Instrumented Function (SIF)[1], sometimes called the emergency shutdown system, may be provided as the fourth protective layer. The safety interlocks are protective systems which are only needed on those rare occasions when normal process controls are inadequate to keep the process within acceptable bounds. A SIF is a combination of sensors, logic solvers, and final elements with a specified Safety Integrity Level (SIL) that detects an out-of-limit condition and brings the process to a functionally safe state. Any SIF will qualify as one IPL. Physical protection may be incorporated as the next layer of protection by using venting devices to prevent equipment failure from overpressure. Should these IPL fail to function, walls or dikes may be present to contain liquid spills. Plant and community emergency response plans further address the hazardous event.

[1] This is a newer, more precise term for a Safety Interlock System (SIS).

Figure 1. Typical Layers of Protection found in modern chemical processing plants


1. Process
2. Process Design
3. Basic Process Control: alarms & supervision
4. Critical alarms, operator supervision, manual intervention
5. Automatic SIF
6. Physical Protection (relief devices)
7. Physical Protection (containment dikes)
8. Plant Emergency Response
9. Community Emergency Response

Source: based on Center for Chemical Process Safety, 1993.

By considering the sequence of events that might lead to a potential incident, another representation can be developed highlighting the efficiency of the protection layers, as shown in Figure 2.

Figure 2. Anatomy of a chemical incident (with e.g. 4 SIFs)

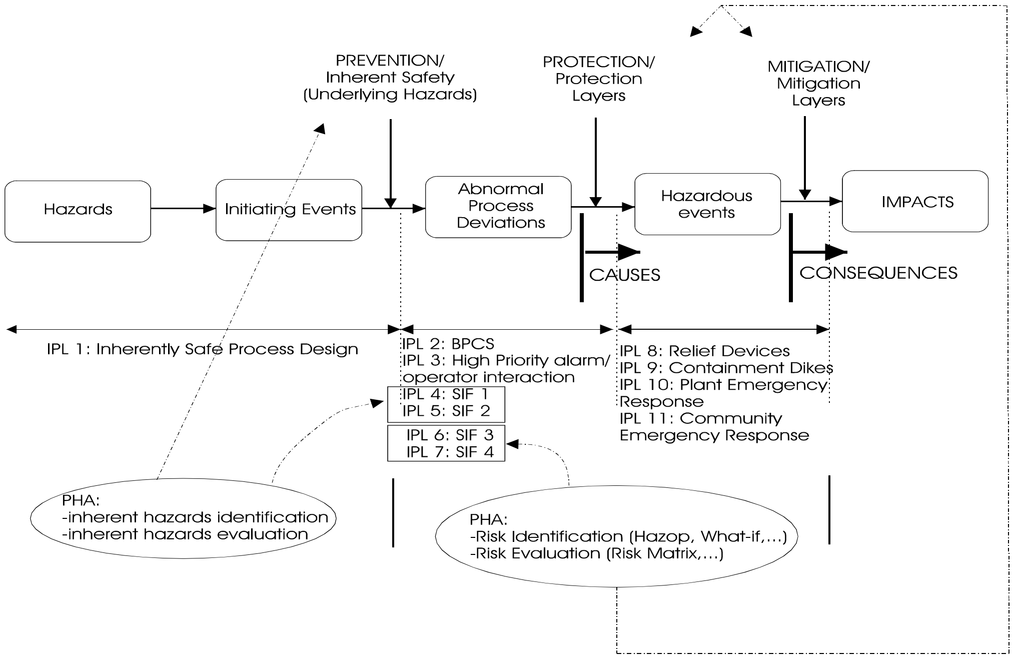

PREVENTION/
Inherent Safety
(Underlying Hazards)
PROTECTION/
Protection
Layers
MITIGATION/
Mitigation
Layers
Hazards
Initiating Events
Abnormal Process Deviations
Hazardous events
IMPACTS
CAUSES
CONSEQUENCES
IPL 1: Inherently Safe Process Design
IPL 2: BPCS
IPL 3: High Priority alarm/ operator interaction
IPL 4: SIF 1
IPL 5: SIF 2
IPL 6: SIF 3
IPL 7: SIF 4
IPL 8: Relief Devices
IPL 9: Containment Dikes
IPL 10: Plant Emergency Response
IPL 11: Community Emergency Response
PHA:
-inherent hazards identification
-inherent hazards evaluation
PHA:
-Risk Identification (Hazop, What-if,...)
-Risk Evaluation (Risk Matrix,...)

Figure 2 also illustrates the benefits of a risk identification approach that can be used to examine inherent safety by considering the underlying hazards of a hazardous substance, a process or an operation. Using such an inherent identification method can be especially recommended for application in a framework where a new installation is added to an existing establishment. Inherently safer features in a process design can reduce the required SIL of the SIF, or can even eliminate the need for a SIF, thus reducing cost of installation and maintenance. Indeed, the Center for Chemical Process Safety (1996) suggests that added-on barriers applied in non-inherently safer processing conditions have some major disadvantages:

(a) the barriers can be expensive to design, build and maintain;

(b) the hazard is still present in the process;

(c) accumulated failures of IPLs can still result in an incident.

Methods that consider underlying hazards include Preliminary Hazards Analysis, Hazard-Barrier-Target and Loss of Containment Analysis. These methods are briefly explained and discussed by Johnson (1999), indicating that, except for the Loss of Containment technique, each is relatively specialized in its application.

The most applied risk evaluation method is the Risk Matrix. Other risk evaluation methods used in the industry are *Layer Of Protection Analysis* (LOPA), *Fault Tree Analysis* (FTA) and *Financial Risk Analysis* (FRA). The quantitative methods of FTA and FRA require a detailed analysis of the likelihood, consequence and impact and therefore the costs associated with these methods may not be justified in most situations. The simplified quantitative analysis of LOPA can be applied to evaluate scenarios that are too complex for only qualitative review and the technique is able to screen which scenarios need more quantitative scrutiny than LOPA implementation itself. As explained by the Center of Chemical Process Safety (1996), LOPA is an ideal tool to assist in developing designs that have an inherently lower risk associated with them, or which require the minimum number of IPLs to achieve a tolerable risk. Using scenarios and the simplified assumptions and calculation methods allows rapid comparisons to be made between alternative designs and safety philosophies.

Like other evaluation methods currently employed throughout the chemical industry, the primary purpose of the Risk Matrix or of LOPA is to determine if there are sufficient layers of protection against an accident scenario. As already mentioned, a scenario may require one or more protection layers depending on the process complexity and the potential severity of a consequence. Note that for a given scenario only one layer must work successfully for the consequence to be prevented. However, since no layer is perfectly effective, sufficient protection layers must be provided to render the risk of the accident tolerable. Therefore, it is very important that a consistent basis is provided for judging whether there are sufficient IPLs to control the risk of an accident for a given scenario. Especially in the process design phase an approach for drafting inherent safety into the process by implementing satisfactory IPLs is needed for effective process safety. In many cases the Safety Instrumented Functions are the final independent layers of protection for preventing hazardous events. Moreover, all SIFs are required to be designed such that they achieve a specified Safety Integrity Level. Therefore, the SIL selection, which is the secondary task to be performed by a risk evaluation method, is critical for process safety. As illustrated in Figure 1, if the target plant process safety cannot be achieved (i.e. the intermediate event likelihood is not acceptable) by non-SIF systems, then SIFs are to be used for achieving a Safety Integrity Level (SIL) predefined by company safety management. In the next section, the use and the selection of SILs are explained.

3.2. Safety Integrity Levels for new chemical equipment

The International Society for Measurement and Control (ISA) and the International Electrotechnical Commission (IEC) have promulgated industry standards to assist in compliance with process safety management requirements for the mechanical integrity of all emergency shutdown systems and safety critical controls. The European IEC 61511 standard (International Standard, 2003) requires that all electrical, electronic and programmable electronic systems, used in SIFs, be designed, operated and maintained such that they achieve a specified Safety Integrity Level (SIL). The SIL is the quantification of the Probability of Failure on Demand of a SIF into four discrete categories. Table 1 gives an overview of such levels.

Table 1. Safety Integrity Levels

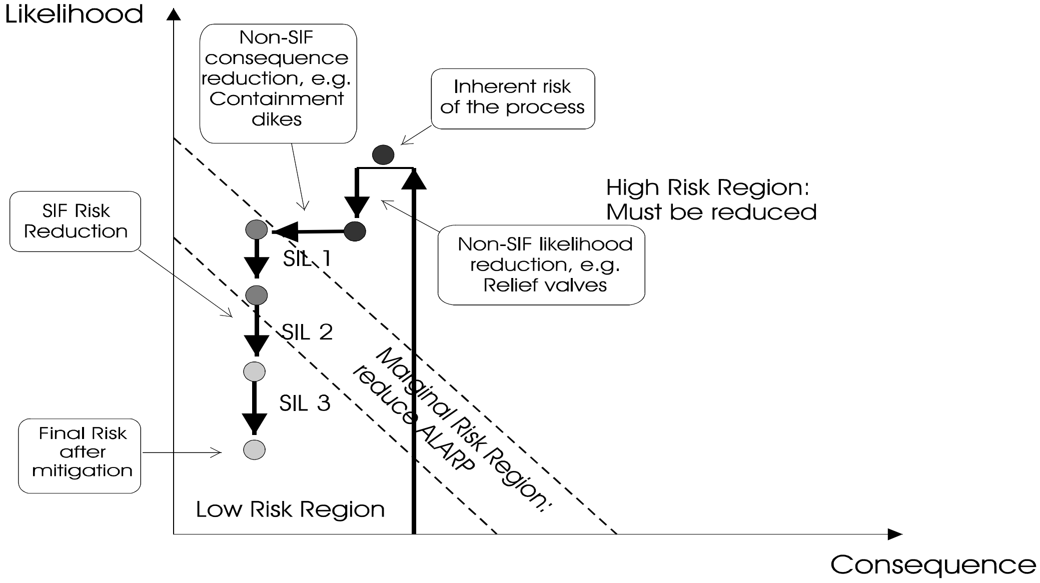
Safety Integrity Level (SIL)	*Safety Availability*	*Probability to Fail on Demand (PFD)*	*Equivalent Risk Reduction Factor (1/PFD)*
SIL 4	>99.99%	>= 10^{-5} to <10^{-4}	10,000 – 100,000
SIL 3	99.9 – 99.99%	>= 10^{-4} to < 10^{-3}	1,000 – 10,000
SIL 2	99 – 99.9%	>= 10^{-3} to < 10^{-2}	100 – 1,000
SIL 1	90 – 99%	>= 10^{-2} to < 10^{-1}	10 – 100

Source: based on Gruhn (1999) and International Standard (2003).

Thus, four corresponding degrees of reduction in hazardous event likelihood are produced by the SILs. SIL 1 provides about two orders of magnitude of event likelihood reduction; SIL 2 about three orders of magnitude, SIL 3 about four orders of magnitude and SIL 4 more than four orders of magnitude. Obviously, the availability targets for SIL 3 and SIL 4 are extremely stringent and the design practices to achieve and maintain these high levels are extensive and costly.

Gardner (1994) points out that methods used to select safety integrity levels are based on an evaluation of three characteristics of the process and the hazardous event associated with the SIF: the severity of the hazardous event consequences (minor, serious, extensive), the likelihood that an upset situation will occur that could lead to these consequences (low, moderate, high) and the number of IPLs. Before a SIL can be selected, the inherent risk of the process must be evaluated. Next, credit for all non-SIF mitigation measures (e.g. relief valves, dikes) must be accounted for, to determine the baseline risk of the process, which is the starting point of the SIL selection. All of the SIF design, operation, and maintenance choices have to be verified against the target SIL. The safety design engineer has to realize that further mitigation with a SIF solely reduces the likelihood of an incident. For example, if the baseline likelihood is 10^{-2} per year, a SIL 2 would reduce the likelihood up to 10^{-5} per year. The risk reduction process is illustrated in Figure 3, in which risk criteria are represented in the form of FN limit lines.

Figure 3. The effect of risk reduction measures


Likelihood
Non-SIF consequence reduction, e.g. Containment dikes
Inherent risk of the process
High Risk Region: Must be reduced
SIF Risk Reduction
Non-SIF likelihood reduction, e.g. Relief valves
SIL 1
SIL 2
SIL 3
Marginal Risk Region; reduce ALARP
Final Risk after mitigation
Low Risk Region
Consequence

Source: based on Marszal (1998).

Determining the necessity of IPLs and SIFs and the required level of their safety integrity is performed using risk analysis identification and –evaluation methods. No one approach for the selection of a SIL is appropriate in every situation. Often, little to no benefit is obtained in reducing the risks with the selection of a higher SIL. Therefore, a phased approach that utilizes simpler methods to screen lower risk operations and systematically progresses to more complex techniques is being proposed in the framework elaborated in section 4. Using the latter procedure, the SIL selection process for preventing external domino risks in case an installation is added to an establishment is optimized.

Summarizing, the SIL must be chosen to reduce the incident frequency to a tolerable level. It is the design basis for all engineering decisions related to the safety instrumented function. When the design is complete, it must be validated against the SIL. Therefore, the safety integrity level closes the design cycle: starting with hazards identification, pursuing with requirements quantification and ending with design validation.

3.3. The Belgian case: Planop

3.3.1. Introduction

In Belgium, a lot of different risk analysis techniques exist in the processing industry. Most of these techniques are deviation analyses and thus are not intended for use in the design phase. A deviation analysis such as Hazop uses concepts like 'risk' and 'measure' to search for deviations or errors in an existing design. In such an approach, the starting-point is a deviation from a parameter or the failure of an installation item or equipment. Hence, the method is not developed for identifying hazards in the design-phase.

Table 2 summarizes the major differences between deviation (or distortion) analysis approaches and design analysis approaches.

Table 2. Differences between Deviation Analysis and Design Analysis

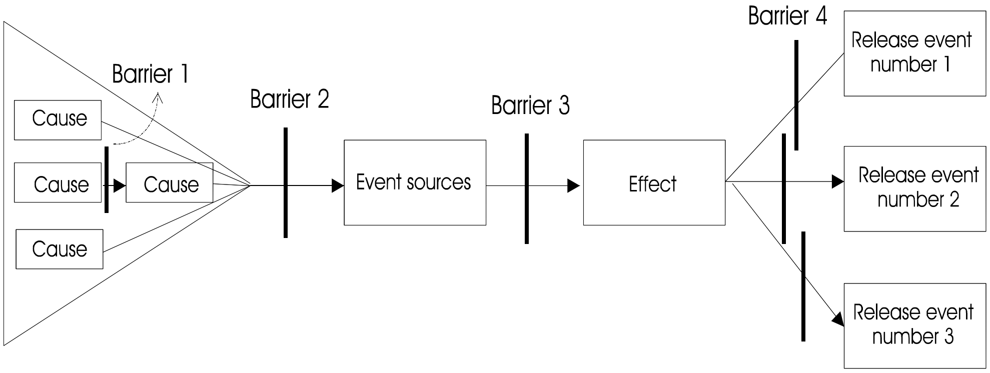
Deviation Analysis	***Design Analysis***
Qualitative risk assessment	Semi-quantitative risk assessment
Add-on safer approach	Inherently safer approach
Used on existing installations (e.g. during installation changes)	Used early in the development phase of an installation
Generally applicable for all kinds of incidents/accidents (operability and safety)	Specifically applicable for preventing and mitigating major accidents
Needs PID plans	No documents required

For enhancing inherent safety in Belgian Seveso companies, the Belgian Federal Government has developed a process design analysis called Planop. Progressive Loss of Containment Analysis – Optimizing Prevention, abbreviated as 'Planop', is a computer-based methodology for performing semi-quantitative risk analyses for chemical process installations. Planop has been elaborated by the Chemical risks Directorate of the Belgian Federal Ministry of Employment, Labour and Social Dialogue (Chemical Risks Directorate, 2003). Planop is divided into two independent parts that can be performed separately: a Loss of Containment Hazard Analysis (LOC-HA) on the one hand and a risk evaluation method through the use of Layers of Protection Analysis (LOPA) on the other. Planop is a method that reduces or eliminates hazards by applying inherently safer concepts to the process design and chemistry, and is therefore promising to use as a risk identification and –evaluation technique in case of adding chemical equipment to an existing industrial area.

3.3.2. Risk identification by Planop

The first step of the Planop procedure identifies all possible root causes and all possible consequences of undesired releases of matter (e.g. hazardous materials) or energy. In this approach, the release analysis is systematically executed individually for each installation subsystem by introducing the concept of the bow-tie; Bowtie models are tools for integrating broad classes of cause-consequence models. The familiar fault tree-event tree models are 'bowtied' in this way; indeed, attaching the fault tree's 'top event' with the event tree's 'initiating event' originally suggested the bowtie metaphor. The bowtie may be conceived as a lens for focusing on causal chains and 'projecting' these onto the space of consequences. These consequences will ultimately be factored into decision problems for risk management. Hence the bowtie's consequence side forms an interface with the decision models. Decisions taken will reflect backwards to causes. This structure not only has proven a worth while concept in accident prediction it also has proven its worth in analysing past accidents and suggest improvements to prevent further re-occurrence The bow-tie connects Causes and Consequences by their causal path through a singe centre event (Haddon, 1973 and Papazoglou *et al.*, 2003). By placing barriers in pathways from cause to consequence the development of an accident can be prevented. Figure 4 illustrates the way Planop identifies release events and takes preventive measures (represented by 'barriers') on different levels. Event sources in Planop can be compared with Hazop deviation parameters.

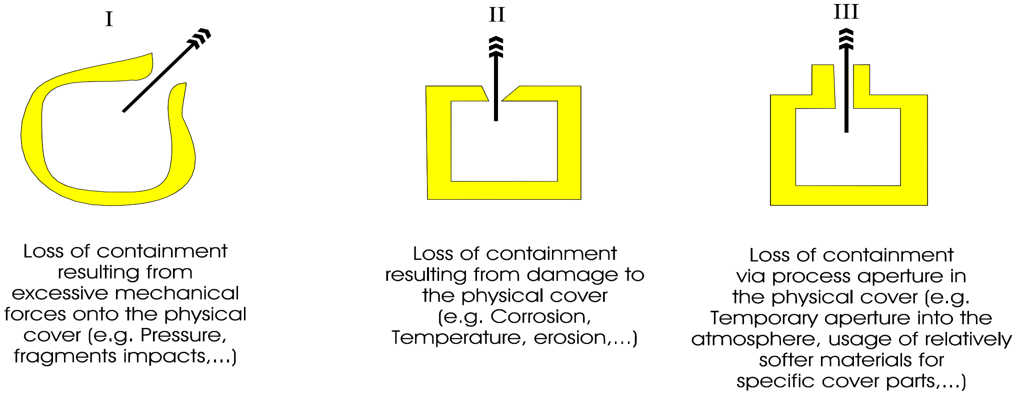
Figure 4. Tree of release causes as implemented by Planop



Source: Chemical Risks Directorate, 2005.

LOC-HA defines event sources as phenomena, conditions or properties of an installation that could lead to an accidental loss of containment of substances or energy. The three types of event sources are depicted in Figure 5.

Figure 5. The three Planop mechanisms for the undesired release of substances and energy

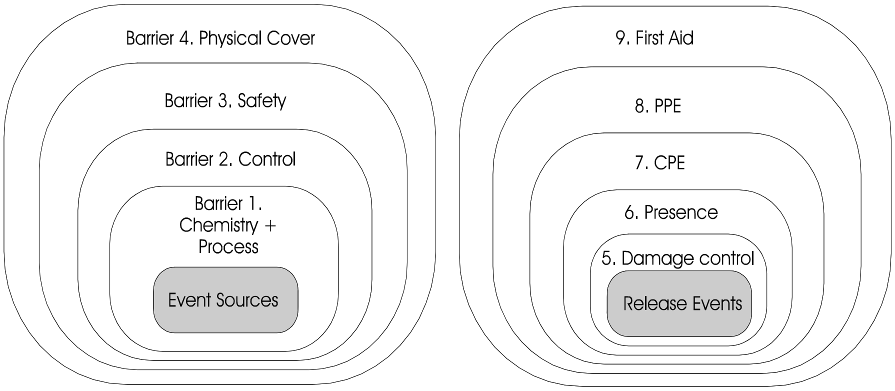

I
II
III
Loss of containment resulting from excessive mechanical forces onto the physical cover (e.g. Pressure, fragments impacts,...)
Loss of containment resulting from damage to the physical cover (e.g. Corrosion, Temperature, erosion,...)
Loss of containment via process aperture in the physical cover (e.g. Temporary aperture into the atmosphere, usage of relatively softer materials for specific cover parts,...)

Source: based on Chemical risks directorate, 2005.

Release events are defined as critical events that may result from an undesired release. Three different types are classified: release, dispersion and impact. Such release events are elaborated in detail by the user.

The next step in the first part of the Planop methodology is proposing prevention measures for avoiding the presence of undesired event sources and proposing mitigation measures for limiting the consequences of release events. The method allows for a very systematic determination of general and specific measures. For each event source and release event, a package of measures capable of adequately reducing the risks is then divided among ‘protection layers’. The set of nine Planop protection layers is depicted in Figure 6 and linked with Figure 4 indicating the prevention barriers. A brief description of the various protection layers is presented in Table 3.

Figure 6. The Planop protection layers



Source: Chemical risks directorate, 2005.

Table 3. Planop protection layer descriptions

Protection layer	***Description***
1. Chemistry + Process	Measures related to the choices of substances and reactions. Design choices with a preventative function.
2. Control	Active prevention measures whose function is not exclusively related to safety.
3. Safety	Active prevention measures whose function is exclusively related to safety.
4. Physical cover	A physical cover is the wall of a vessel, a pipe, a tank, etc.
5. Damage control	Measures that limit the amounts of released substances, hinder dispersion of released substances or prevent the possible ignition of flammable substances.
6. Presence	Measures aimed at restricting the presence of people in the hazard area.
7. CPE	Collective Protective Equipment.
8. PPE	Personal Protective Equipment.
9. First aid	Measures to limit damage that has already been suffered as the result of an undesired release.

Source: Chemical risks directorate, 2005.

3.3.3. Risk evaluation by Planop

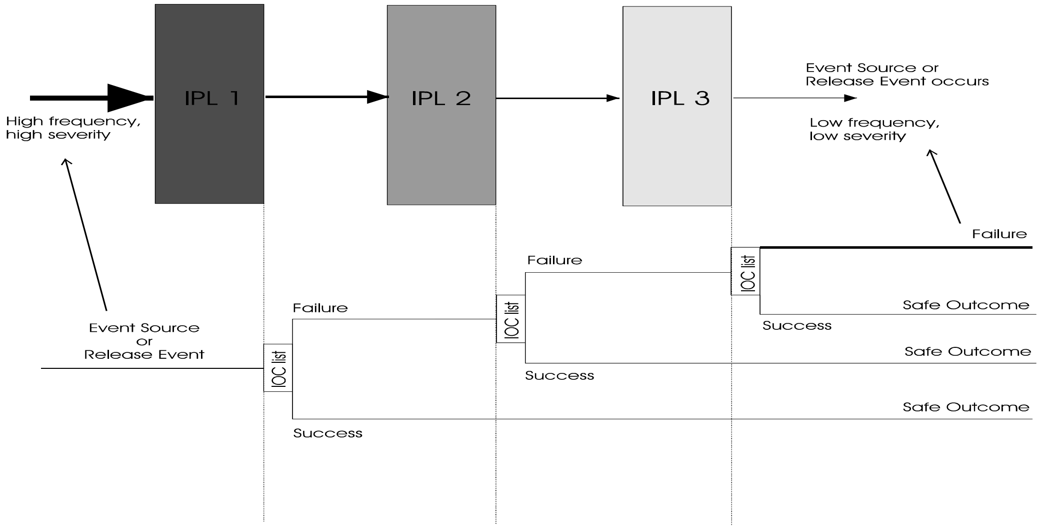
The second part of the Planop procedure is analyzing the effectiveness and the reliability of the proposed measures. A LOPA is performed to determine per hazard how many layers of protection are needed in total to reduce the risk to a tolerable level and to determine what Safety Integrity Level is required for a Safety Instrumented Function.

Planop uses reliability- and effectiveness factors called ‘items of consideration’ (IOC) to analyze the protection layers and thus the measures. Items of consideration can be for example:

- supplementary specifications related to the detailed design of the measure;
- organizational measures related to maintaining or enforcing the measure;
- supplementary measures.

In Figure 7 a graphical model illustrates the IOC analysis process of an event source or a release event executed at the level of each Independent Protection Layer (IPL). Results of an IPL analysis can be a list of Items Of Consideration. Such an inventory of IOC per IPL determines its efficiency and justifies its Safety Integrity Level.

Figure 7. Graphical model of LOPA used in Planop



Source: based on Dowell, 1999.

Dowell (1999) remarks that the concept of Layer of Protection Analysis seems to be at odds with the concept of inherently safer processes, because *'inherently safer'* implies the redundancy of add-on layers to enhance risk reduction. Indeed, one application of inherent safety is to reduce the hazard inherent in the material or the chemistry of the process. Such changes reduce the severity of the consequence. However, reducing the inherent hazard in the process may not be sufficient to meet the risk criteria. Thus, an important second application of so-called *'inherently safer'* is to design the independent protection layers to be "stronger". This application reduces the frequency of the consequence.

3.3.4. Safety documentation by Planop

An important asset of Planop is the way it is integrated into the design process. Performing a Planop analysis for a process installation corresponds to building up a structured database of safety-related information for the installation. The data structure can be built up in parallel with the various stages of the design process, using the information about the installation being designed that becomes available at each stage. Various documents and plans are generated during this evolution. This concept is what is expressed by the key word *'progressive'* in the Planop acronym (Progressive Loss of Containment Analysis – Optimizing Prevention) due to its proactive risk analysis character.

The output of a Planop procedure is a structured overview of all the information that is relevant to the issue of undesired releases:

- Causes and consequences of undesired releases;
- Associated measures with reliability analysis;
- Relevant data for substances and reactions.

This type of overview is an essential input to the plant Safety Management System, being tasked with the maintenance, the regular review and the continuous improvement of these measures. When changes are made to an installation, a structured overview of the causes and consequences of losses of containment forms a good starting-point for investigating the impact of the changes on the question of an undesired release. Information in the Planop files must be updated when new risks are identified or new measures are specified.

The 'event source' concept used in the Planop methodology emphasizes the different nature of the method compared with more traditional risk analysis techniques such as Hazop or the What-if procedure. Planop is based on the idea that substances and energy confined and processed within a restricted volume (pipes, vessels, etc.) have an urge to escape. High and low pressures can be present in an installation; the physical cover can be exposed to aggressive and destructive influences; openings are provided in an installation, inherently introducing the possibility of being opened at the wrong time; relatively weak point are present in an installation. Consequently, the presence of event sources does not represent a design fault, but it is the consequence of fundamental design choices, presenting ‘challenges’ to the installation. It is the responsibility of the designers of the installation to respond to these challenges.

3.3.5. Planop implemented in the Belgian Seveso industry

Planop being elaborated by the Chemical risks inspectorate, part of a Directorate of the Belgian Federal Ministry of Employment, Labour and Social Dialogue, is actively promoted by the Belgian Government. The first version of the technique was released in September 2002. The second version (2.01) debugged, corrected and added with a list of FAQ (in dutch) available online, dates from October 2004.

Companies are tended to use the method because it optimizes the efficiency to collect and to retrieve technical and meta-technical safety related information at any time. The Planop methodology also allows keeping hierarchically structured updated safety information, which is easy auditable and controllable by company reviewers and external inspectors.

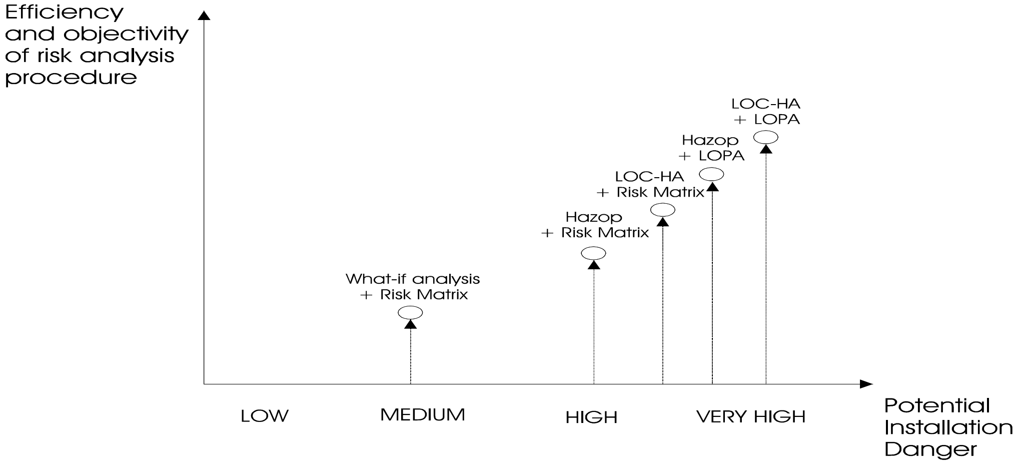
At present, in about a dozen plants situated in Belgium the whole technique or parts of the technique is already implemented.

4. The ‘*Installation Plus*’ framework for preventing external domino risks in case of adding an installation to an existing chemical cluster.

The objective of this paper is to elaborate a framework for promoting cooperation between plants being part of a chemical cluster in case of installation addition to one of the plants of the cluster. Such a framework requires the choice of PHAs usable in the design phase and requires the ability to make optimizing SIL selection choices.

Verschueren (2003) illustrates (see Figure 8) that making a choice between different combinations of risk identification- and risk evaluation approaches depends on the required efficiency and objectivity of the method on the one hand and the potential danger of the investigated installation on the other.

Figure 8. Necessary efficiency and objectivity of some risk analyses versus potential installation danger

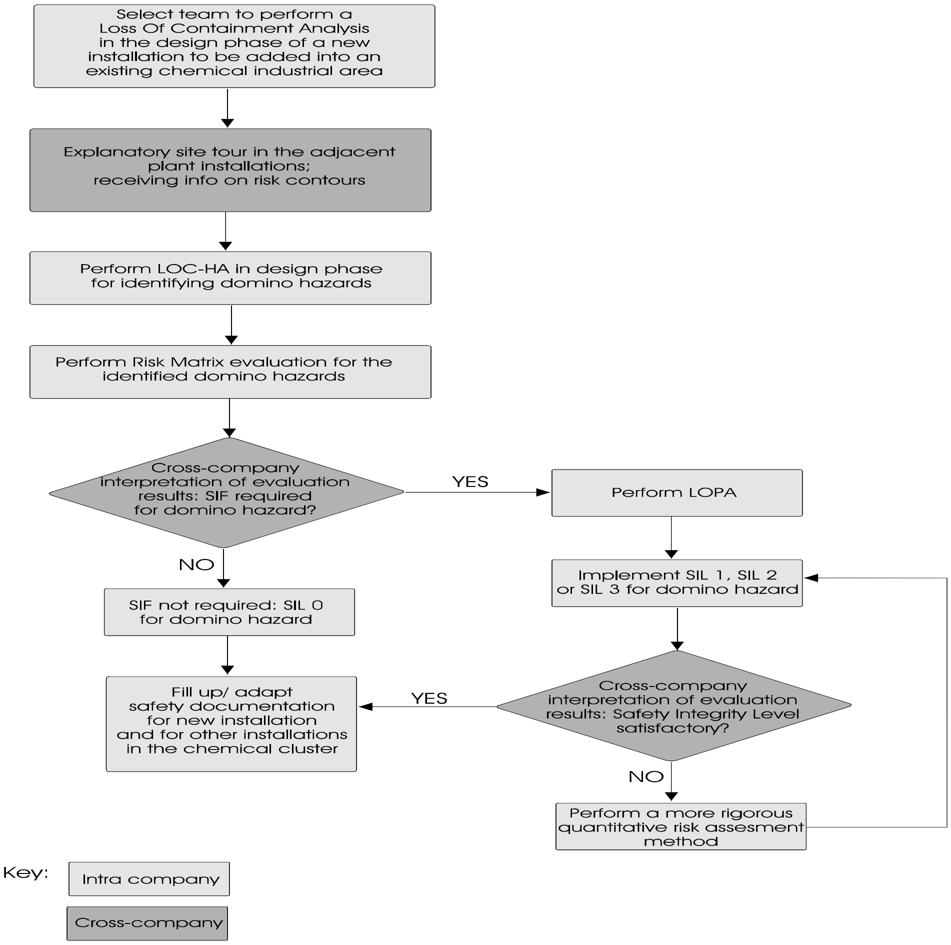


Source: based on Verschueren, 2003.

If an existing chemical complex is modified by the adding of an installation, cross-company danger for domino effects have to be investigated as conscientiously as possible in the earliest possible design phase to prevent hazardous domino events. Therefore, the authors suggest that in the process design risks are identified using for example LOC-HA and then evaluated using e.g. the Risk Matrix or LOPA.

Figure 9 illustrates an external domino framework called "*Installation Plus*", taking into account the confidentiality of plant data and gradually upgrading the selection of Safety Integrity Levels (see section 3.2).

Figure 9. "Installation Plus" Framework for external domino effects prevention for adding an installation to an industrial area

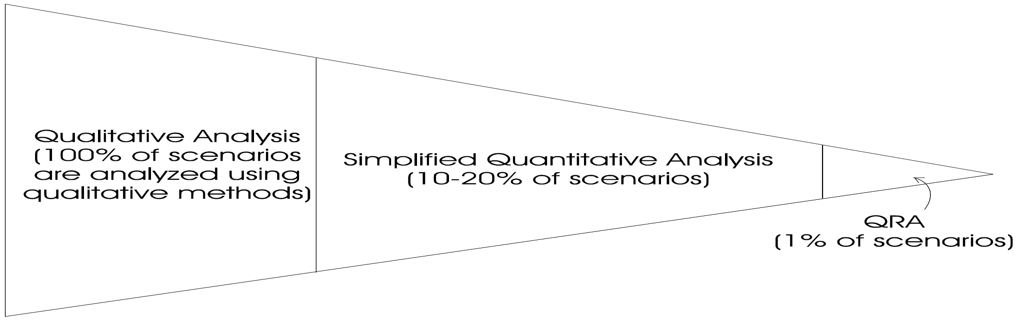

Select team to perform a Loss Of Containment Analysis in the design phase of a new installation to be added into an existing chemical industrial area
Explanatory site tour in the adjacent plant installations; receiving info on risk contours
Perform LOC-HA in design phase for identifying domino hazards
Perform Risk Matrix evaluation for the identified domino hazards
Cross-company interpretation of evaluation results: SIF required for domino hazard?
YES
Perform LOPA
NO
SIF not required: SIL 0 for domino hazard
Implement SIL 1, SIL 2 or SIL 3 for domino hazard
Fill up/ adapt safety documentation for new installation and for other installations in the chemical cluster
YES
Cross-company interpretation of evaluation results: Safety Integrity Level satisfactory?
NO
Perform a more rigorous quantitative risk assesment method
Key:
Intra company
Cross-company

Since the magnitude of all consequence effects reduces with distance from the source, it is clear that the physical separation between the respective installations influences the potential for domino effects to occur. In this context, prior to applying the Installation Plus Framework of Figure 5, an assessment of the land-use planning implications of a proposed modification to an existing industrial area has to be performed. Based on either a consequence based approach, a risk based approach, tables of appropriate distances or even a hybrid approach borrowing and combining elements from the prior mentioned approaches, the safety of the surrounding complex is assessed and risks imposed on the environment are determined (Christou, 1999). The emphasis in such a risk assessment should not be given to the absolute accuracy of its predictions, but rather to its success or failure in demonstrating or improving the safety of the chemical cluster.

In the first stage of the framework, a Loss Of Containment analysis team familiar with the hazardous substances and with the activities processed in the new installation is selected. The team should consist of an operator with experience operating the process under consideration, an engineer with expertise in the process, manufacturing management, a process control engineer, an instrument/electrical maintenance person and a risk analysis specialist trained in the LOPA methodology. Once the team members are chosen, a guided tour to the nearby installations on the premises of the own plant, but also on the premises of neighboring plants is to be organized and risk contour results of all installations concerned are collected. Next, these data are used to perform a Loss Of Containment Hazards Analysis to identify all possible (internal and external) domino hazards in the design phase of the installation. To evaluate the need for a Safety Instrumented Function ensuring the non-occurrence of an identified domino hazard, the Risk Matrix is used. Matrix evaluation results are then discussed by the members of the LOC team and experienced safety engineers of the nearby plant(s). If there is no need for a SIF at all, no further actions are taken and safety documentation concerning the domino hazard is filled up. If the effect of non-SIF risk reduction measures is not satisfactory, LOPA is performed. LOPA should be applied when the qualitative hazard analysis reveals the need for reducing risks, but the team is either unsure of the consequences or unsure of the frequency of the final consequences or concerned that the processes or scenarios are too complex to address qualitatively. Once more, a cross-company interpretation of SIL results must address the issue of the domino risk tolerability. If the risk level determined by LOPA application is judged satisfactory, safety documentation is filled up concerning the domino risk. If the latter is not the case, the scenario will be targeted for a higher level of quantitative risk assessment such as FTA.

Figure 10 depicts the spectrum of risk assessment tools: from purely qualitative to rigorous application of quantitative methods.

Figure 10. Spectrum of tools for risk-based decision-making



Source: CCPS, 2001.

At the left hand side qualitative tools such as Hazop, What-if analysis and the Risk Matrix can be situated. These tools are used to identify scenarios and qualitatively judge if the risk is tolerable. In the middle are semi-quantitative tools such as LOPA, used to provide an order-of-magnitude estimate of risk. At the right hand side, quantitative tools are situated to analyze very complex scenarios.

5. Conclusions

The best long term approach to chemical process safety is through the use of inherent safety. Inherent safety process improvements can be described as those that essentially eliminate hazards from the process. Inherent safety is obviously safer than controlling the hazards with even the safest or highest integrity Safety Instrumented Functions.

Thus, using the appropriate PHA techniques aimed at inherently safe process design during the process of constructing a new chemical installation helps assuring long term effective and efficient implementation of safety measures and induces cost effective facilities. The importance of ensuring that independent, diverse protection layers meet the specifications of the process hazards analysis team cannot be highlighted enough. It guarantees the best possible total system safety. Only when the design intent is met and maintained, the total risk control strategy for the plant is effective. Implementing PHAs developed for enclosing inherent safety into the process design is the first requirement during the design phase.

For optimizing external knock-on prevention in case an installation is added to a chemical cluster, the second requirement is to enhance cooperation between neighboring companies. Therefore, a scheme is elaborated that combines the use of a risk identification technique suited for implementation in inherent safety designing, i.e. loss of containment analysis, and a risk evaluation technique. The latter evaluation method is either the Risk Matrix (performed in case of a first level screening) or a layer of protection analysis (used for assigning SILs in a more quantitative way). In the so-called *Installation Plus* framework, safety engineers from neighboring companies cooperate by discussing evaluation results of external domino risk reduction. This way, in case an installation is added to an industrial area, potential escalation effects between plants being part of that area, possibly leading to a major accident, are prevented through cross-company cooperation in an optimizing way.

Acknowledgements

The authors wish to acknowledge the contribution of Ir. Frank Verschueren, inspector of the Belgian Federal Government, thanking him for his remarks concerning Planop. The authors also wish to thank the plant safety managers who took the time to read and to comment on the paper.

Bibliography:

Bhimavarapu, K., Stavrianidis, P., *Safety Integrity Level Analysis for Processes – Methodologies and Issues,* Factory Mutual Research Corp., Norwood, Massachusetts, 1999.

Carrithers, G.W., Dowell III, A.M. and Hendershot, D.C., *It's Never Too Late for Inherent Safety*, International Conference and Workshop on Process Safety Management and Inherently Safer Processes, October 8-11, 1996, Orlando, Florida, 227-241, New York, American Institute for Chemical Engineers.

Center for Chemical Process Safety (CCPS), *Guidelines for Process Equipment Reliability Data with data tables*, New York, 1989.

Center for Chemical Process Safety (CCPS), *Guidelines for Safe Automation of Chemical Processes*, New York, 1993.

Center for Chemical Process Safety (CCPS), *Inherently safer chemical processes, a life cycle approach*, 1996.

Center for Chemical Process Safety (CCPS), *Layer of Protection Analysis, simplified process risk assessment*, New York, 2001.

Chemical Risks Directorate, available online: www.meta.fgov.be (2005).

Chemical Risks Directorate, *PLANOP: A method for performing loss of containment analyses*, FPS Employment, Labour and Social Dialogue, Brussels, 2003.

Christou, M.D. & Porter, S., Guidance on Land-use planning as required by Council Directive 96/82/EC (Seveso II), Institute for systems informatics and safety, European Communities, 1999.

Cocchiara, M., Bartolozzi, V., Picciotto, A., Galluzzo, M., Integration of interlock system analysis with automated HAZOP analysis, *Reliability Engineering and System Safety* 74 pp. 99-105, 2001.

Dowell, A.M. III, *Layer of Protection Analysis and Inherently Safer Processes*, Rohm and Haas Company, 1999.

Drake, E.M., *An Integrated approach for determining appropriate integrity levels for chemical process Safety Instrumented Functions,* Massachusetts Institute of Technology, Cambridge, Massachusetts, 1994.

Gardner, R.J., Reyne, M.R., *Selection of Safety Interlock Integrity Levels*, Dupont Engineering, 1994.

Gruhn, P., Lessons Learned on Safety Instrumented Systems Design, Moore Process Automation Solutions, Houston, 1999.

Haddon Jr, W., Energy Damage and the Ten Counter Measure Strategies, *Human Factors Journal*, 1973.

International Standard IEC-61511, 1st ed., 2003.

Johnson, R., *Analyze Hazards, Not Just Risks*, Unwin Company, 33rd Annual Loss Prevention Symposium, 1999.

Marszal, E.M., Fuller, B.A., Shah, J.N., *Comparison of Safety Level Selection Methods and Utilization of Risk Based Approaches*, Four Elements Inc., Columbus, Ohio, 1999.

Papazoglou I.A., L.J. Bellamy, A.R. Hale, O.N. Aneziris, B.J.M. Ale, J.G. Post, J.I.H. Oh, I-Risk: development of an integrated technical and management risk methodology for chemical installations, *Journal of Loss Prevention in the Process Industries* 16 (2003) 575–591.

Powell, R.L., *Process Safety and Control Systems Integrity*, International Conference and Workshop on Process Safety Management and Inherently Safer Processes, October 8-11, 1996, Orlando, Florida, 227-241, New York, American Institute for Chemical Engineers.

Reniers, G., Dullaert, W., Ale, B.J.M., Soudan, K., The use of current risk analysis tools for preventing external domino accidents, *Journal of Loss Prevention in the Process Industries,* available online, 2005a.

Reniers, G.L.L., Dullaert, W., Ale, B.J.M., Soudan, K., Developing an External Domino Accident Prevention Framework: Hazwim, *Journal of Loss Prevention in the Process Industries*, available online, 2005b.

Thurston, C.W., *Automation in chemical plant safety: a design philosophy,* in: International Symposium and Workshop on Safe Chemical Process Automation, Center for Chemical Process Safety (CCPS), Health and Safety Executive (HSE), Chemical Manufacturers Association (CMA), IEC, ISA, Houston, Texas, September 27-29, 1994.

Verschueren, F., *Risicoscenarios Zware Ongevallen, identificatie en documentatie van risicoscenario's en bijhorende maatregelen voor zware ongevallen bij Sevesobedrijven d.m.v. de Planop-methodiek,* Lucina, Leuven, 2003.