Process Systems Engineering, 7. Abnormal Events Management and Process Safety

ULLMANN'S ENCYCLOPEDIA OF INDUSTRIAL CHEMISTRY

Gürkan Sin, Technical University of Denmark, CAPEC, Department of Chemical and Biochemical Engineering, Lyngby, Denmark

Kaushik Ghosh, National University of Singapore, Department of Chemical and Biomolecular Engineering, Singapore

Sathish Natarajan, National University of Singapore, Department of Chemical and Biomolecular Engineering, Singapore

Rajagopalan Srinivasan, National University of Singapore, Department of Chemical and Biomolecular Engineering, Singapore

Arief Adhitya, Institute of Chemical and Engineering Sciences, A*Star, Singapore

Iftekhar A. Karimi, National University of Singapore, Department of Chemical and Biomolecular Engineering, Singapore

Stavros Papadokonstantakis, Swiss Federal Institute of Technology (ETH) Zurich, Department of Chemistry and Applied Biosciences, Switzerland

Konrad Hungerbühler, Swiss Federal Institute of Technology (ETH) Zurich, Department of Chemistry and Applied Biosciences, Switzerland

Per Angelo, Maersk Oil, Copenhagen, Denmark

10.1002/14356007.o22_o11

1. Introduction

This article contains contributions reporting the state-of-the-art techniques and methods applied for abnormal events management and process safety practice in chemical and (increasingly) biochemical engineering industries. Methodological developments are particularly emphasized to better fit within the scope of the process systems engineering (PSE) keywords.

The five chapters constituting this article came from academia and industry, which managed to cover a broad range of topics and highlight the current perspectives and principles in research and industrial practice of abnormal event management (AEM) and process safety.

Chapter 2 focuses on monitoring and managing safety during online process operation hence reporting methodologies for monitoring, detecting and diagnosing abnormal events during process operation.

Chapter 3 takes a step back and focuses on the importance of giving considerations to process safety at early stage of process development. To this end, various safety metrics along side health and environmental criteria are considered when screening for suitable process flowsheets.

Chapter 4 provides the state-of-the-art of hazard identification techniques (e.g., FMEA, HAZOP, etc) and risk assessment techniques (e.g., fault tree analysis, consequence analysis, etc.) and methodologies such as layers of protection in the field. As part of risk assessment methodologies, inherently safer process design concept (following the principle "what you don't have, don't leak") has also been emphasized.

Chapter 5 the risk management at the logistic side of the chemical industries and the prevailing methodologies used for minimizing the risk in supply chain of chemical industry is covered.

In Chapter 6, industrial perspectives on management of safety and hazards where the risk management theories are put to test in practice are described. This section covers a brief history of chemical accidents that led to the development of modern safety management systems (SMS) and also provides experiences with different elements of SMS implementation.

Although considerable development has happened in the process safety record of chemical and biochemical industries, yet accidents do occur from time to time. Given the accident in Gulf of Mexico (USA) in 2010 at BP operated Macando well and its huge social, economic, and environmental consequences, indeed the significance of process safety cannot be emphasized more. Surely this event has already been shaking fundamentally the process safety practice in industry (especially offshore oil and gas industries), which will have ramifications on how process safety is managed and audited across the board. This and other accidents have reminded always the importance of taking and treating safety with due care at all levels from academic research (e.g., safety at early stage process development) to the top of the executive management (e.g., self-commitment and provision of adequate resources for safety) in chemical industries.

Ensuring safety of chemical processes and products are the minimum requirement from a societal, political, and environmental point of view. Hence, development of systematic methods and techniques that support hazard identification and risk management for process safety shall remain a highly relevant and important research goal for the PSE community.

2. Abnormal Event Management–Process Monitoring and Fault Diagnosis

2.1. Introduction

Abnormal event management (AEM) involves the timely detection of an abnormal event, diagnosing its causal origins and then taking appropriate supervisory control decisions and actions to bring the process back to a normal, safe-operating state. An abnormal event could arise from the departure of an observed variable from the acceptable range. Process abnormality such as high temperature in reactor or low product quality could occur due to a failed coolant pump or a controller. Such a failure could lead to an abnormal event. Other causes include process parameter changes (catalyst poisoning and heat-exchanger fouling), large disturbances (in concentration of feed stream or ambient temperature), actuator problems (sticking valve), and sensor problems. A key challenge in the process industry today is the development and deployment of intelligent systems that assist human operators during abnormal events particularly in the isolation of faults.

AEM is a safety issue, and safety has been a top priority for companies in the chemical process industries. Figure 1 shows how AEM relates to safety—successful detection and identification of process faults at an early stage can increase the success rate of fault recovery during operations and prevent accidents and unnecessary shutdowns [1]. The plant operators work within a simple framework that has three main areas: normal, abnormal, and emergency operations (see Fig. 1). The plants typically have well-defined normal operating procedures; very basic abnormal operating procedure, such as for shut down; and very good emergency planning and response procedures. AEM relates to the procedures for "Return to Normal" and operating under abnormal conditions, its diagnosis and recovery which can be difficult because of process dynamics and the need for speedy response.

2.2. Process Monitoring and Diagnosis Framework

Abnormalities which occur in the process have to be detected, diagnosed, and corrected. Decision support systems should provide the plant operator and maintenance personal information about the current status of the process and recommend appropriate remedial actions to mitigate the undesired effects of abnormal process behavior. Timely detection of managing faults result in reduced process downtime, improved operations safety, and higher business efficiency. Process monitoring and diagnosis methods seek to automate this to a large extent.

Each monitoring and diagnosis method uses a priori process behavior knowledge in the form of a model (developed off-line) and on-line process measurements to compute residuals whose exceeding a predefined threshold

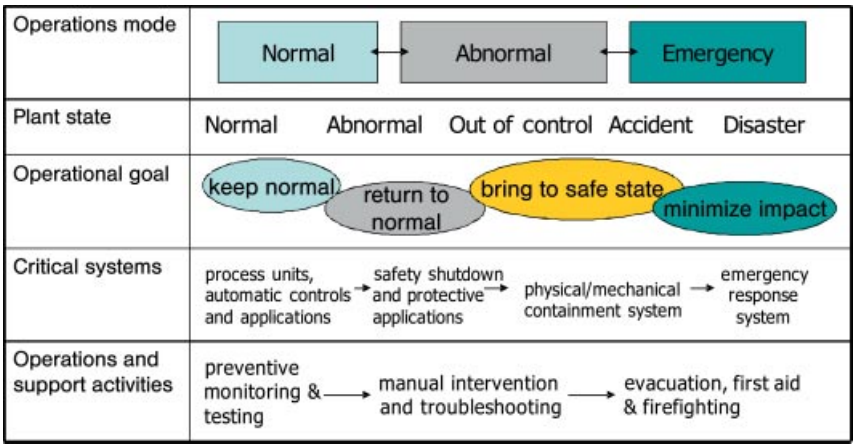

Figure 1. Anatomy of a disaster from an operation perspective [1]

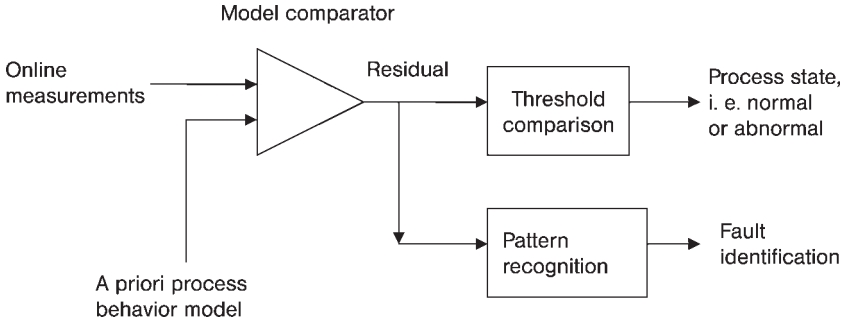

Figure 2. General framework of process monitoring and diagnosis system

indicates abnormality. Figure 2 depicts the general principle behind process monitoring. Features in the on-line measurements and the residuals could also indicate the possible root cause of the abnormality.

Desirable Characteristics of a Fault Diagnostic System. The performance of a process monitoring method is determined by the number of false positive and false negative results it gives and the number of samples required for developing the behavior model. In order to compare various process monitoring and diagnosis methods, it is first useful to identify a set of desirable characteristics that such a system should possess. Then the different methods may be evaluated against such a common set of requirements or standards. The following are a set of desirable characteristics one would like the diagnostic system to possess [2].

Early Detection and Diagnosis. Early and accurate diagnosis is an important and highly desirable attribute. However, quick diagnosis and tolerable performance during normal operation are two conflicting goals [3]. A system that is designed to detect a failure (particularly abrupt changes) quickly will be sensitive to noise and can lead to frequent false alarms during normal operation, which can be disruptive.

Isolability refers to the ability of the diagnostic system to discriminate between different failures. The diagnostic system should be able to assign correct fault class to an abnormal process state with high recognition rate (accuracy).

Robustness. The diagnostic system needs to be robust to various noise and uncertainties. Its performance should degrade gracefully instead of failing totally and abruptly. Also plants operate in various states (operating modes) and undergo transition between them. Although some transients could arise due to abnormal events, others are part of normal process operations. The diagnostic system should be cognizant of the various normal modes of operations.

Adaptability. Processes change and evolve due to changes in external inputs or structural changes due to retrofitting and so on. The operating conditions change not only due to disturbances, but also due to other conditions like changes in production quantities, quality of raw material, etc. In order to be useful and practical, the diagnostic system, particularly the process behavior model, should be easy to maintain.

2.3. Fault Detection and Diagnosis Methods

Numerous computer-aided methods have been developed for process monitoring and diagnosis over the years. Since all process monitoring and diagnosis methods require a priori knowledge about the process and its behaviors, one scheme of classifying them is based on the source of such knowledge. The knowledge may be from fundamental understanding of the process using first principles, also referred to as deep, causal or fundamental knowledge-based methods. This is developed usually from understanding about the physicochemical behaviors like mass, energy, momentum conservative equations, reaction kinetics, thermodynamics, etc. Alternately, the a priori domain knowledge may be gathered from past experience with the process, referred to as shallow, compiled, evidential, or process

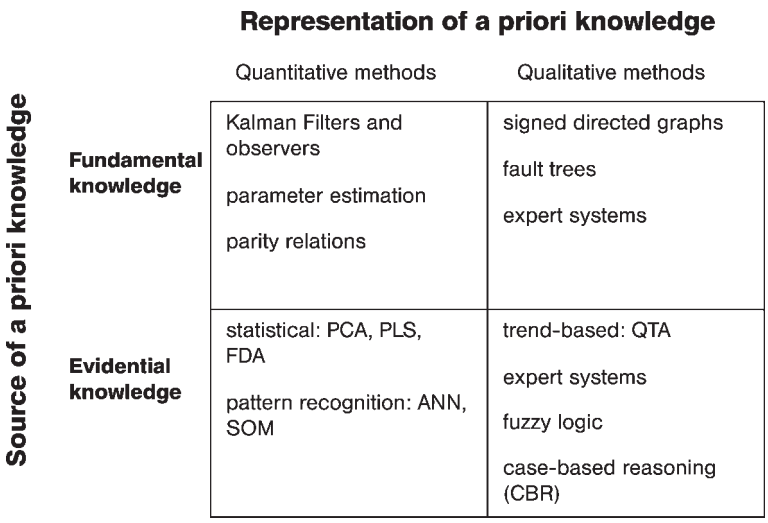

Figure 3. Classification of process monitoring and diagnosis methods

history-based knowledge. Thus monitoring and diagnosis methods could be broadly classified into two major categories:

1. Fundamental knowledge-based methods
2. Evidential knowledge or process history-based methods

These two forms of knowledge about a process could be represented in either qualitative or quantitative schemes (see Fig. 3). Quantitative methods use mathematical equations, while qualitative methods solely rely on discrete qualitative elements (high, low, increasing, decreasing, etc) to represent behavior. Thus, all process monitoring and diagnosis methods can be classified based on the source of knowledge and its representation into any of the four grids shown in Figure 3. Some of these methods in each of the four categories are described in detail next.

2.3.1. Fundamental Knowledge-Based Quantitative Methods

Quantitative methods are also referred to as analytical methods in literature [2, 4]. Based on the measured variables analytical methods generate residuals using detailed dynamic mathematical models. The residuals are the outcomes of consistency checks between the plant observations and the behavior as encoded in the mathematical model. The residual will be nonzero due to faults, disturbances, noise, and/or modeling errors. In the preferred situation, residuals or their transformations will be relatively large when faults are present, and small in the presence of other variations. In this case the presence of faults can be detected by defining appropriate thresholds. In any case, an analytical method will arrive at a diagnostic decision based on the values of the residuals.

The three main ways to generate residuals are parameter estimation, observers or Kalman filters, and parity relations [5]. For parameter estimation, the residuals are the difference between the nominal parameters and the estimated model parameters. Deviations in the model parameters serve as the basis for detecting and diagnosing faults.

The Kalman filter or observer-based method reconstructs the outputs of the system from the measurements or a subset of the measurements. The difference between the measured outputs and the estimated outputs is used as the vector of residuals. Unlike open-loop observers that use only inputs, closed-loop observers/filters, such as Kalman filters, make use of both the input as well as output measurements. Closed-loop filters are therefore inherently more stable and do not require accurate knowledge of the process initial conditions. The Kalman filter is one of the

most widely used tools for state and parameter estimation in stochastic systems and is based on minimizing the least square error criterion of the estimates. In [6], a multilinear model-based fault detection scheme was proposed based on decomposition of operation of a nonlinear process into multiple locally linear regimes. Kalman filters were used for state estimation and residuals generation in each regime. Analysis of residuals using thresholds, faults maps, and logic-charts enabled on-line detection and isolation of faults.

Parity relation checks the consistency of the mathematical equations of the system with the measurements.

2.3.2. Fundamental Knowledge-Based Qualitative Methods

In qualitative model equations input–output relationships are typically expressed in terms of qualitative functions. The process monitoring and diagnosis methods based on qualitative models can be obtained through causal modeling of the system, a detailed description of the system or through fault–symptom analysis. Causal analysis techniques are based on the cause–effect modeling of fault–symptom relationships. Qualitative relationships in these causal models can be obtained from the first principles. Causal analysis techniques like signed directed graphs [7], fault tree, qualitative physics are based on fundamental process knowledge and use a qualitative framework for diagnosing faults.

A signed directed graph (SDG) is a qualitative model that incorporates the cause-and-effect of deviations from normal operations. In directed graph, nodes represent process variable values and directed arcs represent the relationship between them. The directed arcs have a positive (+) or negative (−) sign attached to them and also lead from the "cause" nodes to the "effect" nodes. Sometimes nodes also depict process variables or events (system fault, component failure, or subsystem failures). A node takes the value of 0 when its measured variable is within its normal range, a value of "+" when its measured variable is larger than a high threshold, or "−" when it's measured variable is smaller than the low threshold. Arcs take values of "+" and "−" representing whether the cause and effect change in the same direction or the opposite direction, respectively.

Figure 4A shows a gravity flow-tank system. An SDG of this system is shown in Figure 4B. The following faults are considered in this example: (i) Leak in stream 0, (ii) Leak in stream 1, (iii) Leak in tank, and (iv) Valve stuck in closed position. In this example, when "leak in stream 1" occurs, h will decrease. Therefore, a "−" sign is assigned to the arc which connects these two nodes. To determine root cause during fault the deviations are propagated from the effect nodes to cause nodes via consistent arcs until one or more root nodes are identified. In the above gravity flow-tank example, consider the case where the observed symptoms are that the liquid level h is increasing, while the output flow rate F_{out} is decreasing. These symptoms indicate that the nodes F_{in}, h, and F_{out} take the values of 0, "+", and "−", respectively. Based on SDG shown in Figure 4B, the fault can be determined uniquely as "valve is stuck in the closed position".

2.3.3. Evidential Knowledge-Based Quantitative Methods

In evidential knowledge-based methods the availability of large amount of historical process data replaces fundamental knowledge in determining process behavior. There are different ways in which this data can be transformed and presented as a priori knowledge to a diagnostic system. This extraction process can be either quantitative or qualitative in nature.

The quantitative process history-based methods essentially formulate the diagnostic problem-solving as a pattern recognition problem. The goal of pattern recognition is the classification of data points to in general, predetermined classes. Statistical methods use knowledge of a priori class distributions to perform classification. Neural networks on the other hand assume a functional form for the decision rule.

2.3.3.1. Principal Component Analysis

Principal component analysis (PCA) is the most widely used statistics-based data-driven technique for monitoring industrial systems [8, 9]. It is a dimensionality reduction technique that is

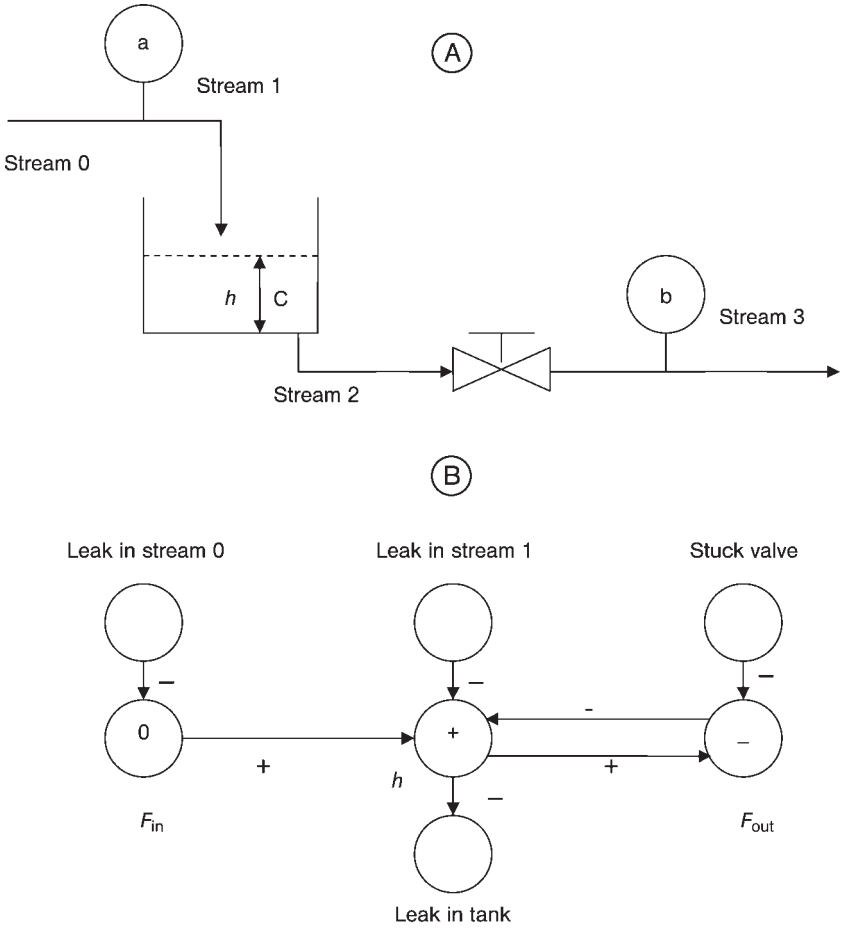

Figure 4. A SDG of a gravity flow-tank system
A) Gravity flow-tank system with three measured variables: a) Input flow rate F_{in}; b) Output flow rate F_{out}; c) Height of liquid level in tank h
B) A signed directed graph for the gravity-tank system with symptoms h is increasing, while F_{out} is decreasing

capable of treating high-dimensional, noisy, and correlated data by projecting it onto a lower dimensional subspace that explains the most pertaining features of the system.

Let $\boldsymbol{X} \in \Re^{nXm}$ represent the data matrix. Where n designates the number of samples (observations) and m denotes the number of variables $(n > m)$. The matrix $\boldsymbol{X}$ is decomposed in terms of a new set of independent variables, the principal components, which are linear combinations of original variables and are defined to be orthogonal to each other. PCA relies on eigenvalue decomposition of the covariance of $\boldsymbol{X}$ in order to reconstruct it as:

$$\boldsymbol{X} = t_1 p_1^T + t_2 p_2^T + \ldots\ldots + t_a p_a^T + \boldsymbol{E} = \boldsymbol{T}\boldsymbol{P}^T + \boldsymbol{E}, \quad a \leq m \tag{1}$$

$$E = \boldsymbol{X} - \boldsymbol{T}\boldsymbol{P}^T = \sum t_i p_i \tag{2}$$

where, $\boldsymbol{T} = [t_1, t_2, \ldots, t_a]; \boldsymbol{T} \in \Re^{nXa}$ is the matrix of principal component scores, which extracts the correlative information of the samples. $\boldsymbol{P} = [p_1, p_2, \ldots, p_a]; \boldsymbol{P} \in \Re^{mXa}$. is the matrix of principal component eigenvectors or principal component loadings, which abstracts the correlative information of the original variables and $\boldsymbol{E} \in \Re^{n \times m}$ is the residual matrix, which is the difference between original data and the reconstruction. Due to the high degree of correlation among the variables, one often finds that the anterior a principal component can explain the main variation in the original data

variables. Therefore, PCA projects the training data matrix $\boldsymbol{X} \in \Re^{nXm}$ into lower dimensional PC score matrix $\boldsymbol{T}$ as

$$\boldsymbol{T} = \boldsymbol{XP};\ \boldsymbol{T} \in \Re^{nXa} \tag{3}$$

Hence, the dimensionality is greatly reduced which allows the dominant process variability to be visualized with a single plot. Fault detection using PCA or its variants is usually performed by monitoring the squared prediction error (SPE) and/or HOTELLING'S T^2 statistic. The former measures the variation of an on-line sample x_i from the PCA model, i.e., lack-of-fit while the latter measures the variation of the sample within the PCA model. The process is considered normal if $SPE_i < Q_\alpha$, where Q_α denotes the upper control limit for confidence level $1-\alpha$ based on a standard normal distribution [10]. An upper control limit $\boldsymbol{T}^2_\alpha$ similar to Q_α can also be derived for the $\boldsymbol{T}^2$ statistic. A fault is flagged when the 95% or 99% confidence limits of $\boldsymbol{T}^2$ statistic and/or SPE value is violated. For fault diagnosis, a fault reconstruction scheme is used wherein separate models are developed for each fault class. The PCA model that shows an in-control status during abnormal operations is considered to flag the right class of fault.

One of the shortcomings of PCA-based methods is that they suffer from an inability to explain their results, i.e., they cannot identify the root cause or describe the fault propagation pathways. PCA-based methods just monitor and detect the abnormal behavior. Recently, PCA-based method has been extended with additional statistical analysis such as LAMDA clustering [11] or case-based reasoning [12] to perform the root cause analysis of the abnormal behavior in sequential batch reactor (SBR) processes.

2.3.3.2. Artificial Neural Network

The artificial neural network (ANN) is a nonlinear mapping between input and output variables consisting of a set of interconnected neurons arranged in layers. Neural networks have been used successfully for classification and nonlinear function approximation problems. Neural network-based process monitoring and diagnosis method uses the relationship between data patterns and fault classes without modeling the internal process states or structure explicitly. The three-layer feedforward ANN shown in Figure 5 is the most popular. The network consists of three components: an input layer (Fig. 5a), a hidden layer (Fig. 5b), and an output layer (Fig. 5c). Each layer contains *neurons* (also called nodes). Each neuron in the hidden layer is connected to all input layer neurons and output layer neurons. No connection is allowed

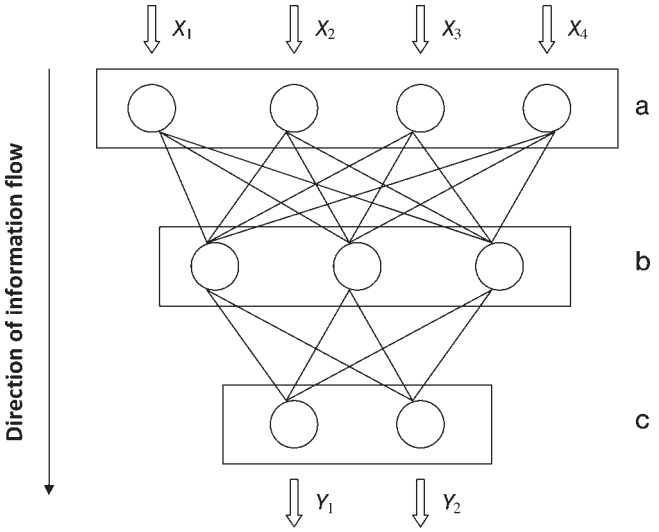

Figure 5. A three-layered feedforward artificial neural network (ANN)
a) Input layer: Each neuron gets one input, on-line measurement; b) Hidden layer: Connects input and output layer; c) Output layer: Identifier of current process state

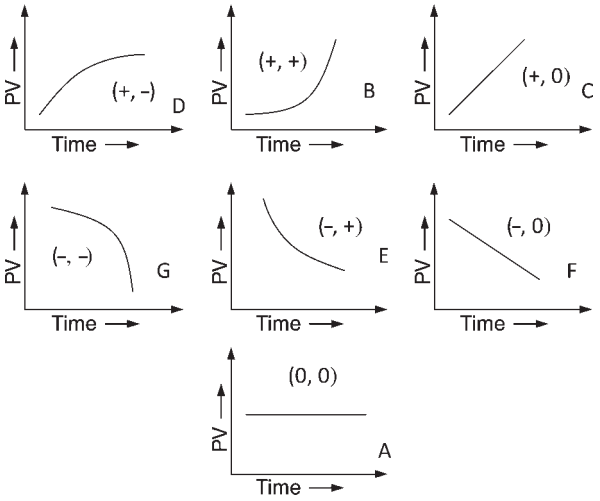

Figure 6. Primitives for trend analysis [13]

within its own layer and the information flow is in one direction only.

One common way to use a neural network for fault diagnosis is to assign the input neurons to on-line measurements and the output neurons to the process state indicators (i.e., normal as well as known process faults). Therefore, the number of input neurons becomes equal to the number of process variables to be monitored while the number of output neurons is equal to the number of different classes in the training data, i.e., both normal and known fault classes. The output pattern corresponding to the normal conditions and the faults can be denoted by a vector. For example, the vector [1 0 0 . . .] is the output pattern for normal condition, the vector [0 1 0 0 . . .] is the output pattern for fault class 1, and so on. During on-line fault detection and diagnosis phase, the measurement is projected on to the trained neural network to map the on-line sample to the process states (normal and known process faults). Among the various output nodes, the one with the largest value is considered to indicate the process state if its value is close to 1.

2.3.4. Evidential Knowledge-Based Qualitative Methods

In qualitative process history-based methods the feature extraction is solely in terms of qualitative elements, such as: high, low, medium, normal or increasing, decreasing, constant, or $+1$, 0, -1, etc. Qualitative trend analysis is an example of qualitative process history-based method. The variation of a process variable (PV) with time is called the trend of that variable. Trend analysis involves hierarchical representation of variable trends, extraction of trends, and their comparison (estimation of similarity) to infer the state of the process. Figure 6 shows the shapes of the seven primitives differentiated based on their first and second derivatives. A trend is represented as a sequence (combination) of these seven primitives. The trend of a process variable is demarcated into simple shapes called *atoms*. The trend analysis approach is based on monitoring the ordered set of atoms that abstract the trend of each process variable. During each state, the variables in the process exhibit a typical trend. So, the normal operation of the plant would have a specific trend signature for different variables. When a fault occurs, process variables vary from their nominal values and ranges, and exhibit trends that are characteristics of the fault. Hence, different faults can be mapped to their characteristic trend signatures.

2.3.5. Expert Systems

An expert system is a computer program that mimics the cognitive behavior of a human expert in a particular domain. In general, plant

operators and engineers have vast experience in operating the process and they gather comprehensive knowledge over the time from their experience regarding the nuances when disturbances/faults occur in the underlying process. The knowledge can be abstracted in terms of a set of logical if-then-else rules. The rule-based expert system consists of a knowledge base, essentially a large set of if-then-else rules and an inference engine which searches through the knowledge base to derive conclusions from given facts.

Some examples of the if-then rules are: For the gravity-tank system shown in Figure 4A:

- If the liquid level h in the tank increases and the output flow rate F_{out} decreases, then the fault is most likely due to "valve stuck in closed position"
- If the liquid level h in the tank decreases and the output flow rate F_{out} decreases, then the fault is most likely due to "leak in tank"

In the expert systems the knowledge representation scheme is largely qualitative. The knowledge base of an expert system may contain evidential knowledge based on heuristics, causal knowledge based on first principles, or combination of the two. Therefore, depending on its knowledge base an expert system could be an evidential knowledge-based qualitative method or could be a fundamental knowledge-based qualitative method or a hybrid.

2.3.6. Hybrid Methods

Each process monitoring and diagnosis method has its own advantages and weaknesses. Thus, a method that works well under one circumstance might not work well under another when different features of the underlying process come to the fore. It is clearly difficult to design a perfect method that efficiently monitors a large-scale, complex industrial process in all likely scenarios. Hence, there is a strong motivation for developing systems that rely on collaboration between multiple methods so as to bring together their strengths and overcome their individual shortcomings. Some of these methods can complement one another resulting in better diagnostic systems. Integrating these complementary features is one way to develop hybrid methods that could overcome the limitations of individual solution strategies. For example, a combined neural network and expert system tool was developed and its effectiveness was demonstrated for transformer fault diagnosis [14]. Other methods with other interactions are reported by [15–17].

2.4. Future Directions

Nowadays, sensors and equipments are becoming "smart" in the sense that they are capable of performing self-diagnostics and determining abnormalities within themselves. Traditional monitoring and diagnosis approaches are monolithic and do not use such information. Further, they largely rely on a single form of knowledge representation. Incorporating the smarts of the sensors and intelligently combining multiple diagnostic perspectives is an important direction for future research. Some further aspects which should be explored are discussed below:

Fusion Methods. A multi-perspective diagnostic system which includes modern sensor diagnostics would need some form of evidence aggregation to arrive at a cohesive conclusion. Decision fusion is expected to play a key part in achieving this so that correct decisions are amplified and incorrect ones cancelled out. Although fusion strategies have been attempted in different fields before, there is not much work being done on using them for process monitoring and diagnosis. Fusion methods can be broadly classified as utility-based and evidence-based methods. Utility-based methods do not utilize any prior knowledge about the performance of monitoring and diagnosis method or evidence from its previous predictions, but are based on some aggregating techniques which evaluate the combined utility functions generated from each method. Examples include simple average, voting techniques, and their variants. In contrast, evidence-based methods use a priori information from previous performance of each method to combine the decisions. Several evidence-based fusion schemes such as Bayesian probability theory, Dempster–Shafer evidence theory, and decision templates could be explored for improving diagnostic performance.

Dempster–Shafer theory could be particularly useful in dealing with scenarios where faults are mutually nonexclusive where traditional Bayesian approach fails.

Cooperative/Peer Learning. Research could focus on establishing learning schemes among monitoring and diagnosis methods which would make each method more intelligent with time. Cooperation strategies can use the decisions and the results of one for guiding other methods especially in their training and model upkeep stages. Generally, the decision vector is shared between monitoring methods; however, other types of information can also be transmitted between methods so that peer-learning can be accomplished from sharing intermediate results as well.

Ensemble learning techniques such as bagging, boosting, and stacking have been applied to generate multiple pattern classifiers. These techniques are based on resampling of training data and theoretically more tractable. These methods can be easily adopted to generate and train multiple process monitoring and diagnosis methods.

Finally, artificial immune systems (AIS) are a new artificial intelligence methodology that is attracting much attention for monitoring engineered systems. In an AIS, principles and processes of the natural immune system are abstracted and applied in pattern recognition and a variety of other applications in the field of science and engineering. One popular immune-inspired principle is negative selection through which self-tolerant *T*-cells are generated, thus allowing the immune system to discriminate self-proteins from foreign (nonself) ones. This principle leads to negative selection algorithm (NSA) wherein a collection of spherical detectors is generated in the complementary (nonself) space and used to classify new (unseen) data as self or nonself. AIS is now used extensively in situations where only large amount of self (normal) samples are available but abnormal samples are either unavailable or very rare as is often the case in process monitoring and fault diagnosis. Samples from a given state (such as normal or known fault) are considered as self. These samples can be used to develop a description of the nonself space in the form of a collection of spherical detectors. This representation is in contrast to traditional statistical and pattern recognition algorithms that store descriptions of the space occupied by the normal samples.

3. Risk Assessment and Inherent Safety in Process Design → Plant and Process Safety, 6. Risk Analysis

3.1. Introduction

An abnormal event in a chemical process industry is a disturbance or a series of disturbances in the process plant which causes the plant conditions to deviate from normal operation. These disturbances may be minimal or sometimes catastrophic, causing production losses, off-specification products and in some cases endangering human life. The failure of equipment within the plant or human errors are the primary sources of these abnormal events which have resulted in a number of accidents, with the Flixborough disaster, United Kingdom (1974), Bhopal gas tragedy, India (1984), Toulouse fertilizer factory explosions, France (2001) and Petrobras offshore platform accident, Brazil (2001) being some of the major ones. In addition, the risks posed by chemical industries to life, property, and environment have significantly increased in recent years as a result of increased population density near industrial complexes, larger size of operation, higher complexity, and use of extreme operating conditions.

The modern approach to chemical process safety is to apply risk management systems theory to the process. This includes identification of the hazards posed by the process, and a continual effort to analyze the risks, and to reduce or control them to the lowest practical levels, while balancing other business objectives. A *hazard* (center for chemical process safety, CCPS, 2009) in a chemical process industry is any source of potential damage or harm to plant equipment which may in turn have adverse effects on humans within or outside the process plant. *Risk* is the chance or probability that a defined consequence (harm) may occur. *Safety*, as defined by the CCPS, 2009, is tolerable risk in comparison to the benefit of the activity. To ensure safety, every chemical plant

is subjected to a process hazard analysis (PHA) in which the various hazards within a process are identified, relevant mitigation steps taken, and the overall process risk reduced.

3.2. Process Hazard Analysis (PHA)

PHA is a set of organized and systematic assessments of the potential hazards associated with an industrial process. A PHA provides information intended to assist managers and employees in making decisions for improving safety and reducing the consequences of unwanted or unplanned releases of hazardous materials. A PHA is directed toward analyzing potential causes and consequences of fires, explosions, releases of toxic or flammable chemicals, and it focuses on equipment, instrumentation, utilities, human actions, and external factors that might impact the process. The first step in PHA is hazard identification, for which there are a variety of methods [18–20]:

- *What/if analysis:* An early method of hazard identification is to review the design by asking a series of questions beginning with "What If?". The method is a team exercise and typically makes use of predetermined questions, but otherwise tends not to be highly structured.
- *Failure mode and effect criticality analysis (FMECA):* Another method of hazard identification is the FMECA. It involves the analysis of the failure modes of an entity, their causes, effects, and associated criticality of the failure.
- *Hazard and operability studies (HAZOP):* A method widely used by the process industries for the identification of hazards at, or close to, the engineering line diagram (ELD) stage is the HAZOP study → Plant and Process Safety, 6. Risk Analysis. It is a team exercise, which involves examining the design intent in the light of guidewords. The purpose of the HAZOP study is to uncover causes and consequences of a facility's response to deviations from design intent or from normal operation, i.e., to reveal if the plant has sufficient control and safety features to ensure, that it can cope with expected deviations normally encountered during operation including start-up, shutdown, and maintenance. Most HAZOP methods require considerable time and resources, lasting anywhere between 1–8 weeks and costing around $20 000 per week [21]. The traditional HAZOP methodology was developed for plants in which control systems were predominantly based on analogue controllers. In recent years, process engineers have increasingly chosen to use programmable logic controllers (PLCs), distributed control systems (DCSs) and computers for process control. While these systems provide flexibility and close control of the process, they introduce an additional mode of failure to the plant. The process engineer who is going to start up and operate the plant no longer writes the instructions himself but explains what he wants to an applications engineer who writes a specification which is given to a programmer (though the same person can be an applications engineer and programmer). The process and applications engineers usually speak different languages and may not understand each other's problems; they may belong to different departments and work in different parts of the building; these factors can introduce errors. A useful summary of different schemes for CHAZOP is provided by [22]. Consideration of three aspects in CHAZOP are suggested by [23]: computer system/environment, input/output (I/O) signals and complex control schemes. The questions relating to the computer system/environment are essentially larger scale, almost overview-type issues that are better addressed within a preliminary design review of the control scheme. Additional information on CHAZOP can be found in [24, 25].
- *Event tree and fault tree analysis:* Event trees and fault trees are logic diagrams used to represent, respectively, the effects of an event and the contributory causes of an event.
- *Consequence analysis and modeling:* Examination of different scenarios of plant disturbance and loss of containment is a central activity in hazard identification. The scenarios may relate to the events before release or to events involved in escalation after release. Hazard identification, therefore, includes methods of developing and structuring scenarios.

- *Human error analysis:* It is well established that human actions play a large role in accidents. Human error analysis is used to take this aspect into account. As a hazard identification technique, human error analysis is qualitative, although a similar term is also sometimes used to describe a quantitative method.

Once the hazards in a plant have been identified through one or more of the above hazard identification techniques, the safety risks associated with them are estimated.

3.2.1. Risk Assessment

Quantitative risk assessment (QRA), also known as probabilistic risk assessment (PRA) or probabilistic safety assessment (PSA), usually deals with major hazards that could cause a high death toll. A full-risk assessment involves the estimation of the frequency and consequences of a range of hazard scenarios and of individual and societal risk. In QRA, risk is characterized by two quantities: 1) the magnitude (severity) of the possible adverse consequence and 2) the likelihood (probability) of occurrence of each consequence. Consequences are expressed numerically (e.g., the number of people potentially hurt or killed) and their likelihoods of occurrence are expressed as probabilities or frequencies (i.e., the number of occurrences or the probability of occurrence per unit time). The total risk is the expected loss: the sum of the products of the consequences multiplied by their probabilities. Once the hazards in the process have been identified the following steps are followed in the quantitative risk assessment:

1. Identify vulnerable targets
2. Develop hazardous and escalation scenarios
3. Identify mitigating features
4. Estimate consequences
5. Estimate frequencies
6. Compute and present risk. Compare with risk criteria
7. Either accept system or modify system to reduce risk or abandon design

Although the results of a QRA are typically expressed in terms of deaths or of casualties, appropriately defined, there are generally other consequences that need to be considered including [18]:

- The write-off of the plant
- The impact on the surrounding area
- The anxiety factor
- Consequential detriment
- The 'What if?' factor

3.2.2. Hazard Indices

The safety of a process may be determined by a number of indices, which are in essence consequence model-based hazard estimation methods. These are the Dow fire and explosion index (F&EI), Dow chemical exposure index, mond index (ICI), instantaneous fractional annual loss index and mortality index.

Dow Fire and Explosion Index. The original purpose of the F&EI was to serve as a guide for the selection of fire protection methods. This was the first practiced safety index, and is still the most widely used one. Most other indices are expansions of this basic index. Once a process unit has been identified for evaluation the F&EI is calculated as follows. First a material factor (MF) that is a characteristic of the most energetic material in the process is obtained. Then two penalty factors (F1 and F2), one for general process hazards (GPHs) and one for special process hazards (SPHs), respectively, are determined, and the process unit hazards factor (PUHF) (F3), which is the product of these, is calculated. The product of the MF and PUHF is the F&EI.

3.3. Design Strategies for Process Risk Management

Process risk management is the term given to collective efforts to manage process risks through a wide variety of strategies, techniques, procedures, policies and systems that can reduce the hazard of a process, the probability of an accident, or both. The risks in a process could be managed by having multiple safeguards deployed in a plant, typically like the *layers of protection*. This concept was introduced in the mid-1990s and is now widely adopted and

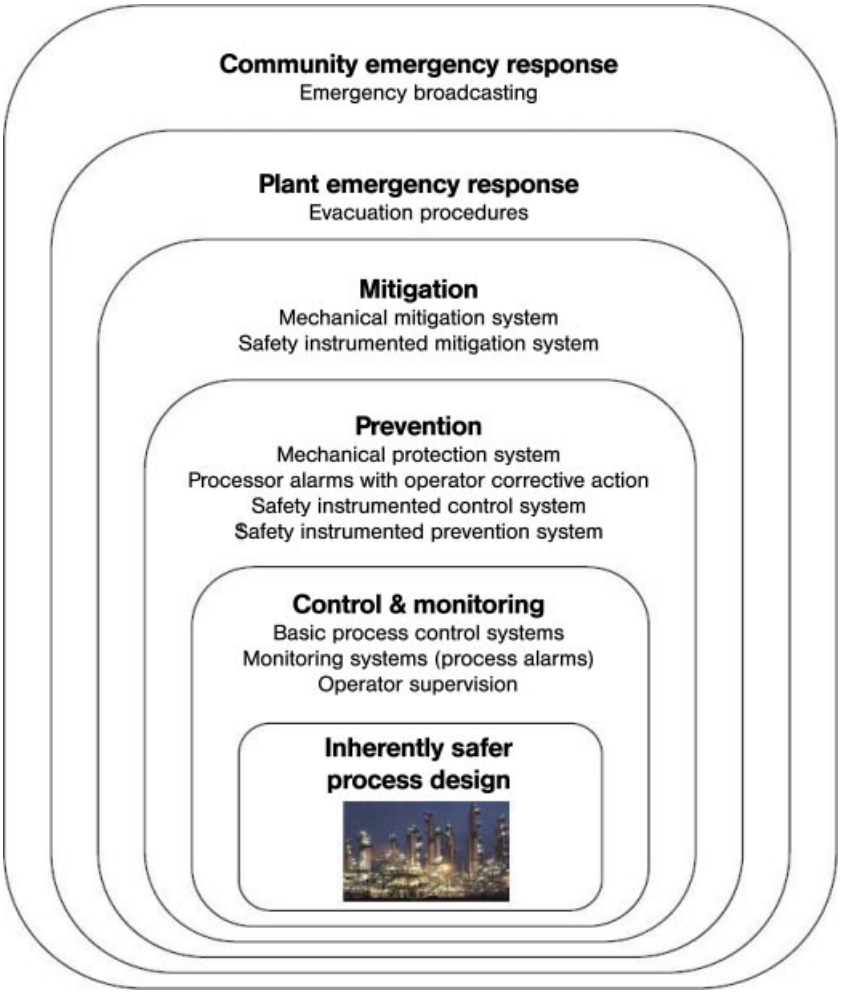

Figure 7. Layers of protection in a chemical plant–each layer adds a magnitude of protection over previous layer [18]

included in safety codes such as independent safety assessor (ISA) 84.01. The basic idea is illustrated in Figure 7 which is self-explanatory. The innermost layer is the process design, followed by basic control systems (BPCS), critical alarms, automatic actions such as the safety interlock systems (SIS); physical protection, dikes, and emergency responses, both plant and community-wide. Each safety layer is independent, specific, dependable and auditable, providing an order of magnitude protection over the previous layer.

Other methods of classifying the risk mitigation strategies are as follows:

- Inherent–Eliminating the hazard by using materials and process conditions that are non-hazardous.
- Passive–Minimizing the hazard through process and equipment design features that reduce either the frequency or consequence of the hazard without the active functioning of any device.
- Active–Using controls, alarms, safety instrumented systems and mitigation systems to detect and respond to process deviations from normal operation.
- Procedural–Using policies, operating procedures, training, administrative checks,

emergency response and other management approaches to prevent accidents.

These four strategies could be used in the various layers in the layers of protection that are present in a chemical plant.

3.3.1. Economics of Risk Management

Process Risk Management is concerned with the avoidance both of personal injury and of economic loss. In both spheres there is an economic balance to be struck. Some costs arise through failure to take proper loss prevention measures; others are incurred through uninformed and unnecessarily expensive measures. In today's environment, many loss prevention measures that were optional in the past are now mandated by government regulation.

The result of not taking adequate measures gives rise to losses and costs such as: accidents, damage, plant design delays, plant commissioning delays, plant downtime, restricted output, etc. But taken safety measures have their own costs as well which add on to total project costs. These costs incurred due to enhanced safety effort may be due to management effort, research effort, design effort, process route, operational constraints, plant siting, plant layout and construction, process instrumentation (trip systems), fire protection, and emergency planning. Often a balance is required between increased safety efforts and benefits to the company. Figure 8 shows typical trends of cost and functional attributes for the various design categories. The initial capital is maximum for inherently safer design, is lesser for passive and active and the least for procedural design solutions. The operating costs, however, is minimum if an inherently safer design is chosen and is higher for other solutions. The plants complexity is minimum and reliability maximum with the selection of an inherently safer design solution. Ideally, a safety measure which provides acceptable risks while at the same time not hindering business activity must be chosen.

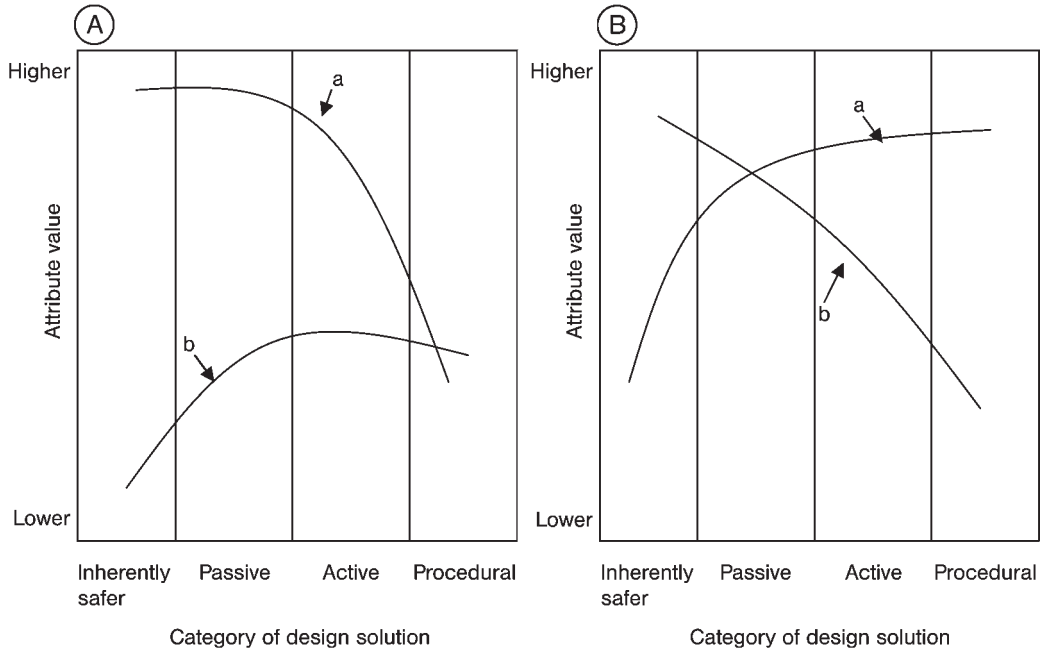

Figure 8. Comparison of cost and functional attributes for design categories (typical trends)
A) Cost for design categories;
a) Initial capital; b) Operating costs;
B) Functional attributes;
a) Complexity; b) Reliability

3.3.2. Inherently Safer Process Design

Inherent safety (IS) is an approach to chemical process safety that focuses on eliminating or reducing the hazards associated with a set of conditions. The process design which includes inherent safety principles is referred to as an inherently safer process design. An inherently safer process should not, however, be considered as "absolutely safe". Implementing inherent safety concepts will move a process in the direction of reduced risk; however, it will not remove all the risks.

Inherent safety is in fact a modern term for an age-old concept: to eliminate hazards rather than accepting and managing them. Since prehistoric times humans have used these principles for their survival, like for example, building villages near a river on high ground rather than managing flood risk by building dikes and walls. But this concept started to be embraced by the chemical process industries only after an article titled "*What you don't have, can't leak*" on lessons from the Flixborough disaster (1974). The name "inherent safety" comes from an extension of this article published as a book [26].

Design Strategies. The search for inherently safer process options begins early and continues throughout the process life cycle. The greatest potential opportunities for impacting process safety occur early in process design and development. Early in development, there is a great deal of freedom in the selection of chemistry, solvents, raw materials, process intermediates, unit operations, plant location and process parameters. Approaches to the design of inherently safer processes and plants have been grouped into four major strategies by [27, 28]:

Minimize means to reduce the quantity of material or energy contained in a manufacturing process or plant. Often, the inventory of hazardous materials on-site is driven by operational and business considerations, like number of transportation containers used, railroad dispatching schedules, trucking schedules, etc. Sometimes inventories are determined by on-site purchasing considerations, such as incoming and outgoing shipments related to prices. Careful coordination with shippers and carriers is required to minimize inventory. The reader is referred to CCPS [29] for examples of process minimization.

Substitute means to replace a hazardous material or process with an alternative that reduces or eliminates the hazard. Examples include substitution in reaction chemistry, solvent usage, materials of construction, heat-transfer media, insulation and shipping containers. For instance, in the *Reppe process* for manufacturing acrylic esters an alcohol reacts with acetylene and carbon monoxide, in the presence of a nickel carbonyl catalyst having both acute and long-term toxicity. The alternative propylene oxidation process uses less hazardous materials to manufacture acrylic acid followed by esterification with the appropriate alcohol [30] to make the corresponding ester. An EPA report [31] contains an extensive review of inherently safer process chemistry options that have been discussed in the literature. This report includes chemistry options that have been investigated in the laboratory, as well as some that have advanced to pilot-plant and even production scale.

Moderate, also called attenuation, means using materials under less hazardous conditions. Moderation of conditions can be accomplished by strategies that are either physical (i.e., lower temperatures, dilution) or chemical (i.e., development of a reaction chemistry which operates at less severe conditions). Dilution reduces the hazards associated with the storage and use of low boiling hazardous materials in two ways: By reducing the storage pressure; by reducing the initial atmospheric concentration if a release occurs. Some materials can be handled in a dilute form to reduce the risk of handling and storage, like being stored in an aqueous form rather than in anhydrous form. Many hazardous materials, such as ammonia and chlorine, can be stored at or below their atmospheric boiling points with refrigeration. A series of case studies that evaluate the benefits of refrigerated storage for six materials–ammonia, butadiene, chlorine, ethylene oxide, propylene oxide and vinyl chloride is provided by [32]. Operating under less severe conditions, as close to ambient temperature and pressure as possible, increases the inherent safety of a chemical process.

Simplify means to eliminate unnecessary complexity, thereby reducing the opportunities

for error and wrong operation. Some suggestions on use of simple technologies in lieu of high or more recent technologies are offered in [26]:

- Fire protection systems should be as simple as possible. For example, new technology for detecting fires by using sophisticated detectors to measure smoke, heat, ultraviolet radiation from fires, is often less reliable than a simple detector that allows the fire to burn through a filament and break an electrical circuit.
- Flare systems should be kept as simple as possible and not be equipped with other appurtenances, such as flame arrestors, water seals, filters, etc. These components are prone to plugging and reduce flare capacity.

While the above four strategies are the main ones, others such as *limitation of effects*, *avoid incorrect assembly* and *making status clear* are also available in literature.

3.4. How to Perform IS Evaluation?

A methodology for performing inherent safety review at various stages of the process life cycle is described in the following sections. Drawing from the principles described by [26], this approach would guide the designer in identifying alternatives that preempt the identified hazards during the various stages of process design.

3.4.1. Product Specification Stage

The objective of inherent safety analysis during the product specification stage is to identify safety issues associated with the product and to challenge the design team to consider alternatives to the product, means of transportation, and handling systems. The inherent hazards related to storage, handling, transportation and incompatibility of materials are identified based on physical, toxicological, chemical, and reactive properties such as flammability limits, median lethal dose (LD_{50}), stability, reactivity, etc. The physical and chemical properties of the material such as its vapor density, boiling point, freezing point, and particle size are considered when evaluating the impact of the hazard. The vapor density of a material determines its atmospheric dispersion characteristics in the atmosphere. The design alternatives at this stage, in general, relate to the use of safer materials or modification of hazardous material into a less hazardous form. The burgeoning field of green chemistry offers general guidelines for designing safer chemicals and modifying hazardous chemicals while preserving the efficacy of function through masking or replacement of functional groups, identifying alternate functional groups, and minimizing bioavailability by changing the shape, size, structure, dilution, and altering properties. However, specific alternatives such as the use of bleaching powder instead of chlorine, the use of toluene instead of benzene as a solvent, handling of solids in the form of pellets or granules, processing with solution, or wetting instead of fine powders can be derived with the help of heuristics [33, 34].

3.4.2. Route Selection Stage

The process route selection is the heart of the design process and determines the inherent hazards associated with the reactor in addition to the number of downstream separation units and the need for recycle. The objective during this stage is to (1) identify the hazards and processing problems that are associated with reactions and chemicals involved in the process route and (2) rank the available process routes. During this stage, raw materials, byproducts, intermediates, catalysts, and the reaction conditions are selected. To evaluate the inherently safe nature of a route, reactions can be classified into intended and unintended reactions. Main reactions and side reactions fall under the category of intended reactions and are defined by the process chemistry. Main reactions are those in which raw materials or intermediates are transformed to products or intermediates. In contrast, side reactions result in the formation of byproducts from raw materials, products, or intermediates. Unintended reactions occur during abnormal process conditions such as utility failure, disproportionate reactants or missing ingredients, contact between incompatible materials, etc. Decomposition due to thermal runaway is an example of an unintended reaction.

Reaction hazards can be identified by focusing on intended and unintended reactions occurring in the process. Hazardous reactions are characterized by high temperature or pressure, large heat release, unstable materials, or chemicals that are sensitive to air, water, rust, or oil. Material properties have to be evaluated to ensure that chemicals that are benign at ambient conditions do not become hazardous at process conditions. This will result in the definition of a safe operating regime for the reaction. Inherent safety analysis during this stage can be performed at two levels, preliminary and detailed, based on the amount of information available.

Process routes available can be ranked using inherent safety indices. It must be simple to use, applicable to both continuous and batch processes at all design stages, and capable of ranking individual hazards with apparent fundamental causes. The index should also promote simplified processes without penalizing novel technology. Finally, a normally acceptable range, which aids comparison with other processes, should be available. The existing indices, prototype index for inherent safety (PIIS) and inherent safety index (ISI), satisfy most of these criteria. PIIS focuses on the main reactions and considers factors such as temperature, pressure, and reaction yield, heat of reaction, flammability, toxicity, explosiveness, and inventory. It can, therefore, be used only during the chemistry selection stage. ISI accounts for side reactions, corrosion, inventory (both inside and outside battery limits), type of equipment, and process structure in addition to the factors considered by PIIS (see Chap. 4).

3.4.3. Flowsheet Development Stage

After a process route has been selected, the flowsheet for the process has to be developed. The major difference between alternate flowsheets is the type and number of unit operations, reactors, number of recycles, and processing aids involved. Opportunities to substitute or eliminate hazardous materials and to alter process conditions are limited at this stage because these are largely determined by process chemistry. Despite the lower impact of design changes on inherent safety, opportunities for influencing the inherent safety of the process still exist. The choice of unit operations, the nature and amount of material handled, operating conditions, and operational philosophy determines the risk associated with equipments. The effectiveness of inherent safety analysis largely depends on the knowledge available to identify hazards, develop alternative designs and to rank process flowsheets. Inherent safety analysis during the flowsheet development stage is envisioned to identify opportunities to eliminate or reduce the need for equipments and instruments, reduce the size of process equipments, identify unit operations that do not require processing aids and involve milder operating conditions, eliminate or reduce the use of hazardous utilities, and minimize the chance of fugitive emissions and accidental leaks. Using available information, the analysis must identify hazards under normal operating conditions as well as under foreseeable abnormal conditions, recommend design rectifications, and rank alternative flowsheets.

Inherent Safety Index for Flowsheets. The flowsheet index (FI) is a measure of the hazardous nature of the process as a whole and is composed of the chemical index (CI) and the process index (PI). The FI is the sum of CI and PI. The CI is based on the maximum index of parameters related to chemicals involved in the whole process. The CI is calculated by the summation of the following sub-indices: heat of main reaction sub-index, heat of side reaction sub-index, flammability sub-index, toxicity sub-index, explosiveness sub-index, reactivity sub-index, chemical interaction sub-index, and corrosion sub-index. The PI is calculated by taking into account the operating conditions, inventory and nature of the equipment. Further details on calculation of these indices are given in [33, 34].

After performing IS evaluation, the particular design option under consideration is either chosen for production, provided risk criteria are satisfied, otherwise the design is iterated until acceptable risks are achieved. While it is possible to minimize risk by making the process inherently safer, it must always be kept in mind that the risk is not completely eliminated.

3.5. Inherent Safety Practices in Industry

The quantity of literature on company inherent safety policies and procedures has continued to increase during the last years, indicating that awareness is improving. IS reviews are now mandated by regulation for high-risk facilities in some US states. A number of companies have published descriptions of their inherent safety review practices:

- Bayer [35] uses a procedure based on hazard analysis, focusing on the application of inherent safety principles to reduce or eliminate hazards.
- Dow [36] uses the Dow fire and explosion index and the Dow Chemical exposure index as measures of inherent safety [37, 38].

Companies like Exxon Chemical, BASF, Rohm and Haas, ICI, Berger, and DuPont have inherently safer design practices incorporated into their overall process system management program.

The general view of safety personnel in industries is that they realize the importance and advantages of IS design and would like to use it if the procedures were simple and did not require too much time since they already have several mandated safety protocols to follow and file periodic reports on them with the regulatory bodies.

4. Hazards Identification in Early Stages of Process Design

4.1. Introduction

The importance of the concepts involved in process risk analysis is best illustrated by the fact that they are included directly or indirectly in at least half of the "Twelve Principles of Green Chemistry" [39], i.e., prevention, atom economy, less hazardous chemical syntheses, use of safer solvents and auxiliaries, reduction of derivatives, real-time analysis for pollution prevention, and inherently safer chemistry for accidental prevention. However, it is also true that the implementation of these principles is not always straightforward since trade-offs may exist between hazard or risk minimization and other green chemistry principles and financial objectives (e.g., optimal use of resources and raw materials).

Moreover, quantifying the effect of the application of these principles through robust, yet not too complicated or data-intensive assessment methods remains a challenging research field. The motivation to look for such simple tools and methodologies arises from the wish to integrate hazard identification and analysis methods into decision-making during early process development phases. These early stages of process design are characterized by more degrees of freedom for implementing changes, but also by more scarce process data for detailed methods to be applied. For instance, this can be a limiting factor for the applicability of methods like HAZOP, fault tree analysis (FTA) FMEA (see Chap. 3) as far as hazard identification and analysis methods are concerned. The application of these detailed methodologies stipulates specialized teams consisting of process and control systems engineers, production operators, maintenance teams, and advisors for plant safety policies (e.g., perhaps in cooperation with insurance companies). The composition of these teams already implies that the respective methods are suitable for later stages of process design where significant process experience has been gained, or even for retrofitting processes already in operation, and not for preliminary design stages, e.g., during the selection of the chemical route and the design of the required downstream processes (Fig. 9).

Starting from information about process chemistry (i.e.; synthesis routes for a given product (P), using raw material (R) and chemical auxiliaries like catalysts (Cat) and solvents (Solv) data are gathered about substance properties and process conditions either from existing databases or lab experiments. Safety, health; and environmental (SHE) hazards assessment procedures can be then implemented either before or after the development and analysis of process flowsheets.

For the problem of hazard identification during these early stages of process design, various index-based methodologies have been proposed, mainly during the 1990s and 2000s [40–45]. A qualitative and quantitative comparison of such methods can be found in the

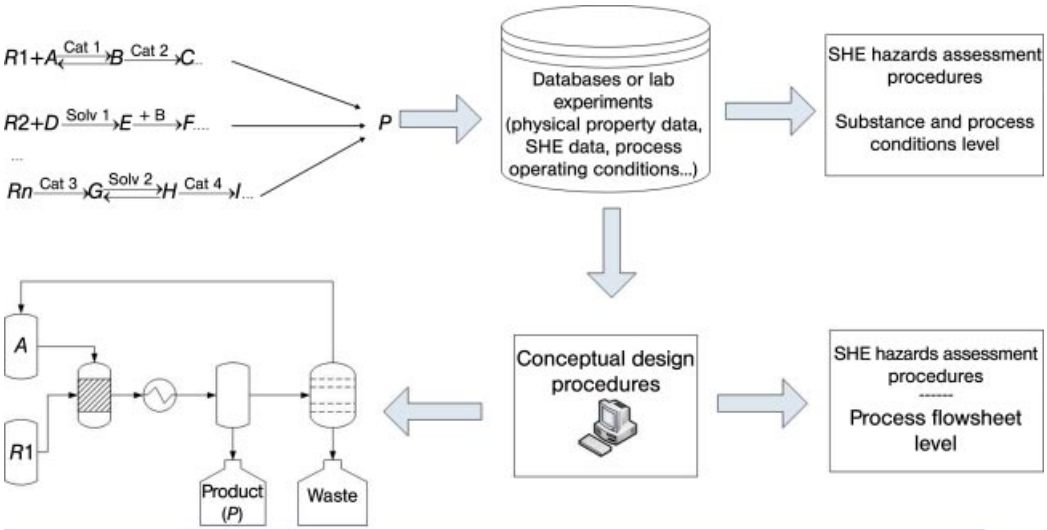

Figure 9. Early stages of process design and hazard assessment

work of [46], where one of the main conclusions was that there is no unique merit of one method over the other in any of the SHE aspects taken into account. Among the compared methods in this study is the one of [47], which has been later modified and integrated into a general multi-objective screening framework for early stages of process design by [48, 49].

4.2. An index-based approach for SHE hazard identification

4.2.1. Overview

An important feature of SHE hazard identification approaches is the kind of data required for the assessment. Generally, two categories of input data can be distinguished:

- Substance related data: including for instance physical properties (e.g., boiling point), substance classification methods (e.g., EC risk phrases and hazard symbols), toxicity data (e.g., immediately dangerous to life and health concentrations (IDLH)), degradation data (e.g., half-life values and biodegradability data after 28 days (OECD 28d)), accumulation data (e.g., octanol–water partition coefficients) and various emission limits.
- Process related data: about operating conditions (e.g., temperature and pressure) and performance (e.g., yield of reaction)

The required data imply that the SHE assessment practitioner should have a complete list of the chemical substances involved in the process and at least an estimation of the main process operating conditions, which could be the result of preliminary modeling or lab experiments. The required substance data of all categories can be obtained from available databases, e.g., Design Institute for Physical Properties (DIPPR-801, 2007) [50], National Institute of Standards and Technology (NIST, 2010) [51], International Uniform Chemical Information Database (IUCLID-5, 2008) [52] (), Canadian Centre for Occupational Health and Safety (CHEMpendium, 2006) material safety datasheets (MSDS) [53], using property estimation methods and quantitative structure-activity relationship (QSAR) techniques or even by conducting lab experiments to fill in data gaps.

The data collection part is a common feature of all the index-based methods and the required effort depends heavily on the SHE effects considered by each method. On the other hand, the process modeling at these early stages of process design involves mainly the construction of simple linear mass balances taking into account reaction yields and separation efficiencies based

on empirical correlations and shortcut models. Rigorous modeling is avoided at these early design stages because of lack of necessary process information (e.g., reaction kinetics) and often overwhelming amount of alternatives that have to be checked regarding available technologies.

4.2.2. Methodology

As mentioned above, the data collection procedure is directed by the settings of each SHE hazard identification method with regard to the effects taken into account. The framework for SHE hazard assessment proposed by [47] attempts to estimate the relevant hazards by using a set of characteristic *dangerous properties* for each SHE category. More specifically, it is assumed that the dangerous properties contributing to the safety hazard are:

- Mobility
- Fire/explosion
- Reaction/decomposition
- Acute toxicity

Those, contributing to the health hazard are:

- Irritation
- Chronic toxicity

Water- and air-mediated effects which must be considered for the environmental hazard like:

- Solid waste
- Degradation
- Accumulation

The calculations proposed by the authors comprise the following three steps:

1. Step 1: A set of m aspects ($A_{i,j,m}$) is used to define an index-value ($IV_{i,j}$) for each dangerous property i and substance j. For this purpose, a "scaling and prioritization" methodology has been proposed, which is exemplified for the dangerous property "accumulation ($i = Acc$)" belonging to environmental hazards by the following calculations:

$$AI_{Acc,j,1} = f_1(\log(BCF)) = \text{linear mapping } [2,4]\rightarrow[0,1] \quad (4)$$

$$AI_{Acc,j,2} = f_2(\log(K_{ow})) \text{ linear mapping}[3,5]\rightarrow[0,1] \quad (5)$$

$$AI_{Acc,j,3} = f_3(Rcodes) = \begin{cases} 1, & \text{if R-code} = 48, 53, 58 \\ 0.5, & \text{if R-code} = 33 \\ 0, & \text{if R-code} = \text{other value} \end{cases} \quad (6)$$

$$AI_{Acc,j,4} = f_4(qualit.inp) = \begin{cases} 1, & \text{if qualit.inp} = \text{high} \\ 0.75, & \text{if qualit.inp} = \text{probable} \\ 0.5, & \text{if qualit.inp} = \text{possible} \\ 0.25, & \text{if qualit.inp} = \text{low} \\ 0, & \text{if qualit.inp} = \text{no} \end{cases} \quad (7)$$

$$AI_{Acc,j,5} = f_5(no\ data) = 1 \quad (8)$$

where $AI_{Acc,j,m}$ denotes an index value for aspect $A_{Acc,j,m}$, BCF is the bioconcentration factor, K_{ow} is the octanol–water partitioning coefficient, *R-codes* refer to EC risk phrases, *qualit.inp* stands for qualitative information about possible accumulation and *no data* refers to the situation that no data for the above categories are available for substance j. These calculations are typically mentioned as scaling of relevant parameters for SHE index calculation, while prioritization refers to the fact that the final index value for the dangerous property "accumulation" ($IV_{Acc,j}$) is calculated according to $AI_{Acc,j,1}$, if BCF data are available for substance j, otherwise according to $AI_{Acc,j,2}$, if K_{ow} data are available for substance j, and so on.
2. Step 2: After all $IV_{i,j}$ values are calculated, they are translated with empirical equations into some kind of physical unit per unit mass, which is then multiplied by the substance mass (m_j) to result in a "so-called" potential of danger ($PoD_{i,j}$). For instance, for the previously calculated $IV_{Acc,j}$:

$$PoD_{Acc,j} = m_j \cdot 10^{(2 \cdot IV_{Acc,j})} \quad [\text{kg}] \quad (9)$$

The reasoning behind this transformation of $IV_{i,j}$ to $PoD_{i,j}$ depends on the dangerous property, i.e., different types of formulas with different constants are proposed for each dangerous property. For example, in the case of "accumulation", as it is clear from the previously described "scaling and prioritization" scheme, the BCF or K_{ow} parameters are used to provide a physical meaning to this scale, i.e., a value of BCF equal to

100 or lower indicates low potential for a substance to accumulate in the food chain, and therefore in a steady-state scenario the *relative factor* for potential to accumulate in the food chain is set to 1 kg per kg of substance released to the environment, while at the same time $IV_{Acc,j} = 0$. Then the cases of $BCF = 1000$ and $BCF = 10000$, which correspond to *relative factor* values of 10 and 100, respectively, were used to define the middle ($IV_{Acc,j} = 0.5$) and maximum ($IV_{Acc,j} = 1$) values of the index scale, and therefore also defined the formula for $PoD_{Acc,j}$. Examples of the physical meaning of $PoD_{i,j}$ for other dangerous properties are: amount of air or water polluted to emission limit (m^3/mg) for air- or water-mediated effects, respectively, belonging to environmental hazard and probable energy potential for reaction with oxygen (kJ/kg) for fire/explosion dangerous property belonging to safety hazard. A detailed definition of the physical meaning and the formulas involved in the calculation of the $PoD_{i,j}$ can be found in [47]. These $PoD_{i,j}$ values can be then aggregated for all substances resulting in a total potential of danger of the process for each of the SHE dangerous properties.

3. Step 3: The last step of the calculation procedure is to reduce the $PoD_{i,j}$ values to acceptable levels by applying technology factors ($T_{i,j,k}$) representing the effect of technology k for a specific substance j into considered dangerous property i. The overall costs associated with the technologies to be applied can be considered as an unbiased aggregation procedure for estimating the overall effect of SHE hazards for a given process. Despite the advantage of such a procedure that avoids subjective weighting and aggregation of index values representing different hazards, the additional scaling parameters needed to transform the index value into a relevant physical unit and the not always trivial task to define the appropriate technology factors and associated costs increase the complexity of calculations and the amount of required data. As already mentioned, this can be a serious limitation for the applicability of this approach, since usually in the earliest stages of process design a fast screening is desirable making simpler approaches more attractive.

Therefore, [48] have modified the method described above by substituting the last two steps with a weighting and aggregation scheme for the SHE hazards based on the number of dangerous properties taken into account for their calculation, so that at the end each dangerous property has equal importance. In this way an overall SHE hazard score is calculated, which can be used to rank process alternatives according to the following formulation:

$$\begin{aligned} S^r &= \sum_c w_c \cdot \bar{H}_c^r \\ H_E^r &= \sum_{i,(i\in E)} \sum_j (z \cdot \max_F (m_j^F) \cdot IV_{i,j}) + \sum_{i,(i\in E)} \sum_{j_o} (m_{j_o}^{\text{out}} \cdot IV_{i,j}) \\ H_H^r &= \sum_{i,(i\in H)} \max_F (\sum_j IV_{i,j}) \end{aligned} \tag{10}$$

$$\begin{aligned} H_S^r &= \sum_{i,(i\in S)} \max_F (\sum_j m_j^F \cdot IV_{i,j}) \\ \bar{H}_c^r &= \frac{H_c^r}{\max_r (H_c^r)} \end{aligned} \tag{11}$$

where S^r refers to the overall score of a process r for the production of a given chemical compound, $\bar{H}_c^r$ refers to the overall normalized hazard for category c (c = E, H, or S standing for environmental, health, and safety categories, respectively), m_j^F is the specific mass flow of substance j in flow F of the process, $m_{j_o}^{\text{out}}$ is the specific mass flow of substance j_o leaving the process (excluding the main product of the process), and z is a fraction of mass emitted to the environment in an accidental case.

According to the aforementioned formulation the material balances of the process are necessary in order to calculate the environmental and safety hazards, while health hazards are evaluated on the basis of an inventory-free scenario. The reasoning for this choice is that health hazards in this framework are meant to capture effects due to the normal operation of the plant and not due to an accidental case. Therefore, the relevant mass would be the dose a worker takes up during a specified period of time. This mass depends on unknown parameters during early phases of process design, like the equipment and the working conditions rather than the inventory. Moreover, some of the scales for the chronic toxicity refer to non-threshold effects, like for instance those of

carcinogens and allergens, a single molecule of which can theoretically be harmful. For this kind of compounds it is often just the presence and not the amount that is critical for safety measures to be taken in order to avoid harm to the personnel. However, it should be understood that this inventory-free formulation for the calculation of the health hazards is a proposition of the authors that heavily depends on which dangerous properties are taken into account (e.g., acute toxicity, for which mass balances should be clearly taken into account, is considered as a dangerous property only for the safety hazard in the original formulation of [47] as well as in those of [48, 49], while it could be argued that acute toxicity should be also considered for the health hazard) as well as on which effects are highlighted for the evaluation of these dangerous properties (e.g., effects of carcinogenicity, mutagenicity, etc.). If the practitioner judges that health hazards should be evaluated on the basis of material balances then the formula for the calculation of H_H^r will be similar to the one of H_S^r. Finally, the formulation presented above can be either applied once for the whole process or separately for each process step.

4.2.3. Application in Case Studies

A simplified version of the methodology of [47] has been used for the assessment of some of the most frequently used solvents in chemical industry. The dangerous properties for the categories SHE have been rearranged according to Figures 10–12.

In this simple case where different substances and not different process alternatives are compared the assessment can be performed by simple addition of the index values for each dangerous property, since mass-flow information is not relevant. Therefore, the maximum SHE score for any substance will be nine. As an example, the values for acetone are presented in Table 1.

In Figure 13, the SHE score results are presented for 11 selected solvents. An extensive evaluation of organic solvents has been performed by [54], including a two-dimensional analysis according to SHE scores and cumulative energy demand (CED) values. This type of analysis can provide a preliminary screening for decision-making during early stages of process design for solvents and other auxiliaries to be used in chemical synthesis.

More detailed examples where this SHE assessment framework has been applied for the selection of process alternatives have been reported by [48, 49], comparing six and seven different chemical synthesis routes in the case of methyl methacrylate (MMA) and 4-(2-methoxyethyl)phenol production, respectively.

4.3. Conclusions and Future Directions

Index-based approaches, like the SHE framework based on the work of [47], are popular in early stages of process design due to their

Figure 10. Dangerous properties and scaling approaches taken into account for an index-based hazard estimation in category "environment"
*: Category persistency estimates the persistency of substances in the water using aquatic half-life
**: Maximum index value is taken when there is more than one parameter at the same priority
WGK: Wassergefährdungsklasse (German water hazard class)
$L(E)C50_{aquatic}$: Aquatic lethal or effect concentration using *Daphnia magna*

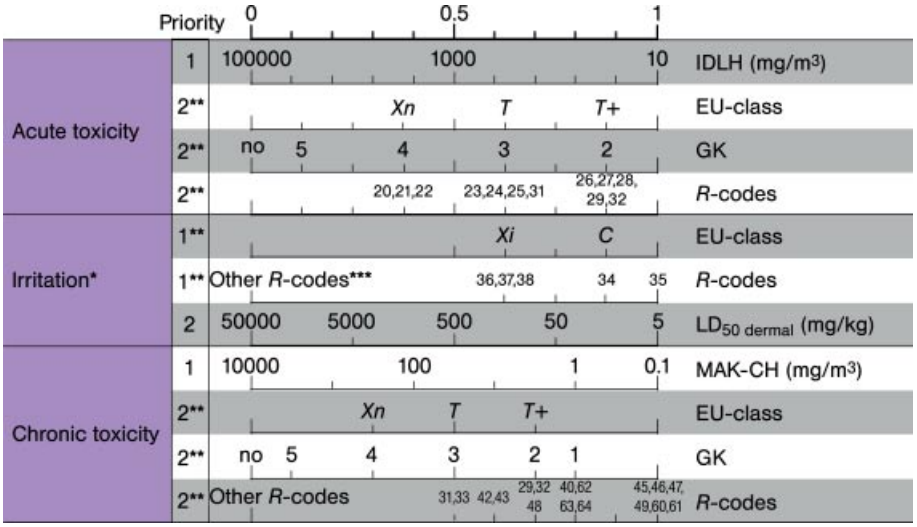

Figure 11. Dangerous properties and scaling approaches taken into account for an index-based hazard estimation in category "health"
*: Category irritation estimates the effect of eye or skin irritation
**: Maximum index value is taken when there is more than one parameter at the same priority
***: Used only when there is no LD_{50} value available
$LD_{50\,dermal}$: Lethal dose via dermal exposure using rat, mouse, rabbit
MAK: Maximale Arbeitsplatzkonzentration (workplace threshold value)
GK: Giftklasse (swiss poison class)

simplicity and the fact that lack of detailed information about the process set-up makes the implementation of more rigorous approaches meaningless. These simple index-based approaches can be used either for substance or for process assessment and they have been applied in various case studies presented in scientific literature. However, points of criticism regarding these approaches about the subjective nature of scaling and weighting schemes, the different coverage of SHE aspects by different frameworks, and the resolution of the overall scores of the proposed indices have also been reported [44, 55].

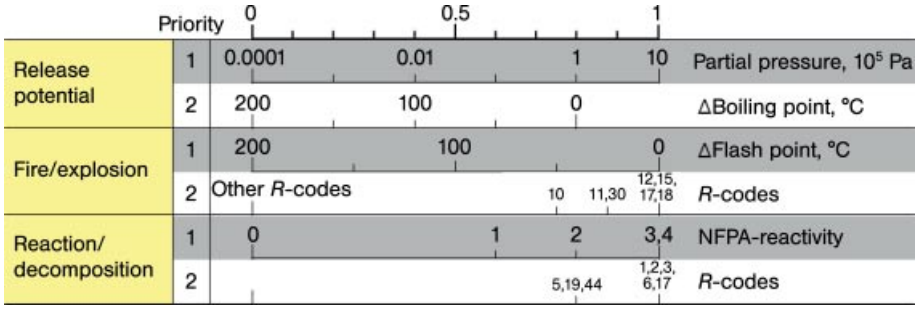

Figure 12. Dangerous properties and scaling approaches taken into account for an index-based hazard estimation in category "safety"
Partial pressure: Partial pressure of pure component at process temperatures (25°C)
ΔBoiling point: Temperature difference between standard boiling point and process temperature (25°C)
ΔFlash point: Temperature difference between flash point and process temperature (25°C)
IDLH: Immediately dangerous to life and health
GK: Giftklasse (swiss poison class)

Table 1. SHE hazard identification for acetone

Dangerous property	Index value	Considered aspect
Persistency	0.13	half life = 1.8 d
Air hazard	0.18	Ind.Val chronic tox.
Water hazard	0.00	LC50 = 7000 mg/L
Acute toxicity	0.30	IDLH = 6500 mg/m^3
Chronic toxicity	0.18	MAK = 1200 mg/m^3
Irritation	0.63	R-code = 36
Release potential	0.70	vapor pressure = 0.3 bar
Fire/explosion	1.00	flash point = −18°C
Reaction/decomposition	0.00	NFPA = 0
Overall score	**3.12**	

Recently, [55] have proposed a new approach for screening inherently benign chemical process routes based on PCA. Although this approach provides a promising alternative to subjective weighting and can be quite flexible regarding missing data and extensibility to new categories for process assessment, there are still a few issues to be resolved regarding its settings. Finally, more emphasis should be given to case studies that compare SHE hazard identification results obtained with simple methods in early stages of process design with more rigorous risk analysis and life-cycle analysis approaches applied in later design stages or even for process in operation. This can improve the robustness of the index-based methods used in early design stages by enriching them with features for presently unaccounted effects, lead to more uniform formulations of these methods, especially with regard to the environmental and the health hazards category and finally enhance the bridge of continuity between different stages in the process design and retrofitting life cycle.

5. Supply Chain Risk Management

5.1. Introduction

A supply chain (SC) is the system of organizations, people, activities, information, and resources involved in transforming raw materials into a finished product and delivering it to the end customer. Supply chain management (SCM) encompasses the planning and management of all activities involved in sourcing, procurement, conversion, and logistics to ensure smooth and efficient operations. SCM is an important element in enterprise management and a preferred way to reduce costs, improve performance, and manage the business amidst various uncertainties. In a global survey of companies in both discrete and process industries, the median SCM cost was reported to be 10% of revenue [56]; however, the cost in the process-based industries could be as high as 30% [57].

In recent years, due to increasing competition and tightening profit margins, companies have adopted a number of strategies to operate

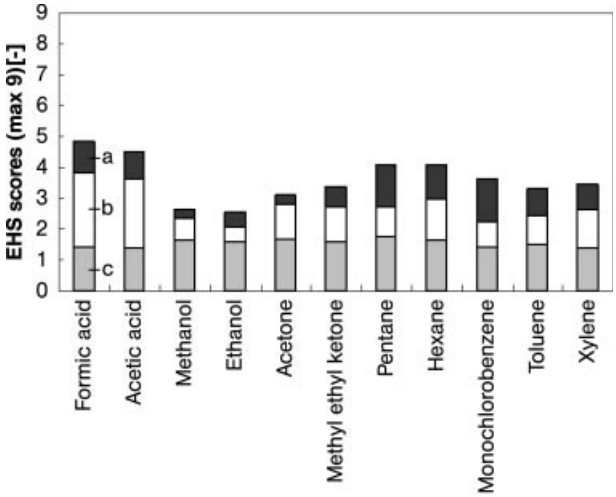

Figure 13. Results of the SHE hazard identification for 11 selected pure organic solvents
a) Environment; b) Health; c) Safety

more efficiently and reduce SC costs. In general, lower cost and higher efficiencies are accomplished through a globalized SC, higher capacity utilization, lower inventories, and just-in-time activities. However, there is a trade-off between efficiency and vulnerability. For instance, a survey by the Procurement Strategy Council reveals that 40% of large businesses rely on a single supplier [58]. Single sourcing decreases cost, but production continuity hinges upon the single supplier. Similarly, outsourcing leads to a more complex SC with more links exposed to a greater variety of disruptions. Sourcing from and distributing to other countries in other continents result in a globalized SC with exposure to new risks including political, cultural, and security risks. Just-in-time production and inventory reduction eliminate buffers which could be critical for business continuity when an unexpected event strikes. Hence, there is a clear need for enterprises to manage SC risk and reduce vulnerability so that they can respond and recover from disruptions promptly and efficiently. However, a recent survey reveals that only 42% of businesses have corporate standards and practices for overseeing the mitigation of SC risk [59].

Some recent events highlight the importance of SC risk management. Hurricane Katrina disrupted operations of Chevron Oronite's lube additive plant in Belle Chasse, Louisiana, USA, and tipped the marine lubricants industry into a crisis [60]. In 2000, there was a fire accident at a Philips' chip plant in Albuquerque, New Mexico, disrupting supply of radio frequency chips to Ericsson. Slow in managing the supply disruption and securing alternate supplies, Ericsson consequently lost significant market share and eventually left the mobile handset market [61]. These examples illustrate the domino effects inherent in SCs, which directly or indirectly translate into financial losses. It is reported that SC glitches negatively impacted stock prices by nearly 20% [62]. Another study reported that when chief financial officers (CFOs) and risk managers were asked what would cause the most disruption to the business, SC matters came second only to labor issues [58].

In the SC context, risk is defined as the potential negative impact that may arise from an adverse situation such as a disruption to SC operations, which will be discussed in Section 5.2. This definition of risk includes, but is not limited to, financial risk, where it primarily refers to investment loss. SC risk is one aspect of enterprise risk management, which can be broadly classified into market, credit, and operational risks [63]. SC risk falls under operational risk.

Disruption can be defined as any event or situation that causes deviation from normal or planned SC operations. Disruptions bring about adverse effects such as blockage of material and information flow, loss of ability to deliver the right quantity of the right product to the right place and at the right time, inability to meet quality requirements, loss of cost efficiency, under- or oversupply, and process shutdown. The complex interactions among the constituent entities make the SC inherently vulnerable to disruptions. A disruption in the production side of a supplier can have implications for the web of transportation and logistics services that move material from one plant to another, and eventually propagate to final products delivered to customers. Similarly, disruptions in the information and communication technologies that support the SC operation can simultaneously propagate across the entire network rapidly. Such disruptions occur not only from disasters but also due to "normal" dynamics, such as limited capacity in a fast-growing industry, demand changes due to new competitors, or sudden loss of customer confidence.

Risk management and *disruption management* are closely related. Risks are often measured in two dimensions—frequency and severity. Risk management aims to reduce either or both to acceptable levels by having proper safeguards and mitigating procedures which protect against the risks. Disruption management aims to minimize the impact of disruptions as they occur and restore the SC to normal operation as soon as possible. Having a reliable disruption management system will reduce the severity of the disruption when it strikes. Hence, disruption management can be viewed as a part of risk management.

SC risk can be an implicit consideration in SCM at the different levels: strategic, tactical, and operational. For example, at the strategic and tactical levels, demand uncertainties are taken into account in SC design [64] and

planning [65]. At the operational level, uncertainties in supply, demand, and other risks are considered in robust scheduling [66, 67]. On the other hand, SC risk management—the focus of this chapter—is explicitly aimed at dealing with and managing SC risk. It is a growing research area [68] and continues to attract more attention, especially in the operations research, SCM, and logistics communities [69].

5.2. Supply Chain Risk Classification

SC risk can be classified in several different ways. Based on the source, SC risk can be classified into [70]:

- *Environmental:* these are any uncertainties arising from the SC–environment interaction, e.g., accidents, socio-political actions, and natural disasters
- *Network:* these risks arise from interactions between organizations within the SC, e.g., outsourcing risks, distorted information, and lack of responsiveness of SC partners
- *Organizational:* these risk sources lie within the boundaries of the SC parties, e.g., labor strikes, machine failures, and IT-system disruptions

Based on the scale, SC risk can be classified into [71]:

- Single-stage (or company): affecting just a single organization or member of the SC
- Supply chain: affecting an entire SC
- Regional: affecting a whole region, not just the SC

Based on its measures, SC risk can be generally classified into:

- High-probability, low-severity: these risks arise from day-to-day variability and uncertainties
- Low-probability, high-severity: management of these risks has also been termed as business continuity or disaster management [72]. For example, these are disruptions caused by terrorist attacks, natural disasters, and other physical events such as industrial accidents and labor strikes [73] or chemical, biological, radiological, and cyber events [74]

Another classification is based on whether the risk is controllable (e.g., cost, design), partially controllable (e.g., fire accidents, employee accidents), or uncontrollable (e.g., earthquake, hurricane) [75].

5.3. Framework for Supply Chain Risk Management

The general framework for SC risk management is shown in Figure 14 and comprises the following steps:

1. Risk identification: The first step is to recognize uncertainties and risks faced by the SC.

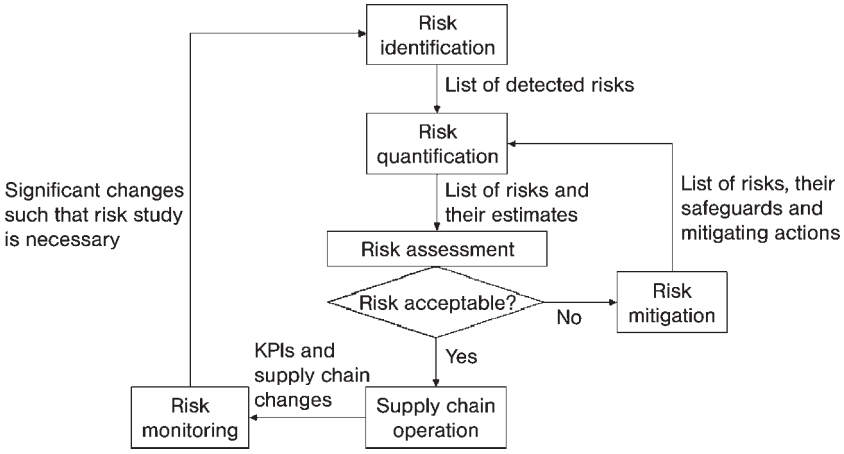

Figure 14. Supply chain risk management framework [76]

With globalization and increased outsourcing practices, the number of parties involved in the SC and the links connecting them have increased significantly. Hence, some risks may not be obvious and need to be identified in this step.

2. Risk quantification: Risk is usually quantified in financial terms and/or ranked according to some predefined criteria. Both risk dimensions (frequency and severity) need to be considered, taking into account the effects of safeguards and mitigating actions, if any.
3. Risk assessment: The risk management team decides whether the risk quantified in the previous step is acceptable based on experience, industry standards, benchmarks, or business targets. If not, additional mitigation actions or safeguards are required.
4. Risk mitigation: Mitigating actions and safeguards such as emergency procedures and redundancies have to be developed for the risks, based on both the SC model and inputs from the risk management team or relevant personnel. Two types of mitigating action can be differentiated–preventive and responsive. Once the risks have been deemed acceptable, SC operations proceed with the appropriate safeguards and mitigating actions in place.
5. Risk monitoring: The SC structure and operation do not remain stationary but changes regularly due to, for example, new suppliers, new regulations, new operating conditions, new products, etc. The risk management team should continually monitor the SC for new risks. The team might be required to start from step (1) to consider the new risks arising from these changes.

This framework is comparable to the risk management process in [70, 77].

5.4. Methods for Supply Chain Risk Management

5.4.1. Supply Chain Risk Identification

Two of the tools used for risk identification are *risk checklist* and *risk taxonomy* [78]. Risk checklist is a list of risks that were identified on previous projects, and often developed from managers' past in-house experience. The risk taxonomy provides a structure to organize the checklist of known enterprise risks into general classes. For example, enterprise risks are divided into internal processes and business environment. Each can be further classified, for instance, internal processes can be divided into financial, operational, and technological risks. Risk identification is performed by going through each item in the checklists and taxonomies and evaluating their applicability and implications in the situation at hand. The key strength of these methods is their flexibility, which makes them applicable to diverse situations. Two shortcomings arise from application of these methods to SC risk identification. First, they are rather ad-hoc and not systematic. Second, they are not tailored to SC and thus do not consider the complexity which arises from the interconnections among supply chain entities. Both of these may lead to "blind spots" and unidentified risks.

Risk identification could also be done through *stress testing*, i.e., identifying key suppliers, customers, plant capacity, distribution centers and shipping lanes, and asking "what if" questions to probe potential sources of risk and assess possible SC impacts [79]. Role-playing or "red-blue teaming" is a similar approach commonly used in the military [80]. In this approach, a red team generates a set of scenarios that they believe can lead to serious disruptions. The blue team attempts to provide mitigation or countermeasures against the scenarios. These methods are also flexible but suffer the same shortcomings of checklists and taxonomies, they are ad-hoc and not systematic.

A more structured risk identification approach is based on the HAZOP analysis method from chemical process risk management [76]. SC networks are in many ways similar to chemical plants. Drawing from this analogy, SC structure and operations can be represented using flow diagrams, equivalent to process flow diagrams (PFDs). Following the HAZOP method, SC risk identification can be performed by systematically generating deviations in different SC parameters, and identifying their possible causes, consequences, safeguards, and mitigating actions. The deviations are generated using a set of guidewords in combination with specific parameters from the flow diagrams.

Table 2. Sample guidewords and parameters for HAZOP

Guidewords	Meaning
No	none of the design intent is achieved
High	quantitative increase in a parameter
Low	quantitative decrease in a parameter
Early/late	the timing is different from the intention
Parameters	**Examples**
Material flow	raw material, side product, energy, utility, etc.
Information flow	order, quote, forecast, message, signal for action, etc.
Finance flow	cash, credit, share, receivables, pledge, etc.

Table 2 gives a nonexhaustive list of these guidewords and parameters. The guideword "low" can be combined with a flow to result in, for example, the deviation "low demand". Possible causes and consequences can be identified by tracing the flows in the flow diagrams. Safeguards are any items or procedures which help to protect against a particular deviation. It could protect against the deviation before it occurs, i.e., reducing the frequency, or help to recover quickly and minimize impact after it occurs, i.e., reducing the severity. An example of the former is safety stock, which protects against demand uncertainty; an example of the latter is insurance. Mitigating actions are additional items or procedures on top of any existing safeguards which are deemed necessary to manage the deviation. Table 3 shows a sample SC-HAZOP result for the deviation "no crude arrival" in a refinery SC.

SC-HAZOP has two notable advantages. It is systematic, because the deviations studied are generated using predefined guidewords and pertinent system parameters. It is also complete, because it is structured around a representation of the whole process in the form of flow diagrams. A possible disadvantage is that the SC-HAZOP life cycle requires considerable effort and resources, from developing the diagrams, analyzing deviations, identifying safeguards and mitigating actions, to documenting the results.

5.4.2. Supply Chain Risk Quantification

Risk quantification can be done through *risk estimation* and *risk mapping* [81, 82]. In this approach, the identified risks are rated on their probability and severity. Relevant personnel and domain experts are asked to fill a survey form (Fig. 15) to estimate the risks' probability and severity. The risks are then placed on a risk map, a two-dimensional map with one axis for probability and another for severity, according to its aggregate probability and consequences rating (Fig. 16). Based on the risk map, the decision maker can decide a priority of risks to focus on, e.g., those with higher probability and/or higher severity. This approach quantifies the risks in terms of probability and severity ratings and results in a qualitative ranking of the identified risks.

A more quantitative output for further risk quantification can be obtained through *simulation* [83, 84]. Simulation models of the SC are used to capture the behavior of the SC entities, their interactions, the resulting dynamics, and the various uncertainties. Given a set of input parameters, the SC operation can be simulated and the SC performance can be quantified as captured in a number of KPIs (key performance indicators) such as profit, total cost, and demand fulfillment level. Different risk scenarios and risk mitigating strategies can be simulated to quantify their benefits and costs.

5.4.3. Supply Chain Risk Mitigation

Six general risk mitigation strategies are:

Redundancy. Additional resources to guard against uncertainty, e.g., safety stock, backup equipment. Redundancy involves additional cost and thus, the trade-off between vulnerability and cost. Redundancy can be reduced without increasing vulnerability by improving risk mitigation capabilities through other strategies.

Table 3. Sample SC-HAZOP result

Deviation	Causes	Consequences	Safeguards	Mitigating actions
No crude arrival	jetty unavailability; shipper disruption; supplier stock-out	low stock, out-of-crude; operation disrupted; demand unfulfilled	safety stock; emergency suppliers	more reliable shipper; frequent check with supplier/logistics; rescheduling

Probability						Severity					
very low				very high		very low				very high	
□	□	□	□	□	supplier failure	□	□	□	□	□	
□	□	□	□	□	supplier quality problems	□	□	□	□	□	
□	□	□	□	□	machine breakdowns	□	□	□	□	□	
□	□	□	□	□	transportation failure	□	□	□	□	□	
□	□	□	□	□	accident (e.g., fire)	□	□	□	□	□	
□	□	□	□	□	terrorist attack	□	□	□	□	□	
□	□	□	□	□	increasing raw material prices	□	□	□	□	□	

Figure 15. Sample survey form for risk estimation

Risk Sharing. Risk is shared among different members of the SC through contractual requirements, e.g., buy-back contract and revenue sharing contract. A similar strategy is *risk transfer*, usually through insurance.

Visibility. Uncertainties in production, transportation, and other variables could propagate through the SC leading to a lack of confidence in its overall operation. This can be managed by improving visibility and control [85]. The key to improved visibility is shared information among supply chain members which translates to less "just-in-case" safety stock, shortened lead-time, and reduced cost. Visibility also significantly minimizes the bullwhip effect, i.e., the amplification of order fluctuations as one moves upstream in the SC. Control of SC operations is essential as information is useful only if necessary actions can be taken accordingly, for example, if a flexible production line can efficiently handle order changes once the information arrives.

Flexibility. Companies can reduce redundancy without increasing vulnerability by having inherently flexible SC designs that are demand-responsive. Reducing the number of parts and product variants allows aggregate forecasting, which is more accurate and creates inherent flexibility–inventory can be deployed to serve multiple products and markets. Other measures to build flexibility include interchangeability, postponement, and supplier and customer relations management [86].

Agility. The ability to thrive in a continuously changing, unpredictable business environment. This can be achieved, for example, by working with highly responsive suppliers. Agility is a key for inventory reduction, as it allows the enterprise to adapt to market

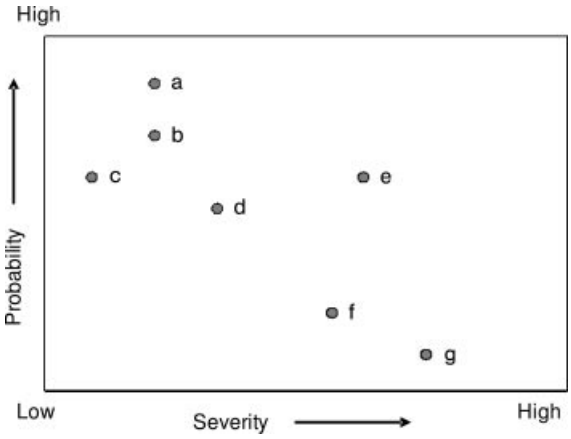

Figure 16. Sample risk map
a) Machine breakdown; b) Transportation failure; c) Supplier quality problems; d) Supplier failure; e) Increasing raw material prices; f) Accident (e.g., fire); g) Terrorist attack

variations more efficiently and respond to consumer demand more quickly. Combining agility with leanness (inventory reduction) enables cost effectiveness of the upstream chain and high service levels even in a volatile marketplace in the downstream chain [87].

Disruption Management. A disruption management system should be capable of detecting abnormal situations before they occur, diagnosing the root cause, and proposing corrective actions as required [88]. It should also be capable of coordinating SC resources to return the SC to normal and planned operation [89].

For other and more specific risk mitigation strategies, the reader is referred to [80, 86, 87, 90].

5.5. Conclusion and Future Directions

Today's SCs strive to be increasingly efficient and effective by adopting strategies such as outsourcing, globalized operation, just-in-time practices, and lean inventory. However, these measures to operate the SC more efficiently often lead to increased fragility and risk exposure. As uncertainties become more prevalent and disruptions arise from many sources, SC risk management has become imperative. The SC risk management framework comprises risk identification, risk quantification, risk assessment, risk mitigation, and risk monitoring. Various methods for risk identification, risk quantification, and risk mitigation have been presented.

Going forward, new risks are entering the SC. Energy source and cost will continue to be uncertain. This could have a significant impact for SCs as energy and fuel cost makes up the majority of logistics cost. The uncertain global political climate will impact SCs operating across national borders. Demand could be volatile as new markets emerge, shifting the longer-term demand pattern from Japan to China and from Europe to Middle East and North Africa. Increased focus on sustainability of SCs brings about new risks and opportunities [91]. In the literature, there has not been much attention on common cause failure, i.e. multiple things going wrong due to a common root cause, e.g. widespread power failure.

6. Safety Management in Industrial Practice

6.1. Management of Major Hazards in the Process Industries

The chemical process industry has been the source of some of the largest accidents and disasters caused by human activity → Plant and Process Safety, 1. Introduction.

Considering the risks involved with chemical processing most, if not all, organizations working in the chemical process industries have to manage major hazards. The actual types of hazards vary widely over the industries, from well blow-outs in the oil industry, dust explosions in huge storage silos, to poisoning and biohazards associated with the release of microscopic quantities of toxic or biological material. There will obviously be differences in the detail of how the very industry specific hazards are managed. However, the current theory and practice of how to overall manage such hazards is applicable over the full spectrum of hazards in the chemical processing industries.

The accidents associated with major hazards are often termed process safety accidents as opposed to workplace safety accidents. The workplace safety accidents comprise individual accidents, e.g., slips, trips, and falls. Both of the terms major hazards and process safety will be used in the following. It is worth noting that the methods for managing process safety can be used for all industries with major hazards, e.g., transportation including airlines, nuclear plants, etc., and conversely the experiences from these industries have proven extremely relevant to better manage the risk associated with the more narrow chemical industry definition of process safety. Therefore both examples from chemical process industries and from other major hazard industries will be relevant when developing an understanding of process safety issues.

Aside from some truly unforeseeable natural disasters like meteors, accidents happen because of failure of humans. Such human failings may involve the failure of a frontline operator,

whether a chemical plant operator or an airline pilot. However, investigations will almost inevitably be flawed if they conclude that human error at the frontline operator level was the root cause of an incident. Very often accidents are caused by latent human error, such as a flaw in the original design, by an error in maintenance, or by a change in the construction, procedures, etc. which was not thoroughly checked. Likewise actions or omissions of the higher organizational levels are frequent causes of accidents. A thorough incident investigation will thus generally reveal failings at several different levels of an organization.

Therefore, managing the major hazards within an organization is the responsibility of the chief executive officer (CEO) and the wider management team. They have to clearly state their commitment to process safety and ensure that the resources in terms of funds, staffing, standards, competencies, etc, are available. Subject to ownership structure, local legislation, etc. the board and owners will also carry responsibility for ensuring that process safety activities are resourced and managed responsibly in the organization.

6.1.1. Definitions

- *Accident:* an undesirable event leading to injury or death
- *Barrier* is a protective measure to prevent incidents from happening, could be a physical protective device, e.g., a pressure relief valve or a procedure, a training programme, etc.
- *Dormant factors* are often part of the causation for an incident, whether a weakness of design carried out years before the incident, a weakness in operating procedures etc.
- *Hazard* is a condition that has potential to cause an accident. That is, what can go wrong in a specific plant or activity.
- *Human factors* are with extremely few exceptions part of the causation for all accidents, whether human factors affect the original design, the leadership for a plant, the operating practices, etc.
- *Immediate cause:* e.g., the immediate cause for a gas escape was a hole in a pipe
- *Intermediate cause:* the hole that caused a gas escape was caused by corrosion
- *Incident* more broadly includes both accidents and near misses
- *Latent factors* are typically a weakness in the design which have not been detected and thus lies dormant for years to be exposed when several barriers fail
- *Major hazard* is about the hazards which can result in a major accident, e.g., serious injuries, fatalities, major plant, or environmental damage
- *Near miss:* an undesirable event which has the potential to lead to injury or death
- *Process safety incident:* an incident where the application of complex technology is involved. When investigating these incidents they often have complex causation, including, e.g., design error, operating error, lack of supervision, lack of maintenance, inadequate management of change, etc. and combinations thereof. In the broadest definition process safety incidents includes both those directly related to the chemical process industries, and other incidents with similar causation and complexity, e.g., airplane incidents.
- *Risk* is the combined impact of a hazard, i.e., how likely is that a certain hazard will result in fatalities
- *Root cause* initiating cause for an incident, e.g., the cause for the hole was that the pipe was not being maintained. This could go even deeper, e.g., new management had decided to cut maintenance costs because they did not appreciate the risks involved.
- *Workplace safety incident* a relatively simple incident involving a single person or a few persons and their interactions. Examples are, slips trips and falls, hand tool accidents, working at heights, dropped objects, working with chemicals, etc. Workplace incidents have the potential to cause injury or death of a single or a few persons.

6.1.2. History of Process Safety

Using the broad definition of process safety incidents as part of major hazards incidents, process safety incidents became part of human life as the technologies developed.

One of the early technologies with major hazard potential was ship transportation, going back at least a couple of thousand years. The early development of ship designs was based on

generations of trial and error. When the design failed, it often resulted in a sunken ship and possibly a number of fatalities. Over generations the designs became better and as the theory for ship design became more well understood robust standards were developed and applied. Likewise the safety associated with the operation of ships developed as navigational charts and instruments became available and more sophisticated. Over centuries, navigators competencies were developed and formalized through apprenticeships and formal education. Even better safety was obtained as improved weather forecasting was introduced, iceberg positions were mapped and made available to ships en route, and GPS was introduced, etc.

However, despite the major progress since antiquity in ship building technology, in propulsion systems, in crew competency, in weather forecasting, in navigational charts and navigation methods, electronic equipment, etc., incidents still occur, often as a result of complex causation where several barriers have failed, e.g., General Slocum (1904, 1021 fatalities) (see Fig. 17), Titanic (1912, 1517 fatalities), and more recently Herald of Free Enterprise (1987, 193 fatalities).

Generally as a technology develops, the occurrence of simple failure modes gradually become rarer as barriers are put in place for each likely failure mode. These barriers could be better design, better maintenance, better competency of staff, operating procedures, etc., i.e., the sum of the progress in experience and theory. However, over time barriers get tested again and again, occasionally individual barriers fail and on rare occasions all barriers fail simultaneously and an accident occur. This concept has been described by James Reason in the "swiss cheese model" [92] (Fig. 18].

The swiss cheese model has been used universally from, e.g., road safety to hospital safety and chemical process safety.

6.2. Major Accidents-Case Studies

Major accidents resulting in multiple fatalities, major environmental damage, etc. are subject of detailed investigation and are often followed by litigation and prosecution of responsible individuals and organizations. Such major incidents have often had major long term impact on their respective industries.

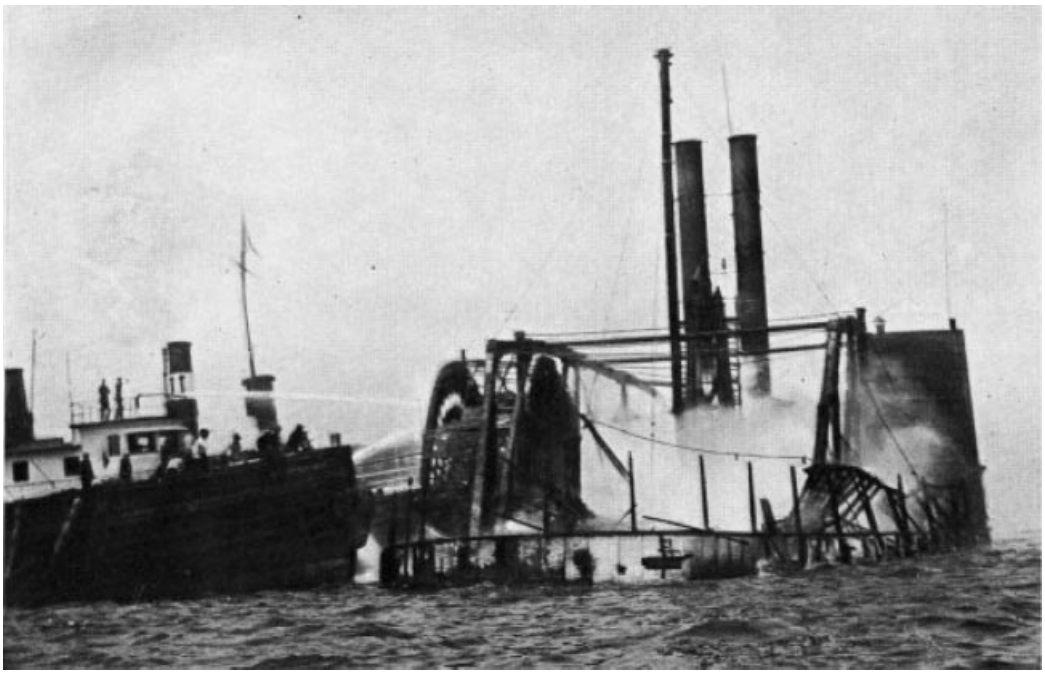

Figure 17. Firefighters working to extinguish the fire on the grounded General Slocum

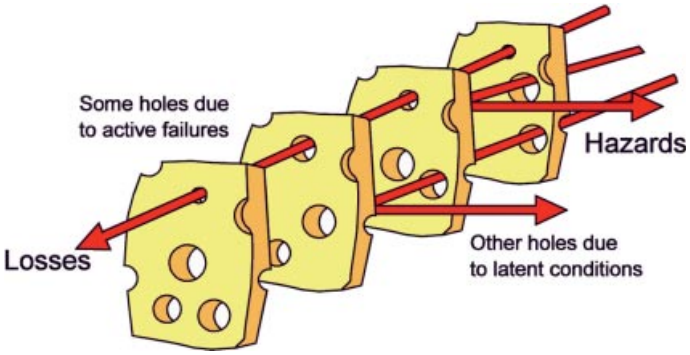

Figure 18. Swiss cheese model with successive layers of defences

It is obviously essential to understand in detail the specific processes which an organization is responsible in order to efficiently manage process safety. However, the study of past industry incidents will provide important inspiration, insights, and knowledge for process safety activities in an organization.

Short descriptions are given below of a few selected accidents, highlighting the main events and causation for illustration if the issues discussed here. For comprehensive case stories please refer to the literature, e.g., [93, 94].

Flixborough. On 1 June 1974, the Nypro factory at Flixborough exploded resulting in 28 on-site fatalities as well as injuries and extensive damage in surrounding villages → Plant and Process Safety, 4. Chemical Process Safety Regulations.

The major issues in the case of the Flixborough disaster were:

- The original plant design relied on a process configuration with massive inventories of hot pressurised flammable components, a process with much smaller inventory could have been designed. That is, a latent factor that would greatly increase the risk in case of a leak.
- With the office block within the plant, there was a major unnecessary exposure, which due to fortunate timings did not influence the number of deaths. Another latent factor that during some 30% of the time would greatly increase the consequences of an explosion.
- A temporary modification was allowed to be installed without full engineering design verification. A failing at supervisory and management level allowing such a change to the plant to be made without appropriate engineering checks.

Seveso. On 10 July 1976, reaction products containing highly toxic dioxin happened from a herbicide plant near the village of Seveso in northern Italy. Several hundred people developed the skin disease chloracne, but there were no immediate fatalities.

The accident resulted in major new legislation based on the European Community Seveso Directive → Legal Aspects, Chapter 5.

The incident revealed several weaknesses:

- The safety of shutdown the batch processes at different stages of completion was not well understood, especially in light of the unfortunate legislation requiring untimely shutdowns. The potential relief cases for the bursting disk were incomplete, hence, omitting the liquid collection vessel downstream. That is, the process was poorly understood and poorly designed.
- The heating system design was not fail safe in the sense that it was able to overheat the process.
- The local communities had no knowledge of the hazards associated with the nearby chemical plant, thus an example of poor stakeholder management.
- The emergency response was ineffective.

Bhopal. The Bhopal accident happened on 3 December 1984 and was the worst accident in the history of the chemical industry. There is significant uncertainty about the number of

fatalities, ranging from an official number of 2259 immediate deaths to unofficial estimates including long term deaths of some 10 000–20 000 → Plant and Process Safety, 4. Chemical Process Safety Regulations.

The main issues in the Bhopal disaster were:

- The use of hazardous chemicals (MIC) instead of less hazardous ones. Latent design issue.
- Storing these chemicals in large tanks instead of much smaller steel drums. Latent design issue.
- Possible corroding material in pipelines. Lack of integrity management issue.
- Poor maintenance after the plant ceased production in the early 1980s. Lack of integrity management issue.
- Failure of several safety systems (due to poor maintenance and regulations).
- Safety systems being switched off to save money—including the methyl isocyanate (MIC) tank refrigeration system which alone would have prevented the disaster.
- The problem was made worse by the plant's location near a densely populated area, nonexistent catastrophe plans and shortcomings in health care and socioeconomic rehabilitation. Analysis shows that the parties responsible for the magnitude of the disaster are the two owners, Union Carbide Corporation and the Government of India, and to some extent, the Government of Madhya Pradesh.

Piper Alpha. The Piper Alpha platform in the United Kingdom North Sea was destroyed on 6 July 2008 by a series of explosions and fires, killing 167 men. The initiation and escalation of this accident had a complex causation where several barriers were ineffective. Some of the main issues were:

- The permit to work system was ineffective.
- The firewater could not be used due to the electrical pumps being knocked out by the explosion and the diesel driven pumps were on manual start due to diver work earlier in the day, but were inaccessible due to the fires so they could not be started.
- The high-pressure pipeline risers were exposed to the fires and eventually failed catastrophically causing massive fires and explosions. This was aggravated by nearby platforms continuing to produce into the common pipeline system rather than initiating depressurization.
- Escape from the muster area in the accommodation became impossible as the fires progressed.

6.3. Comprehensive Process Safety Management-Risk-Based Process Safety

The above examples in combination with thousands of others show that managing process safety effectively requires a comprehensive approach covering a considerable number of subjects, in order that sufficient effective barriers exist to prevent major accidents from happening.

Organizations have thus established comprehensive systems for how to manage process safety. Such systems have several elements covering the all aspects necessary for effective managing process safety.

In the following such a system, the risk-based process safety (RBPS) elements will be described. This system was published by the Center for Chemical Process Safety (CCPS) under AIChE [95].

The RBPS has four main categories:

1. Commit to process safety: Ensure that management and employees care about process safety, ensure that there is acceptance and compliance with standards and demonstrate commitment to stakeholders
2. Understand hazard and risk: Know what you operate, identify hazards and manage and minimize risk through analysis etc.
3. Manage risk: Know how to operate and maintain the process, control changes and manage incidents
4. Learn from experience: Investigate incidents, monitor performance through reviews, audits and KPIs, and ensure that findings are acted effectively upon

These four main categories have been divided into 20 elements, described in this section, covering all aspects of process safety:

Each element will require careful consideration, but will take on different substance and

importance subject to the type of industrial activity at hand, location, country, organizational context, etc. It is essential that dependable practices are established and maintained for each element.

6.3.1. Commit To Process Safety

Process Safety Culture. In order that process safety can be managed efficiently, an open and questioning environment must be in place where process safety issues and concerns can be raised by all stakeholders and be dealt with in a timely fashion. There must be a sense of vulnerability, i.e., nobody should take process safety for granted, also when there have not been major incidents for a long time.

The process safety culture requires the involvement of and is a responsibility for the entire organization, but the strong commitment by top management is indispensable if a strong culture is to develop.

Compliance with Standards. Standards comprise international industry standards, legislation and company standards for how to, e.g., design, operate, and maintain a process plant. An organization needs to determine which standards apply and ensure that they are available and updated to all relevant staff.

A culture of compliance with mandatory standards, whether internal or external, is essential. Notwithstanding, deviations from standards may occasionally be required. Hence, a formalized system for approval of such deviations must be in place. Company standards must be effective, i.e., written to be useful for the end user, possible to comply with and kept up to date.

Process safety competency of an organization comprises continuous learning and improvement of process safety competency, and further that the knowledge is available to the relevant people and applied.

In order for effective learning and sharing of knowledge to take place, top management must encourage openness and sharing of knowledge between shifts, plants, business units, etc.

Workforce Involvement. The workforce at all levels obtain valuable experiences and knowledge of how systems and equipment actually work. Hence, the active involvement of the workforce will be necessary to ensure that this knowledge is effectively captured and made available to, e.g., future plant designs.

The active involvement of the workforce will also assist in developing a questioning and learning environment.

Stakeholder Outreach. A process plant will have a number of stakeholders, in some cases this may be a very considerable number. These stakeholders will both be internal, e.g., the workforce, and external, such as regulatory bodies, business partners, customers and vendors, environmental interest groups, fishermen and other business potentially affected, and the wider public especially those living close to the plant.

6.3.2. Understand Hazards and Risks

Process Knowledge Management. Developing and maintaining process information in the form of written technical documents and specifications, engineering drawings and calculations, specifications for design and fabrication, material safety sheets, etc. is key to understanding risks and developing other RBPS elements. For example, risk analysis, procedures, training material, management of change, etc.

Hazard identification and risk analysis concerns the identification of hazards and evaluation of the risk. Identification of hazards should take place early on to ensure that the appropriate remedial actions are put in place and to ensure that the risk level is commensurate with the risk appetite of the organization.

6.3.3. Manage Risk

Operating Procedures. In order to ensure a consistent high performance in executing critical activities, these activities should be documented in the form of operating procedures. Operating procedures are written instructions, whether stored in hardcopy or electronically,

which lists the steps and describes how specific tasks are to be performed.

Safe working practices includes procedures for nonroutine activities such as work permits including hot work and entry into confined spaces etc.

Asset integrity and reliability is about ensuring that equipment and systems are properly designed, installed, and remains fit for use until its retirement.

Asset integrity comprises:

- Verification and documentation of the integrity of the initial design, construction, and installation of equipment and systems.
- Ensuring that during operation of the equipment and systems, they remain within the design envelope.
- The execution and documentation of inspection, testing, and preventive maintenance programs by qualified personnel.
- Controlled and documented repairs and adjustments to equipment.
- A quality assurance and control program to ensure the quality of initial fabrication, installation, and subsequent maintenance activities.

Contractor Management. In many industries, contractors execute many work scopes on behalf of the company. For example, it is customary in the oil industry to contract a whole drilling rig including crew to drill oil and gas wells on behalf of the oil company. The contractor must have procedures and systems in place which ensures that the contractor can operate to the same standards as the company.

Training and performance assurance covers the training and instruction of staff to specific job and task requirements as well as the assurance that workers have understood the training to the level required.

Management of change (MOC) is the discipline of ensuring that changes to a chemical process plant or other technical installation are adequately evaluated, risk assessed, and appropriate corrective action taken before implementation. Ineffective MOC is one of the common contributory or root causes of incidents.

Operational readiness comprises the activities to verify that new plants or existing plants that have been shut down for modification or other activities are ready for start-up.

Conduct of Operations. To ensure that operations consistently remain within safe operating limits, the objectives must be clearly stated and the operations executed by qualified staff.

Emergency Management. Organizations responsible for hazardous activities must be able to deal effectively with emergencies. A clear line of command must be established and the organization must be empowered to deal with the required emergency response.

6.3.4. Learn From Experience

Incident Investigation. Accidents and near misses provide important opportunities for learning and thereby preventing recurrence. Through effective investigation, organizational and other weaknesses can be exposed and appropriate action taken to rectify such weaknesses.

Measurement and Metrics. Defining and monitoring critical key performance indicators (KPIs) is an important method to judge the efficiency of the overall process safety management activities. Based on low or declining performance corrective action can be taken ahead of reaching the lowest acceptable level.

Auditing provides another set of observations of the efficiency of the process safety management activities. Programmes should be established covering all relevant activities and RBPS elements. Effective follow-up on audits and monitoring of the follow-up is important to maintaining high standards.

Management Review and Continuous Improvement. Management review is the routine monitoring of the performance of the management system. It should be planned and recurring covering the entire management system and the 20 RBPS elements.

6.4. How to Implement a RBPS System

The 20 RBPS elements provide a catalogue of issues to address subject to the type of industry and risks involved. Many companies have set up process safety management systems to address some if not all of these issues. Others may have less elaborate systems, which they wish to improve or are considering how to arrange the process safety management system in the first place. For those initiating a process safety management program, a detailed strategy for stakeholder management may not be the first issue to address, hence, an example of a prioritized list of actions is given below for inspiration on how to commence building process safety performance in an organization. These first steps must over time be broadened, considering all 20 elements.

Management Commitment. In order for all levels of an organization to take process safety seriously, the senior management must demonstrate a strong commitment to process safety and that they support an open dialogue about any issue that could affect process safety.

Employee Involvement. Actively engage employees in the work to improve process safety including the activities below.

Identify Hazards. Identify the hazards (HAZID) associated with the activities the organization is engaged in.

Incident Investigation. Clearly demonstrate that all process safety incidents will be investigated and that the results will be acted effectively upon. In cases where disciplinary action is involved, it is important that such actions are just.

Management System. Provide a simple accessible management system comprising high-level policies and the necessary procedures and standards for safety-critical work activities, e.g., operational, and maintenance procedures.

Management of Change. Develop an understanding of the importance of identifying and managing changes, whether associated with the technical plant, feed-streams, products, procedures, organization, etc.

Changes affecting process safety can be associated with a wide range of activities, a nonexhaustive list comprises:

- Design changes
- Changes to raw materials and/or product specification
- Temporary changes (repairs, bypasses, temporary equipment, etc.)
- Organizational changes (planned reorganization, new staff, absence due to illness)
- Legislative changes
- Procedural changes
- Change of subcontractors and vendors
- Budget cuts

Inadequate MOC is one of the common causes for incidents and often there have been no MOC activities carried out, because the change was not recognized in the first place. Changes can be very subtle and difficult to recognize in a busy work environment. For example, an experienced operator not turning up for the night shift should cause a reschedule of critical activities planned for the shift. However, the issue may not be spotted by the shift manager or if spotted, it may be that many other activities are contingent on the work that this operator should have performed, hence, a potentially inadequate replacement is found not to delay other activities.

Managing change requires firstly awareness training so staff at all levels become aware of the need to manage change and aware of the critical types of changes which should be considered. Secondly, processes should be in place to register and handle the different types of changes, e. g., design review, HAZOP, and approval by a technical authority for an engineering design change.

Process Safety Competency. Establish an overview of competencies required and a system to register the available competencies in the organization. Develop programmes to develop staff.

Quantitative Risk Assessment (QRA). Supplement the hazard register with more quantitative evaluations to prioritize activities, e.g,.

maintenance, where the impact on risk is highest.

6.5. Conclusion

For an organization to develop a high performance in process safety will require a strong and consistent drive and long-term commitment at all levels. Applying RBPS or other similarly comprehensive approaches will ensure that process safety is promoted over a sufficiently broad range of issues that the chance of success greatly increases.

The approach and implementation of a RBPS or similar systems will require adaption to the industrial hazards and complexities, local legislation, workforce, stakeholders, etc. in order that a practical process safety management system can built which will be effective for the particular plant.

References

1 I. Nimmo: "Adequately address abnormal operations", *Chem. Eng. Prog.* **91** (1995) no. 9, 36–45.

2 V. Venkatasubramanian et al.: "A review of process fault detection and diagnosis Part I: Quantitative model-based methods", *Comput. Chem. Eng.* **27** (2003) 293–311.

3 A.S. Willsky, H.L. Jones: "A generlized likelihood ratio approach to the detection and estimation of jumps in linear systems". *IEEE Trans. Autom. Control* **AC-21** (1976) 108–112.

4 L.H. Chiang, E.L. Russell, R.D. Braatz: *Fault detection and diagnosis in industrial systems*, Springer Verlag, Berlin 2001.

5 P.M. Frank, S.X. Ding, T. Marcu: "Model-based fault diagnosis in technical processes", *Transactions of the Institution of Measurement and Control* **22** (2000) no. 1, 57–101.

6 A. Bhagwat, R. Srinivasan, P.R. Krishnaswamy: "Fault detection during process transitions: a model-based approach", *Chem. Eng. Sci.* **58** (2003) 309–325.

7 Y. Tsuge et al.: "Fault diagnosis algorithm based on the signed directed graph and its modifications", *Ind. Chem. Eng. Symp. Ser.* **92** (1985) 133–144.

8 P. Nomikos, J.F. MacGregor: "Monitoring of Batch Processes using Multi-way Principal Component Analysis". *AIChE J.* **40** (1994) no. 8, 1361–1375.

9 J.F. MacGregor, T. Kourti: "Statistical Process control of multivariate processes", *Control Engineering Practice* **3** (1995) 403–404.

10 J.E. Jackson: *A User's Guide to Principal Components*, J. Wiley & Sons, New York 1991.

11 K. Villez, M. Ruiz, G. Sin, C. Rosén, J. Colomer, P.A. Vanrolleghem: "Combining Multiway Principal Component Analysis (MPCA) and clustering for efficient data mining of historical data sets of SBR processes", *Water Sci. Technol.* **57** (2007) no. 10, 1659–1666.

12 M.L.R. Ordonez: Multivariate Statistical Process Control and Case-Based Reasoning, for Situation Assessment of Sequential Batch Reactors, PhD Thesis, University of Girona, Girona 2008.

13 R. Rengaswamy, V. Venkatasubramanian: "A syntactic pattern- recognition approach for process monitoring and fault diagnosis", *Engineering Applications of Artificial Intelligence* **8** (1995) no. 1, 35–51.

14 L. Wang, Y. Liu, P.J. Griffin: "A combined ANN and expert system tool for transformer fault diagnosis". *IEEE Trans. Power Delivery* **13** (1998) 1224–1229.

15 D. Mylaraswamy, V. Venkatasubramanian: "A hybrid framework for large scale process fault diagnosis", *Comput. Chem. Eng.* **21** (1997) 935–940.

16 B. Özyurt, A. Kandel: "A hybrid hierarchical neural network-fuzzy expert system approach to chemical process fault diagnosis", *Fuzzy Sets and Systems* **83** (1996) 11–25.

17 H. Vedam, V. Venkatasubramanian: "PCA-SDG based process monitoring and fault diagnosis", *Control Engineering Practice* **7** (1999) 903–917.

18 S. Mannan: "Hazard Identification, assessment and control", in *Loss Prevention in Process Industries*, 3rd ed., Elsevier, Amsterdam 2005.

19 F. Crawley, B. Tyler: *Hazard Identification Methods*, Institution of Chemical Engineers, Rugby 2003.

20 G.L. Wells: *Hazard Identification and Risk Assessment*, Institution of Chemical Engineers, Rugby 1996.

21 V. Venkatasubramanian, J. Zhao, S. Viswanathan: "Intelligent systems for HAZOP analysis of complex process plants", *Comput. Chem. Eng.* **24** (2000) 2291–2302.

22 T. Kletz, P. Chung, E. Broomfield, C. Shen-Orr: *Computer Control and Human Error*, Institution of Chemical Engineers, Rugby 1995.

23 P. Andow: *Guidance on HAZOP procedures for Computer Controlled Plants*, HSMO, London 1991.

24 J.B. Lear: "Implementing Safe, Operable Control Systems", *Control* **95**, 1995.

25 I. Nimmo, S.R. Nunns, B.W. Eddershaw: *Loss Prevention Bulletin*, vol. 111, Institution of Chemical Engineers, Rugby 1993, p. 13.

26 T.A. Keltz: *Process Plants: A Handbook for Inherently Safer Design*, Taylor & Francis, Philadelphia 1998.

27 T.A. Kletz: *Plant Design for Safety*, The Institution of Chemical Engineers, Rugby 1991.

28 The Institution of Chemical Engineers and The International Process Safety Group: *Inherently Safer Process Design*, The Institution of Chemical Engineers, Rugby 1995.

29 CCPS: *Inherently Safer Chemical Processes: a life cycle approach*, 2nd ed., "Center for Chemical Process Safety", J. Wiley & Sons, New York 2009.

30 S. Hochheiser: *Rohm and Haas, History of a Chemical Company*, University of Pennsylvania Press, Philadelphia 1986.

31 D. Lin, A. Mittelman, V. Halpin, D. Cannon: "Inherently Safer Chemistry: A Guide to Current Industrial Processes to Address High Risk Chemicals", U.S. Environmental Protection Agency, Washington 1994.

32 J. Marshall, A. Mundt, M. Hult, T. McKealvy, P. Myers, J. Sawyer: "The relative risk of pressurized and refridgerated storage for six chemicals", *Process Saf. Prog.* **14** (1995) no. 3, 200–211.

33 C. Palaniappan, R. Srinivasan, R. Tan: "Expert system for design of inherently safer processes 1. Route Selection Stage", *Ind. Eng. Chem. Res.* **41** (2002) no. 26, 6698–6710.

34 C. Palaniappan, R. Srinivasan, R. Tan: "Expert system for design of inherently safer processes 2. Flowsheet Development Stage", *Ind. Eng. Chem. Res.* **41** (2002) no. 26, 6711–6722.

35 V. Pilz: *Bayers procedure for the design and operation of safe chemicalk plants, Inherently Safer Process Design*, The Institution of Chemical engineers, Rugby 1995, 4.54–4.56.

36 N.E. Scheffler: "Inherently safer latex plants", *Process Safety Progress* **15** (1996) no. 1, 11–17.

37 Dow Chemical Company: *Dow's Chemical Exposure Index Guide*, 1st ed., American Institute of Chemical Engineers, New York 1994.

38 Dow Chemical Company: *Dow's Fire and Explosion Index, Hazard Classification Guide*, 7th ed., American Institute of Chemical Engineers, New York 1994.

39 P.T. Anastas, J.C. Warner: *Green Chemistry: Theory and Practice*, Oxford University Press, Oxford 1998, p. 30.

40 D.W. Edwards, D. Lawrence: "Assessing the inherent safety of chemical process routes: is there a relation between plant costs and inherent safety?", *Proc. Saf. Environ. Protect, Trans IChemE* **71** (1993) PartB, 252–258.

41 A.M. Heikkilä, M. Hurme, M. Järveläinen: "Safety considerations in process synthesis", *Comput. Chem. Eng.* **20** (1996) 115–120.

42 S.R. Cave, D.W. Edwards: "Chemical process route selection based on assessment of inherent environmental hazard", *Comput. Chem. Eng.* **21** (1997) 965–970.

43 F.I. Khan, S.A. Abbasi: "Multivariate hazard identification and ranking system", *Process Saf. Prog.* **17** (1998) 157–170.

44 J.P. Gupta, D.W. Edwards: "A simple graphical method for measuring inherent safety", *J. Hazard. Mater.* **104** (2003) 15–30.

45 C. Palaniappan, R. Srinivasan, R. Tan: "Selection of inherently safer process routes: a case study", *Chem. Eng. Proces.* **43** (2004) 647–653.

46 I.K. Adu et al.: "Comparison of methods for assessing environmental, health and safety (EHS) hazards in early phases of chemical process design", *Process Saf. Environ. Protect.* **86** (2008) 77–93.

47 G. Koller, U. Fischer, K. Hungerbühler: "Assessing safety, health, and environmental impact early during process development", *Ind. Eng. Chem. Res.* **39** (2000) 960–972.

48 H. Sugiyama, U. Fischer, K. Hungerbühler: "Decision framework for chemical process design including different stages of environmental, health, and safety assessment", *AIChE J.* **54** (2008) 1037–1053.

49 T. Albrecht, S. Papadokonstantakis, H. Sugiyama, K. Hungerbühler "Demonstrating multi-objective screening of chemical batch process alternatives during early design phases" *Chem. Eng. Res. Des.* **88** (2010) 529–550.

50 Design Institute for Physical Properties, American Institute of Chemical Engineers (AIChE), USA 2007, http://dippr.byu.edu/ (accessed 19.01.2012).

51 National Institute of Standards and Technology (NIST), USA 2010, http://www.nist.gov/srd/ (accessed 19.01.2012).

52 International Uniform Chemical Information Database, European Chemicals Agency (ECHA), Helsinki, Finland 2008, http://iuclid.eu/ (accessed 19.01.2012).

53 Canadian Centre for Occupational Health and Safety (CHEMpendium), Hamilton, Canada 2006 http://www.ccohs.ca/ (accessed 19.01.2012).

54 C. Capello, U. Fischer, K. Hungerbühler: "What is a green solvent? A comprehensive framework for the environmental assessment of solvents", *Green Chem.* **9** (2007) 927–934.

55 R. Srinivasan, N.T. Nhan: "A statistical approach for evaluating inherent benignness of chemical process routes in early design stages", *Process Saf. Environ. Protect.* **86** (2008) 163–174.

56 J. Roussel: *Can supply chain planning systems deliver the goods*?, PRTM's Insight, 2002.

57 I. Karimi, R. Srinivasan, L.H. Por: "Unlock Supply Chain Improvements through Effective Logistics", *Chem. Eng. Prog.* **5** (2002) 32–38.

58 K. Sadgrove: *The Complete Guide to Business Risk Management*, Gower Publ., Aldershot 2005.

59 The McKinsey Quarterly: Understanding supply chain risk: A McKinsey Global Survey, http://www.mckinseyquarterly.com/Understanding_supply_chain_risk_A_McKinsey_Global_Survey_1847 (accessed 17 January 2012).

60 T. Sullivan: "Special Report: Road to Recovery–Oronite Strives to Regain Customer Confidence", *Lube Report* **6** (2006) no. 25.

61 A. Norrman, U. Jansson: "Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident", *International Journal of Physical Distribution & Logistics Management* **34** (2004) no. 5, 434–456.

62 J.M. Kilgore: "Mitigating Supply Chain Risks", *89th Annual International Supply Management Conference*, Philadelphia, 2004, pp. 25–28.

63 J. Lam: *Enterprise Risk Management: From Incentives to Controls*, J. Wiley & Sons, New York 2003.

64 G. Guillen et al.: "Multiobjective supply chain design under uncertainty", *Chem. Eng. Sci.* **60** (2005) 1535–1553.

65 Z. Li, M.G. Ierapetritou: "Process scheduling under uncertainty: Review and challenges", *Comput. Chem. Eng.* **32** (2008) 715–727.

66 B. Karri, R. Srinivasan, I.A. Karimi: "Robustness measures for operation schedules subject to disruptions", *Ind. Eng. Chem. Res.* **48** (2009) no. 20, 9204–9214.

67 J. Li, I.A. Karimi, R. Srinivasan: "Robust crude oil scheduling under uncertainty", *18th European Symposium on Computer Aided Process Engineering (ESCAPE 18)*, Lyon, France, June 1–4, 2008.

68 U. Paulsson: "Managing risks in supply chains–an article review", *NOFOMA*, Oulu, Finland, June 12–13, 2003.

69 C. Brindley: *Supply Chain Risk*, Ashgate Publ., Hampshire 2004, pp. 14–27.

70 U. Jüttner, H. Peck, M. Christopher: "Supply Chain Risk Management: Outlining an Agenda for Future Research", *International Journal of Logistics: Research and Application* **6** (2003) 197–210.

71 N. Malini, I. Capar, A. Narayanan: "Managing supply chains in times of crisis: a review of literature and insights", *International Journal of Physical Distribution & Logistics Management* **39** (2009) no. 7, 535–573.

72 O.K. Helferich: "Securing the supply chain against disaster", *Distribution Business Management Journal* **2** (2002) no. 3, 10–14.

73 C.B. Pickett: "Strategies for Maximizing Supply Chain Resilience: Learning from the Past to Prepare for the Future", Massachusetts Institute of Technology. Ph.D. Thesis, Massachusetts, 2003.

74 R.P. Lensing: "Historical Events and Supply Chain Disruption: Chemical, Biological, Radiological and Cyber Events", Massachusetts Institute of Technology, Ph.D. Thesis, Massachusetts, 2003.

75 T. Wu, J. Blackhurst, V. Chidambaram: "A model for inbound supply risk analysis", *Computers in Industry* **57** (2006) 350–365.

76 A. Adhitya, R. Srinivasan, I.A. Karimi: "Supply chain risk identification using a HAZOP-based approach", *AIChE J.* **55** (2009) no. 6, 1447–1463.

77 J. Hallikas et al.: "Risk management processes in supplier networks", *International Journal of Production Economics* **90** (2004) 47–58.

78 R.J. Chapman: *Simple Tools and Techniques for Enterprise Risk Management*, J. Wiley & Sons, New York 2006.

79 S. Chopra, M.S. Sodhi: "Managing Risk to Avoid Supply Chain Breakdown", *MIT Sloan Management Review* **46** (2004), 53–61.

80 P.R. Kleindorfer, L.N. Van Wassenhove: "Managing Risk in Global Supply Chains", in H. Gatigon, J. Kimberly (eds.): *The Alliance on Globalization*, Cambridge University Press, Cambridge 2004.

81 A. Oke, M. Gopalakrishnan: "Managing disruptions in supply chains: A case study of a retail supply chain", *International Journal of Production Economics* **118** (2009) 168–174.

82 J.-H. Thun, D. Hoenig: "An empirical analysis of supply chain risk management in the German automotive industry", *International Journal of Production Economics* **131** (2009) no. 1, 242–249.

83 G. Tuncel, G. Alpan: "Risk assessment and management for supply chain networks: A case study", *Computers in Industry* **61** (2010) 250–259.

84 S.S. Pitty et al.: "Decision support for integrated refinery supply chains: Part 1. Dynamic simulation", *Comput. Chem. Eng.* **32** (2008) no. 11, 2767–2786.

85 M. Christopher, H. Lee: "Mitigating supply chain risk through improved confidence", *International Journal of Physical Distribution & Logistics Management* **34** (2004) 388–396.

86 Y. Sheffi: *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*, MIT Press, Cambridge 2005.

87 M.N. Faisal, D.K. Banwet, R. Shankar: "Supply chain risk mitigation: modeling the enablers", *Business Process Management Journal* **12** (2006) no. 4, 535–552.

88 A. Adhitya, R. Srinivasan, I.A. Karimi: "A model-based rescheduling framework for managing abnormal supply chain events", *Comput. Chem. Eng.* **31** (2007) 496–518.

89 C.W Craighead, J. Blackhurst, M.J. Rungtusanatham, R.B. Handfield: "The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities", *Decision Sciences* **38** (2007) no. 1, 131–156.

90 D. Elkins et al.: "Eighteen ways to guard against disruption", *Supply Chain Management Review* **9** (2005) 46–53.

91 The McKinsey Quarterly. (2010) . McKinsey Global Survey results: How companies manage sustainability. http://www.mckinseyquarterly.com/Energy_Resources_Materials/Strategy_Analysis/How_companies_manage_sustainability_McKinsey_Global_Survey_results__2558 (accessed on 7 April 2010).

92 J. Reason: "Human error: models and management", *Br. Med. J.* **18** (2000) no. 320, 768–770.

93 Trevor Kletz: *A Handbook for Inherently Safer Design*, Taylor & Francis, Philadelphia 1998.

94 Trevor Kletz: *Learning from Accidents*, 3rd ed., Gulf Publ., Houston 2001.

95 Center for Chemical Process Safety: *Guidelines for the Management of Change for Process Safety*, Wiley-VCH Verlag, Weinheim 2007.

96 D. Beaty: *The Naked Pilot–The Human Factor in Aircraft Accidents*, Airlife Publishing Ltd., Marlborough 1995.

97 Center for Chemical Process Safety: *Guidelines for Chemical Process Quantitative Risk Analysis*, 2nd ed., Wiley-VCH, Weinheim 2000.

98 Center for Chemical Process Safety: *Guidelines for Hazard Evaluation Procedures*, 3rd ed., Wiley-VCH, Weinheim 2008.

99 J.R. Chiles: *Inviting Disaster–Lessons from the Edge of Technology*, Harper Business, New York 2001.

100 J. Groeneweg: Controlling the Controllable–Preventing Business Upsets, 5th ed., Global Safety Group, Den Haag 2002.

101 C. Perrow: *Normal Accidents–Living With High-Risk Technologies*, Basic Books Inc., New York 1984.