Publication V

Kidam, K., Hurme, M., Method for identifying contributors to chemical process accidents, Process Safety and Environmental Protection, Volume 91, Issue 5, September 2013, Pages 367–377, doi:10.1016/j.psep.2012.08.002.

© 2012 Institution of Chemical Engineers (IChemE)

Reprinted with permission from Elsevier.

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

journal homepage: www.elsevier.com/locate/psep

# Method for identifying contributors to chemical process accidents

*Kamarizan Kidam*[a,b,*], *Markku Hurme*[a]

[a] *Aalto University, Department of Biotechnology and Chemical Technology, P.O. Box 16100, 00076 Aalto, Finland*
[b] *Universiti Teknologi Malaysia, Department of Chemical Engineering, 81310 UTM Skudai, Malaysia*

ABSTRACT

The paper presents a new method for identifying contributors to chemical process accidents by exploiting knowledge on causes of past accident cases. Accident reports from the Failure Knowledge Database were analyzed and utilized for hazard identification. The accident information gathered was used as a basis to develop an accidents ranking and points-to-look-for approach for the safe design and operation of chemical process equipment. In the method, accident contributors including technical, design and operation errors of major process equipment types and piping are identified. The method is applicable throughout the process lifecycle, even for process changes in the early design stages. The Bhopal tragedy is used as a case study to demonstrate and test the method. The proposed method can predict on average up to 85% of accident causes and design and operation errors.

© 2012 The Institution of Chemical Engineers. Published by Elsevier B.V. All rights reserved.

*Keywords:* Accident contributor; Design error; Hazard identification; Plant design; Process lifecycle

## 1. Introduction

The accident rate in the chemical process industry (CPI) has not decreasing in spite of all the efforts as shown by recent studies (Niemitz, 2010; Prem et al., 2010). The risk level of chemical process plant operation is higher than before and its complexity has increased significantly. Bigger chemical plants are built involving hazardous chemicals with severe processing conditions. At the same time there are present threats to safety performance due to cost-cuttings and restructuring of organizations (Pasman, 2010). These phenomena increase the brain drain and corporate forgettory as discussed by Kletz (1993).

In chemical plant design, the current trend in risk reduction is to utilize the outer layers of protection (i.e. add-on and procedural layers) and often the inherently safer layer is ignored (Hendershot, 2011; Mannan, 2005). Earlier in the 1960s and 1970s, the focus of loss prevention was more technical and design-oriented. However, nowadays more emphasis is given to the human and organizational aspects e.g. the safety management system and safety culture (Pasman, 2010).

Several statistical studies have found that the contribution of design to accidents is significant (Taylor, 2007a; Kidam and Hurme, in press-a) even though safety analyses such as hazard and operability study (Hazop) have been used for decades. Therefore, it is time to take another look at enhancement by means of the inner circle of layers of protection (LOP).

According to OECD (2005), the large majority of accidents in the CPI could have been avoided if lessons learned and available knowledge had been effectively implemented. It has been claimed that about 95% of accident causes are known (Drogaris, 1993) and accidents occur or recur due to poor dissemination and utilization of past accident information (Kletz, 1993; Lindberg et al., 2010). In general, there is enough knowledge to prevent accidents; the challenge is how to make use of lessons learned from accidents.

In this paper, the process safety knowledge from accident cases is utilized and disseminated into design for better accident prevention through design. The paper attempts to develop a method for safer design and operation of chemical processes by exploiting existing knowledge on the reasons for

* *Corresponding author at*: Aalto University, Department of Biotechnology and Chemical Technology, P.O. Box 16100, 00076 Aalto, Finland. Tel.: +358 9 47022641; fax: +358 94512694.
E-mail addresses: kamarizan@gmail.com, kamarizan.kidam@aalto.fi (K. Kidam).
Received 8 May 2012; Received in revised form 9 August 2012; Accepted 13 August 2012
0957-5820/$ – see front matter © 2012 The Institution of Chemical Engineers. Published by Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.psep.2012.08.002

earlier accident cases. Accident information is used for identifying process hazards throughout the process design lifecycle.

## 2. Existing design evaluation methods

There are several well-accepted safety analysis methods for the safe design and operation of chemical processes. According to Crowl and Lauvar (2011) and Seider et al. (2009), the most commonly used safety evaluation methods during chemical plant design are Checklists, Hazop, Layer of Protection Analysis (LOPA), hazard surveys such as Dow Fire and Explosion Index (F&EI), and safety reviews. In general, each method has its advantages and limitations depending on their safety evaluation criteria and when it is being used within the plant design lifecycle (Crawley and Tyler, 2003; Marhavilas et al., 2011a).

Generally, a design team only uses a limited number of safety methods to evaluate their design and the application depends very much on the stage of the design. The majority of the safety methods are complex and knowledge-intensive and therefore requiring training and experience (Khan and Abbasi, 1998; Tixier et al., 2002). Furthermore, the application of complex safety methods is expensive and time-consuming, which may delay the project. According to Hurme and Rahman (2005), every safety method requires a different amount of process information, which makes it best applicable only at certain design stages. In general, most of the existing safety methods are not fully suitable for use in the early stages of plant design, when the cost of eliminating design errors is lowest, although e.g. Hazop and Dow F&EI can be used as an abridged form also earlier.

Based on the above-mentioned issues, the limitation of some well-accepted safety methods in design are discussed and considered in terms of safety method development.

### 2.1. Checklist-based analysis

Checklist-based analysis is very popular, easy to use and can be applied at any phase of the process lifecycle. It is a list of items to check, developed for general or specific safety usage. The main limitation of checklist-based analysis is its creation and application for new and novel processes (Crawley and Tyler, 2003). This is critical for hazard identification of new chemical plant designs. The quality of the checklist may vary and validation is very subjective. The checklist creator or user should have extensive safety knowledge and working experience. Checklists are a very open-ended format, which makes the results difficult to assess. Moreover, the completeness of assessment using a checklist is uncertain and the chances of overlooking hazards are high.

### 2.2. Hazard and operability studies (Hazop)

Hazop is the most widely used safety method in the CPI (Kletz, 2010). It is a well-structured, systematic and effective procedure to identify process hazards as well as operating problems. Taylor (2007b) found that Hazop can detect up to 95% of the design errors that can be seen from piping and instrumentation diagrams (P&ID). However, Hazop needs detailed process information, sound engineering judgment, experienced team members, and may take weeks to complete (Crowl and Lauvar, 2011). These limitations make the assessment expensive and time-consuming. Additionally, the result of the assessment increases the complexity of the plant through add-on protection systems. In this case, the hazard still remains in the process plant.

Further, Duguid (2001) and Taylor (2007b) pointed out that Hazop studies do not deal with mechanical, layout or operating procedure errors, and consider only some of the possibilities for human error. Nor do they consider the escalation of accident contributors that might lead to a major accident (Krishnan, 2005). Hazop is not fully applicable at the early phase of plant design due to the detailed data and information required. In the full form it is done based on the P&ID in basic or detailed engineering as the last check, although some companies perform it earlier in design as a pre-Hazop and also in operation stage in some years intervals.

### 2.3. Hazard surveys

A typical hazard survey method is the Dow Fire and Explosion Index (F&EI), which is very useful for predicting and mitigating fire and explosion hazards. The hazards are ranked systematically by using penalty/credit points using forms. The main assessment criteria are chemical or material factors, general process and special process hazards. The consequences of accidents are determined by the maximum probable property damage and maximum probable days outage. Based on the calculated index value, the degree of hazards is classified as light, moderate, intermediate, heavy or severe.

The Dow F&EI is very useful for plant positioning and layout. Safe spacing can be estimated according to the hazard index value. However, it requires detailed plant and process information, which makes this method not fully applicable at the early phase of plant design. Dow F&EI has been described as a measure of inherent safety by Khan and Amyotte (2003) even Kidam et al. (2008) found that the F&EI did not correlate well with inherent safety indices at process route and subprocess levels, since the hazards evaluated reflect mainly fire and explosion aspects. Dow F&EI is however sensitive to process changes at unit process and equipment level, for which the inherent safety indices are not well applicable because of their low level of detail.

### 2.4. Other methods

Other methods available for hazard identification include What-If Analysis, Fault Tree Analysis (FTA), and Failure Modes and Effects Analysis (FMEA). What-If Analysis is easy to use and applicable to all human activities. However, the method is very dependent on the skill and knowledge of the team members. The method is so flexible that it means some hazards can easily be overlooked. The results are qualitative and difficult to assess for compliance and its completeness. On the other hand, FTA and FMEA require detailed knowledge of the process.

### 2.5. Methods exploiting accident data

In the literature, there are several methods that utilize accident data. For example, Meel et al. (2007) developed the Operational Risk Assessment (ORA) by exploiting an accident database. The paper utilizes accident data to model the rate of occurrence of incidents in the CPI using Bayesian theory. Marhavilas and Koulouriotis (2008) proposed a risk estimation methodological framework using real accident data. The method consists of two risk assessment techniques, which

are Proportional Risk Assessment and Decision Matrix Risk Assessment. The main purpose of these methods is to identify and ranked the important hazard sources at work. The methods were tested in the metal industry.

Recently, Marhavilas et al. (2011b) presented a new method called the Hybrid Risk Assessment Process (HRAP). The method is semi-quantitative and uses occupational accidents data as a basis to rate hazards at work. The data from a power supply company was used as a case study. In general, the methods mentioned above are useful for identifying and assessing hazards at work, however they do not discuss plant design.

### 2.6. *Reflection*

As discussed above, current safety methods do not utilize the knowledge from past accidents in design. Even though the contribution of design to accidents is significant (Drogaris, 1993; Duguid, 2001; Taylor, 2007a), no design-oriented safety methods have been developed based on accident information for the CPI.

From a plant design point of view, current safety methods (Hazop, F&EI, etc.) are effective for evaluating safety. They are however originally designed for the later stages of design because of their need detail process information. In many cases, they are often used as a short form or partially, not the whole procedure. Although Hazop is effective in removing process engineering related faults, the problem is that Hazop is often done too late, when the process design is ready and all process design related changes are expensive. In this case Hazop acts as a final check only and process risks are controlled mainly by add-on safety protection systems. The process hazards remain and the plant complexity is potentially increased.

As mentioned by Hurme and Rahman (2005), each design phase provides a different amount of process information that limits the applicability of the safety methods. The accident contributors (e.g. design errors) arise evenly (in the range of 20–26%) throughout the process design lifecycle stages (Kidam and Hurme, in press-b). The most critical design decisions are at the pre-design stage when the large conceptual design decisions are made, such as route and sub-system selection (Kidam and Hurme, in press-a). If design errors (e.g. chemical reactivity and incompatibility, inappropriate process condition selections, etc.) are overlooked at this stage, they will cause many problems later. Therefore design support is also essential in the early design stages and late design checks are not enough, since they do not remove the hazards but simply complicate the add-on protection levels.

In view of these aspects, it is necessary to develop a safety method that considers the above factors, i.e. the amount of information available during design, the origin and timing of design errors and the relative importance of design decisions. The method should utilize the existing accident information to prevent the same errors from being made repeatedly and be applicable throughout the process lifecycle for hazard identification. The accident information used in the method is derived from the Failure Knowledge Database (FKD, 2011).

## 3. Method for accident contributor identification

The purpose of the method is to identify the accident contributors throughout the process lifecycle and evaluate their importance in causing accidents. The method enables the engineer to foresee potential accident contributors and design and operation errors that commonly arise and are typically overlooked in design activities. Therefore, lifecycle-based safety and design evaluation allows early detection of common design problems and supports the designer during the design work.

The method for identifying accident contributors of chemical process accidents is illustrated in Fig. 1. The evaluation is made for each piece of process equipment as follows. In Step 1 equipment is selected. The potential accident contributors and their root causes are identified in Step 2 through (a) frequent accident contributors, (b) frequent main-contributors, (c) specific contributors (d) contributors that act relatively often as main contributors (SMC), and (e) contributors in the high risk cluster. In Step 3, the potential accident mechanism is identified through the interconnection of contributors.

Then, in Step 4, the potential design and operation errors are identified and linked to design through their potential time of occurrence in the process design lifecycle. The evaluation is continued for all the major equipment in the process. Finally, in Step 5, the results of the analysis are summarized and all the design principles and decisions are documented for later use.

### 3.1. *Identification of accident contributors*

Potential accident contributors are identified in Step 2 by various methods and viewpoints: frequent accident contributors, frequent main contributors, relative frequency, share as main contributor, and cluster of risky contributors (Fig. 1).

Most *frequent accident contributors* of the equipment are identified based on their frequency in earlier CPI accidents. These include both main and sub contributors. The most common ones are summarized in Table 1 with their root causes. A detailed accident ranking is given by Kidam and Hurme (in press-c).

The most *frequent main-contributors* (MC) to accidents are also identified based on their earlier frequency in process accidents (Kidam and Hurme, in press-c). The main-contributor of an accident is the one that triggers and plays a major role in the accident. The most common main-contributors are summarized in Table 2. The values shown in Table 2 are the numbers of cases where the contributor has acted as a main-contributor in the accidents in the FKD database.

Next, less frequent but *specific contributors* are identified. This identification is based on the contributors which are much more frequent than average in the accidents of certain equipment types. Table 3 gives the relatively high contributors for equipment types (Kidam and Hurme, in press-c). For instance erosion is 2.7 times more common an accident contributor in piping than the average for all equipment types.

Depending on the type of equipment, certain accident contributors tend to act more often as main contributors. These contributors are obviously crucial in accident prevention. The *share as main contributor* (SMC) presents the capability of a contributor to cause an accident possibly even alone (Kidam and Hurme, in press-c). The SMC is determined by dividing the frequency as main contributor by the overall frequency of the contributor.

Table 4 shows the SMCs of accident contributors for each equipment type. For example poor layout, which has the highest overall SMC, is on average 70% as a main contributor and only 30% as a sub contributor. However, SMC does not present

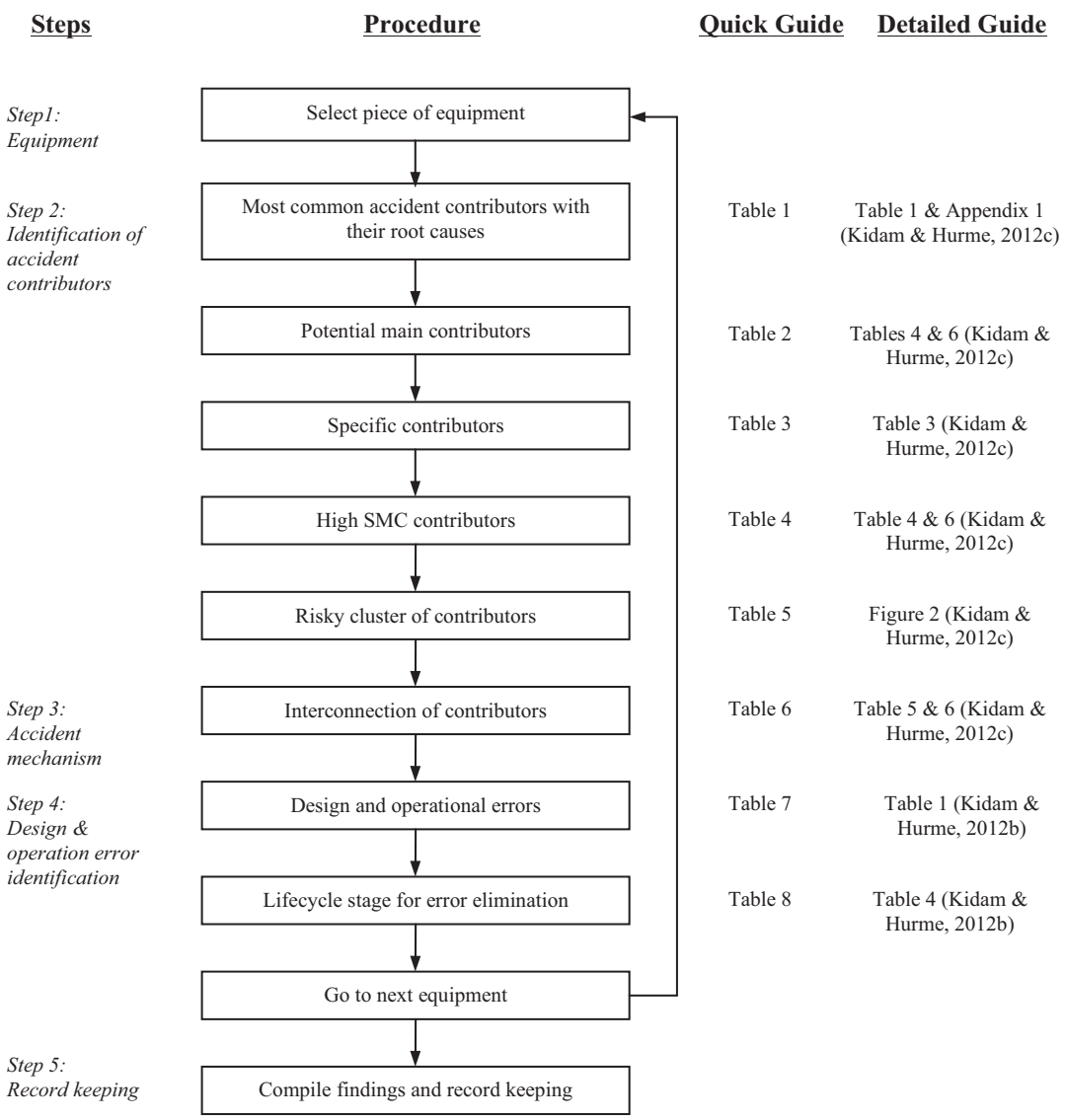


**Fig. 1 – Flow chart of the methodology.**

**Table 1 – Most common accident contributors of process equipment accidents (Kidam and Hurme, in press-c).**

| Types of equipment | Top three accident contributors with their root causes and frequencies |
|---|---|
| Piping system | - Human and organizational (41) – organizational failure – no/poor contractor control<br>- Fabrication, construction and installation (30) – poor work quality – incorrect setting<br>- Layout (25) – physical arrangement – wrong/incorrect positioning |
| Storage tank | - Human and organizational (36) – organizational failure – poor planning<br>- Flow-related (15) – layout – operator–technical interface error<br>- Heat transfer (10) – heat generation/accumulation – unwanted reaction |
| Reactor | - Heat transfer (17) – insufficient heat removal – low flow rate of cooling medium<br>- Reaction (17) – unfinished reaction – power failure; backup not available<br>- Contamination (12) – flow in – pressure difference |
| Separation equipment | - Contaminations (15) – waste oil – lack of detection and effect analysis<br>- Heat transfer (9) – hot spot – dried conditions<br>- Reaction (9) – unwanted reaction – process contaminations |
| Process vessel | - Contamination (14) – flow in – pressure different<br>- Human and organizational (12) – organizational failure – no double check on site<br>- Reaction (12) – unwanted reaction – process contaminations |
| Heat transfer eq. | - Human and organizational (12) – organizational failure – lack of inspection<br>- Contamination (11) – flow in – wall failure/crack<br>- Heat transfer (11) – hot spot – detailed internal structure error such as dead-end |

**Table 2 – The frequency of main-contributors in CPI accidents (Kidam and Hurme, in press-c).**

| Accident contributors | Piping system | Reactor | Storage tank | Process vessel | Heat transfer eq. | Separation eq. | Overall |
|---|---|---|---|---|---|---|---|
| Human and organizational | 12 | 7 | 13 | 5 | 5 | 4 | 46 |
| Contamination | 5 | 9 | 1 | 13 | 4 | 7 | 39 |
| Flow-related | 9 | 5 | 12 | 5 | 3 | 3 | 37 |
| Heat transfer | 7 | 12 | 4 | 4 | 4 | 3 | 34 |
| Layout | 19 | | 4 | 3 | 3 | 2 | 31 |
| Fabrication, construction and installation | 17 | 1 | 5 | 1 | 3 | | 27 |
| Reaction | | 16 | 1 | 2 | | 4 | 23 |
| Construction material | 13 | | 4 | 1 | 2 | 1 | 21 |
| Corrosion | 9 | 2 | 3 | 1 | 6 | | 21 |
| Utilities-related | 1 | | | | | 1 | 2 |
| External factors | | | 2 | | | | 2 |
| Static electricity | | | 1 | | | | 1 |
| Total | 92 | 52 | 50 | 35 | 30 | 25 | 284 |

**Table 3 – The relative frequency values of specific accident contributors for main equipment types (Kidam and Hurme, in press-c).**

| Equipment | Accident contributors | Times more common than average |
|---|---|---|
| Piping system | Erosion | 2.7 |
| | Vibration | 2.4 |
| | Fabrication/construction/installation | 1.9 |
| | Corrosion | 1.5 |
| | Layout | 1.5 |
| Storage tank | External factor | 4.0 |
| | Human and organizational | 1.7 |
| | Static electricity | 1.7 |
| | Mechanical failure | 1.5 |
| Reactor | Reaction-oriented | 2.7 |
| | Heat transfer | 2.0 |
| Heat transfer equipment | Construction material | 1.8 |
| | Corrosion | 1.8 |
| Process vessel | Static electricity | 2.1 |
| | Reaction-oriented | 2.0 |
| | Contamination | 1.6 |
| Separation equipment | Utility | 5.0 |
| | Contamination | 2.1 |
| | Reaction-oriented | 1.8 |

**Table 4 – Share of main contributors (SMC) as main accident contributor, % (Kidam and Hurme, in press-c).**

| Accident contributors | Reactor | Process vessel | Storage tank | Separation eq. | Heat transfer eq. | Piping system | Overall |
|---|---|---|---|---|---|---|---|
| Layout | | 60 | 67 | 67 | 75 | 76 | 70 |
| Fabrication, construction and installation | 50 | 100 | 100 | | 60 | 57 | 63 |
| Construction material | | 50 | 100 | 100 | 25 | 68 | 57 |
| Corrosion | 67 | 100 | 75 | | 75 | 41 | 55 |
| Flow-related | 83 | 50 | 80 | 38 | 33 | 39 | 52 |
| Contamination | 75 | 93 | 17 | 47 | 36 | 29 | 52 |
| Utilities-related | | | | 50 | | 50 | 50 |
| Heat transfer | 71 | 50 | 40 | 33 | 36 | 41 | 47 |
| Reaction | 94 | 17 | 33 | 44 | | | 43 |
| Human and organizational | 7 | 40 | 36 | 44 | 42 | 29 | 38 |
| External factor | | | 22 | | | | 15 |
| Static electricity | | | 17 | | | | 5 |
| Average | 69 | 49 | 46 | 42 | 41 | 39 | 46 |

**Table 5 – Cluster of high-risk accident contributors (cluster 1 in Kidam and Hurme, in press-c).**

| Equipment | Contributors |
|---|---|
| Reactor | Reaction, heat transfer, and contamination |
| Storage tank | Flow-related |
| Heat transfer eq. | Corrosion and human and organizational |
| Process vessel | Contamination, flow-related and heat transfer |
| Separation eq. | Contamination, human and organizational and reaction |
| Piping system | Layout, fabrication construction and installation, construction material, corrosion, flow-related, and heat transfer |

the frequency, therefore some of the high SMC contributors may occur rarely. Therefore, Kidam and Hurme (in press-c) analyzed accident contributors based on both their frequency and SMC. A *cluster of risky contributors* was identified in which the contributors have both high frequency and high SMC (i.e. cluster 1 in their study). These high-risk contributors, which are frequent and often act as main-contributors, are summarized in Table 5.

### 3.2. *Detection of potential accident mechanism*

Certain accident contributors have a tendency to act together, as found by Kidam and Hurme (in press-c) and summarized in Table 6. These interconnections can be used for detecting accident mechanisms in Step 3. For example, a strong relationship between flow-related and human and organizational errors can be seen for storage tanks (20%) in Table 6, while in pressure vessel failures, the strongest relationship is found between contamination and reaction (14%). The percentages show the level of interaction between contributors; e.g. for vessels, 14% of accident main-contributors have contamination as main-contributor and reaction as sub contributor.

### 3.3. *Identification of design and operation errors*

In Step 4, typical design and operation errors and their timing in the plant lifecycle are identified. The aim is to prevent the same errors from being repeated. Organizations tend to forget learning from accidents because people move on and retire. Kidam and Hurme (in press-b) found that design errors contribute to nearly 80% of accidents. This value is based on a wide definition of design error, which only excludes operation-related human and organizational errors and external factors.

The *design and operation error identification* is based on the statistical frequency of errors for different equipment types. A summary of the three most frequent errors for the main types of process equipment is presented in Table 7. The full error ranking was presented by Kidam and Hurme (in press-b).

For identifying the right *timing* for error elimination, the accident contributors are linked to the process design lifecycle by identifying their time of occurrence during design and operation activities (Kidam and Hurme, in press-b). This can be done based on the statistics of the time of the error made, as shown in Table 8.

Table 8 shows that the design of each equipment type has unique accident contributors and a specific time of occurrence during a design project. The design error timing points out the time in the plant lifecycle when accident contributor elimination should be done. Therefore the analysis provides guidelines on how to identify and eliminate common accident contributors early. This is important since process changes at an early stage of plant design are much easier and cheaper than later changes.

In the method presented in Fig. 1, evaluation continues until accident contributors for all the process equipment and piping have been identified. In Step 5, the results are compiled and the accident contributors and improvements are listed. The design error and accident contributor statistics referred to also provide ideas on appropriate hazard elimination and risk reduction strategies. This can be done by using a hierarchy of control such as inherently safer, add-on engineered and procedural levels.

## 4. Bhopal case study

The method proposed is demonstrated and tested herein by the Bhopal case study. The Bhopal gas tragedy was the worst industrial accident in the world, killing over 2000 persons immediately and injuring more than 200,000 people at the Union Carbide plant in Bhopal, India in 1984.

In the process, methyl isocyanate (MIC) was an intermediate for producing a pesticide. Chemically, MIC is a toxic, reactive, volatile, and flammable substance. The MIC storage tank (T610) was contaminated by water through the overhead pressure venting system.

MIC reacts with water in an exothermic way. The reaction is catalyzed by rust and other compounds. Water flowed into intermediate storage tank T610, probably because of errors in water washing operation and piping layout. A runaway reaction occurred resulting in high temperature, vaporization of MIC and high pressure activating a safety valve. Due to multiple failures of the protection system (detector, alarm, gas scrubber, flare, etc.), a large amount of MIC gas leaked. The leaked gas spread towards the city zone, covering residential areas and causing multiple casualties (Chouhan, 2005; Mannan, 2005).

### 4.1. *Method application and results*

The method presented is applied below to MIC storage tank T610. Although T610 was a storage tank, its function, structure and operation resemble more a process vessel. Therefore, the equipment types selected to represent tank T610 were pressure vessel and storage tank. The piping system was also analyzed. Here, the detailed assessment is demonstrated for the process vessel only. The analysis results are presented in Table 9 based on the following (please refer to Fig. 1):

- Step 1: The *Equipment* type selected to represent T610 is process vessel.
- Step 2a: As seen from Table 1, among typical *accident contributors* are contamination (14 cases) caused by flow-in (8 cases) due to the human–technical interface (4). Second is human and organizational (12) due to organizational failures (10) that overlook the needs for procedure to double-check the operation on site (3). Third is reaction (12) by unwanted chemical reaction (9) due to process

**Table 6 – The interconnections between main and sub contributors of accidents for each equipment type (% of main contributors).**

| Equipment | Interconnection level | |
|---|---|---|
| | Largest | Others |
| Piping | • Layout to: Human and organizational, 9% | • Flow-related to: Human and organizational, 7%<br>• Layout to: Contamination, 8%; flow-related, 5%<br>• Fabrication, construction and installation to: Mechanical failure, 5%; vibration, 7%<br>• Construction material to: Corrosion, 8% |
| Storage tank | • Flow-related to: Human and organizational, 20% | • Human and organizational to: Heat transfer, 6%<br>• Heat transfer to: Human and organizational, 6%<br>• Construction material to: Static, 6%; human and organizational, 6%<br>• Fabrication, construction and installation to: External factor, 6%<br>• Layout: Human and organizational, 6% |
| Reactor | • Reaction to: Heat transfer, 10% | |
| Process vessel | • Contamination to: Reaction, 14% | • Contamination to: Human and organizational, 9%<br>• Heat transfer to: Reaction, 11% |
| Heat transfer eq. | • Corrosion to: Contamination, 10%; construction material, 10%<br>• Human and organizational to: Flow-related, 10% | |
| Separation equipment | • Contamination to: Human and organizational, 12%<br>• Reaction to: Heat transfer, 12% | |

contamination (3). Their detailed root causes can be identified as presented by Kidam and Hurme (in press-c).

- Step 2b: The *main contributors* to the Bhopal tragedy from the vessel point of view can be identified using Table 2. These are contaminations (13), flow-related (5), human and organizational (5), and heat transfer (4) aspects.
- Step 2c: The *specific contributors* are identified using Table 3, where process hazards such as static electricity (2.1 times more the average), reaction (2.0 times) and contamination (1.6) are recognized for a vessel.
- Step 2d: According to Table 4, the *high SMCs* for a vessel are corrosion (100%), fabrication/construction/installation (100%) and contamination (93%).
- Step 2e: The most *risky contributors* for vessel are contamination, flow-related and heat transfer aspects as listed in Table 5.
- Step 3: The *accident mechanisms* for a vessel failure are related to the strong relation between contamination – reaction (14%), heat transfer – reaction (11%) and contamination – human and organizational aspects (9%) as seen from Table 6.
- Step 4a: The *design and operation errors* are identified through Table 7. The common faults for a process vessel are:
  - reactivity and incompatibility (29 cases) – reaction with contaminants;
  - protection (19) – lack of ignition source control; and
  - process condition (15) – reaction with contaminants.

**Table 7 – Most frequent design and operation errors and their root causes (Kidam and Hurme, in press-b).**

| Types of equipment | Most common errors |
|---|---|
| Reactor | • Reactivity/incompatibility (17) – reactive/incompatible with heat transfer medium<br>• Process condition (16) – no or unknown safe limit of trace chemical or contaminants<br>• Utility set-up (13) – higher heating/cooling capacity selected versus as needed |
| Storage tank | • Organizational failure (25) – poor planning and lack of maintenance<br>• Protection (17) – no or inadequate nitrogen blanket<br>• Unsuitable parts (13) – sampling tools that accumulate/discharge static electricity |
| Heat transfer equipment | • Process condition (13) – corrosive environment created by contaminants<br>• Organizational failure (8) – lack of inspection/testing<br>• Protection (7) – inadequate static electricity control |
| Process vessel | • Reactivity/incompatibility (29) – reaction with contaminants<br>• Protection (19) – lack of ignition source control (i.e. non-explosion-proof equipment)<br>• Process condition (15) – reaction with contaminants |
| Separation equipment | • Process condition (25) – reactive by-product/impurities that are accumulated/concentrated in the process<br>• Reactivity/incompatibility (22) – reaction with contaminants<br>• Utility set-up (11) – inadequate cooling capacity (i.e. natural cooling) |
| Piping system | • Layout (44) – physical arrangement and shape errors<br>• Materials of construction (37) – less than adequate mechanical strength<br>• Organizational failure (26) – poor contractor management and lack of maintenance |

**Table 8 – Points-to-look-for list of design and operation errors (Kidam and Hurme, in press-b).**

| Equipment | Piping system | Storage tank | Reactor | Process vessel | Separation eq. | Heat transfer eq. | All |
|---|---|---|---|---|---|---|---|
| Process R&D and pre-design | - Process contaminations, 6 | | - Reaction with contaminants, 4<br>- Process contaminations, 3<br>- Uneven flow/dry condition, 3<br>- Reactive heat transfer medium, 3 | - Reaction with contaminants, 6<br>- Secondary reaction, 6<br>- Process contaminations, 6<br>- Hazardous material generated, 4<br>- High temperature, 3<br>- Waste handling, 3 | - Process contaminants, 7<br>- Reaction with contaminants, 7<br>- Secondary reaction, 7 | - Process contaminations, 3 | - Process contaminants, 26<br>- Reaction with contaminants, 17<br>- Secondary reaction, 13 |
| Basic Engineering | - Mechanical specification, 13<br>- Chemical specification, 11<br>- Physical arrangement, 9<br>- Sizing/thickness, 7<br>- Shared piping, 4<br>- Single valve, 3 | - Physical arrangement, 3<br>- Friction/impact, 3<br>- Flammable sealing/cleaning agent, 3 | - Extreme heating/cooling source, 4<br>- Physical arrangement 4<br>- Chemical resistance spec, 3<br>- Lack of detection by automation, 3 | - Friction/impact, 3<br>- Physical arrangement, 3 | - Incompatible heat transfer medium, 3<br>- Utility set-up: various | - Incompatible heat transfer medium, 3<br>- Single valve, 2 | - Mechanical and chemical specification, 27<br>- Physical arrangement, 19<br>- Sizing, 7<br>- Incompatible heat transfer medium, 6 |
| Detailed Engineering | - Physical arrangement, 9<br>- Dead end, 8<br>- Support arrangement, 5<br>- U-shape, 5<br>- Flow restriction, 3 | - Spark generated parts, 9<br>- No nitrogen blanket, 8<br>- Static electricity, 7<br>- Non-conductive part, 6 | - Setting error, 4<br>- No nitrogen blanket, 4<br>- Feeding mechanism, 4<br>- Maintenance/repair (operating manual), 3 | - Non-explosion proof, 4<br>- Static electricity, 4<br>- No nitrogen blanket, 3 | - Static electricity, 3<br>- No nitrogen blanket, 2<br>- Sensor failed, 2 | - No nitrogen blanket, 2<br>- Static electricity, 2 | - No nitrogen blanket, 19<br>- Static electricity, 19 |
| Construction and start-up | - Bolt tightening related, 2<br>- Poor fabrication/construction quality, 2 | - Stress concentrated, 3 | - Welding defect, 2 | - Poor fabrication/construction quality, 3 | | - Stress concentrated, 4 | - Mechanical stress, 7<br>- Poor fabrication/construction quality, 5 |
| Operations | - Contractor mgt/control, 5<br>- Lack of maintenance, 5<br>- No double and physical check, 4<br>- Work permit, 3<br>- Poor mgt system, 3<br>- No problem reporting system, 3 | - Poor planning, 5<br>- Lack of maintenance, 5<br>- Lack of analysis, 4<br>- Misjudgement, 4<br>- Not follow procedure, 4<br>- No double and physical check, 4 | - Lack of analysis, 3<br>- No double and physical check, 2 | - No double and physical check, 3<br>- Lack of analysis, 2 | - No double and physical check, 2<br>- Not follow procedure, 2 | - Not follow procedure, 3<br>- Lack of inspection/testing, 2 | - No double and physical check, 15<br>- Lack of maintenance/inspection/testing, 12<br>- Lack of analysis, 9<br>- Not follow procedure, 9 |
| Modification | | | Various, 11 | | | Various, 5 | |

*Note*: The number shows the accident contributor frequency.

**Table 9 – Results for Bhopal T610 analysis as a pressure vessel.**

| Steps | Testing parameters | Findings |
|---|---|---|
| 1 | Equipment types | Process vessel |
| 2a | Accident contributors (Table 1) | a. Contamination, 14 cases – flow-in, 8 cases; human/technical interface, 4 cases<br>b. Human and organizational, 12 – organizational failure, 10; no procedure, 3<br>c. Reaction, 12 – unwanted reaction, 9; contamination, 3<br>d. Flow-related, 10 – human/technical interface, 3 |
| 2b | Main contributors, MC (Table 2) | a. Contamination, 13<br>b. Flow-related, 5<br>c. Human and organizational, 5<br>d. Heat transfer, 4 |
| 2c | Specific contributors (Table 3) | a. Static electricity, 2.1 times more than average<br>b. Reaction, 2.0<br>c. Contamination, 1.6 |
| 2d | High, SMC (Table 4) | a. Corrosion, 100%<br>b. Fabrication/construction/installation, 100%<br>c. Contamination, 93% |
| 2e | Cluster analysis (Table 5) | a. Contamination<br>b. Flow-related<br>c. Heat transfer |
| 3 | Accident mechanism (Table 6) | a. Contamination – reaction, 5<br>b. Heat transfer – reaction, 4<br>c. Contamination – human and organizational, 3 |
| 4a | Design and operation faults (Table 7) | a. Reactivity/incompatibility, 29 – reaction with contaminants, 6<br>b. Protection, 19 – lack of ignition source control, 11<br>c. Process condition, 15 – reaction with contaminants, 6 |
| 4b | Lifecycle location (Table 8) | a. R&D and preliminary design – reaction with contaminants, 6; secondary reaction, 6; contamination, 6; hazardous material and heat generation, 4; high temperature, 3<br>b. Basic design – physical arrangement, 3<br>c. Detailed design – non-explosion-proof, 4; static electricity, 4 |

– Step 4b: The *lifecycle* aspects of vessel design and operation are reviewed based on Table 8. As seen from the table, the focus for error elimination is in the R&D and preliminary design steps, since the reaction and chemical incompatibility aspects, which are the most frequent errors made, are decided in these stages.

The results are summarized in Table 9. In the contributor category, contamination (14 cases) was the largest accident contributor, identified with its largest root cause 'flow-in' which was due to human–technical interface problems and pressure difference. In second place was the reaction contributor (12) with its root cause 'unwanted reaction', which was due to contamination. The contribution of contamination and reaction were large also in main-contributors, relatively high contributors and SMCs aspects. The mechanism of the accident proposed by the interconnection study (Step 3) was therefore: human and organizational aspects – contamination – reaction – heat transfer problems.

Based on the findings above, the vessel-based assessment strongly points to contamination as the major accident contributor and its connection to an unwanted chemical reaction in the vessel. Further, the result shows that these accident contributors should be identified and controlled at the early stage of a design project i.e. at the research and development and preliminary engineering stages.

### 4.2. *Analysis of results*

The accident contributors were analyzed using the equipment types 'tank' and 'vessel' for T610. The related piping was also analyzed. The results are compared in Table 10 with the actual Bhopal accident contributors. These were extracted from the data of Chouhan et al. (2004) and Chouhan (2005). Also the critical accident contributors for each piece of equipment were identified from their data and presented as underlined in Table 10.

If the analysis method found the contributor, it is marked X. If the finding was not at the top of the contributor Tables 1–8, the mark is in brackets (X). The actual critical accident contributors are underlined. Note that different critical contributors were selected for the piping and the vessel/tank. If the contributor was not found by the method, it is marked O. The non-relevant contributors to each piece of equipment analyzed are marked –.

Table 10 shows that for piping, the relevant accident contributors and faults were found. Also, the accident mechanism is well predicted. In the 'tank' analysis, the contamination was not found as a contributor, neither were the inventory aspect as a design error and procedures as operating errors. For the 'vessel', all contributors were found but two of them are weak. Inventory as a design error was not found, nor were procedures as an operating error. The accident mechanism is only partly predicted in the tank option whereas the vessel option gives a better prediction.

**Table 10 – Comparison of the method results with the real accident.**

| Accident causes | Found by method | | |
|---|---|---|---|
| | Piping | Storage tank | Process vessel |
| *Contributors* | | | |
| a. Connectivity and layout | X | – | – |
| b. Material of construction | (X) | – | – |
| c. Corrosion | X | X | – |
| d. Flow related/flow-in | X | X | (X) |
| e. Human and organizational | X | O | X |
| f. Contamination | – | X | X |
| g. Heat transfer | | (X) | (X) |
| h. Reaction | | | X |
| *Design faults* | | | |
| a. Jumper line | X | – | – |
| b. Wrong construction material | X | – | – |
| c. Valves | (X) | – | – |
| d. Contaminant/reaction | – | (X) | X |
| e. Inventory/size | – | O | O |
| *Operational faults* | | | |
| a. Maintenance | X | X | (X) |
| b. Work permits | X | (X) | X |
| c. Procedures | X | O | O |
| e. Not follow procedure | X | X | X |
| f. Training | X | (X) | (X) |
| *Accident mechanism* | | | |
| - Human and organizational (HO) | L–HO: strong | F–HO: strong | C–R: strong |
| - Layout (L) | L–C: strong | H–HO: moderate | H–R: strong |
| - Flow related (F) | L–F: strong | | C–HO: moderate |
| - Contamination (C) | F–HO: strong | | |
| - Reaction (R) | M–C: strong | | |
| - Heat transfer (H) | (L–R): weak | | |
| - Material of construction (M) | | | |

*Note*: X, high frequency; (X), low frequency; –, not relevant; O, did not found; underlined, actual critical contributors.

**Table 11 – Comparison of predicted accident parameters with the real ones (%).**

| Accident parameters | (1) Piping system | (2) Process vessel | (3) Storage tank | Average 1 and 2 | Average 1, 2 and 3 |
|---|---|---|---|---|---|
| Contributors | 100 | 100 | 70 | 100 | 90 |
| Design faults | 85 | 50 | 30 | 68 | 55 |
| Operational faults | 100 | 60 | 60 | 80 | 73 |
| Accident mechanism | 90 | 75 | 50 | 83 | 72 |
| Critical contributor (underlined in Table 10) | 100 | 100 | 50 | 100 | 83 |
| Average | 95 | 77 | 52 | 86 | 75 |

Table 11 summarizes the prediction capability of the method in numeric form. Piping is predicted best, at 95% on average. The storage tank option is the worst, at approximately 50%, because T610 was not a normal storage tank. The average prediction capability is 86% for piping and vessel, and 75% if tank is included as an option. The accident contributors were the best predicted aspect with 90–100% accuracy.

## 5. Discussion and conclusions

The current approach of loss prevention in the CPI mainly utilizes outer layers of protection, which are organizational and human-oriented. Based on accident analyses however, the contribution of technical and design factors to accidents is significant (Taylor, 2007a). Each accident has on average 2.3 non-operations related (i.e. technical) contributors (Kidam and Hurme, in press-a). These design-oriented faults should be addressed through design changes, not through procedural changes or by asking workers to be more careful at work.

Current design-oriented safety methods have limitations in their applicability. Many of them, e.g. Hazop, are not fully applicable in the early stages of plant design and instead act often as a final check when the process design is done. However, no significant design changes can be made at this point due to economic factors. Therefore most of the risk reduction is often achieved using add-on safety systems.

The main drawback of current design methods is that knowledge available from earlier accidents is largely ignored, nor are there any methods utilizing this knowledge. As a result, similar accidents tend to recur. In addition the current safety methods are often used in such a way that they do not fully support the design process or guide the process engineer to design a safer chemical plant. Thus, the opportunity and

benefits of detecting and eliminating process hazards at an early stage of plant design cannot be fully utilized.

A new method to support the design process is needed. This paper presents a method for identification of accident contributors and design and operation errors. Their causes and the timing of erroneous design are also shown. The identification is done using several techniques based on accident and design error statistics derived from a database of earlier accidents. The identification is based on the most frequent accident contributors, main contributors and uncommon but specific contributors, which are capable of causing accidents alone. The accident mechanism is analyzed through the interconnection of contributors. Frequent design and operation errors and their lifecycle timing are pointed out to show the design stage where action should be taken to eliminate the accident contributor.

The method has been demonstrated and tested using the Bhopal tragedy case study. The method successfully identified the accident contributors, pointed out common design and operating errors and the time when design improvements should be implemented during the process lifecycle. On average, the proposed method can predict up to 85% of accident contributors and design and operation errors if the type of equipment is selected correctly. This may be the main problem with the method, when the process includes unconventional or novel types of equipment, which are not available in earlier accident information.

In conclusion, the identification method proposed has several advantages that overcome some of the limitations of current design/safety methods. However, it is not meant to substitute but to supplement methods such as Hazop that are used commonly in design. The most important feature of the method is that it identifies accident contributors and potential design errors and gives the designer ideas on their removal throughout a design project. The safety analysis can start early and hazards be controlled earlier in the plant lifecycle by utilizing inner layers of protection. As a result, cost and safety benefits can be achieved as a result of early process design changes.

## References


Chouhan, T.R., Alvares, C., Jaising, I., Jayaraman, N., 2004. Bhopal: The Inside Story, 2nd ed. The Apex Press, Goa, India.

Chouhan, T.R., 2005. The unfolding of the Bhopal disaster. J. Loss Prevent. Process Ind. 18 (4–6), 205–208.

Crawley, F., Tyler, B., 2003. Hazard Identification Methods. IChemE, Rugby.

Crowl, D.A., Lauvar, J.F., 2011. Chemical Process Safety—Fundamentals with Applications, 3rd ed. Pearson Education Inc., New Jersey.

Duguid, I.M., 2001. Take this safety database to heart. Chem. Eng. 108 (7), 80–84.

Drogaris, G., 1993. Learning from major accidents involving dangerous substances. Saf. Sci. 16, 89–113.

FKD, 2011. Failure Knowledge Database. http://www.sozogaku.com/fkd/en/ (available online 29.05.11).

Hendershot D.C., 2011. Inherently Safer Design: An Overview of Key Elements, Professional Safety, The American Society of Safety Engineers', http://findarticles.com/p/articles/mi_hb5618/is_201102/ai_n57036565/?tag =content;col1.

Hurme, M., Rahman, M., 2005. Implementing inherent safety throughout process lifecycle. J. Loss Prevent. Process Ind. 18, 238–244.

Khan, F.I., Abbasi, S.A., 1998. Techniques and methodologies for risk analysis in chemical process industries. J. Loss Prevent. Process Ind. 11, 261–277.

Khan, F.I., Amyotte, P.R., 2003. How to make inherent safety practice a reality. Can. J. Chem. Eng. 81, 2–16.

Kidam, K., Hassim, M.H., Hurme, M., 2008. Enhancement of inherent safety in chemical industry. Chem. Eng. Trans. 13, 287–294.

Kidam, K., Hurme, M. Design as a contributor to chemical process accidents. J. Loss Prevent. Process Ind., in press-a.

Kidam, K., Hurme, M. Origin of equipment design and operation errors. J. Loss Prevent. Process Ind., in press-b.

Kidam, K., Hurme, M. Analysis of equipment failures as contributors to chemical process accidents. Process Saf. Environ. Prot., in press-c.

Kletz, T.A., 1993. Lessons From Disaster: How Organizations Have No Memory and Accidents Recur. IChemE, Rugby, UK.

Kletz, T.A., 2010. An obituary: ICI's contribution to process safety and why it came to an end. J. Loss Prevent. Process Ind. 23 (6), 954–957.

Krishnan, G.U., 2005. What Hazop studies cannot do. Hydrocarb. Process. (Oct), 93–95.

Lindberg, A.-K., Hansson, S.O., Rollenhagen, C., 2010. Learning from accidents—what more do we need to know? Saf. Sci. 48 (6), 714–721.

Mannan, M.S., 2005. Lee's Loss Prevention in Process Industry, vol. 1., 3rd ed. Elsevier-Butterworth Heinemann, Burlington.

Marhavilas, P.K., Koulouriotis, D.E., 2008. A risk-estimation methodological framework using quantitative assessment techniques and real accidents' data: Application in an aluminum extrusion industry. J. Loss Prevent. Process Ind. 21 (6), 596–603.

Marhavilas, P.K., Koulouriotis, D., Gemeni, V., 2011a. Risk analysis and assessment methodologies in the work sites: on a review, classification and comparative study of the scientific literature of the period 2000–2009. J. Loss Prevent. Process Ind. 24 (5), 477–523.

Marhavilas, P.K., Koulouriotis, D.E., Mitrakas, C., 2011b. On the development of a new hybrid risk assessment process using occupational accidents' data: application on the Greek Public Electric Power Provider. J. Loss Prevent. Process Ind. 24 (5), 671–687.

Meel, A., O'Neill, L.M., Levin, J.H., Seider, W.D., Oktem, U., Keren, N., 2007. Operational risk assessment of chemical industries by exploiting accident databases. J. Loss Prevent. Process Ind. 20 (2), 113–127.

Niemitz, K.J., 2010. Process safety culture or what are the performance determining steps? In: Workshop on Safety Performance Indicators, Ispra, 17–19th March.

OECD, 2005. Report of the OECD Workshop on Lessons Learned from Chemical Accidents and Incidents. Organisation for Economic Co-operation and Development, Number 14, 21–23 September 2004. Karlskoga, Sweden.

Pasman, H.J., 2010. Will a safe process be sufficient or do we have to do a bit more? In: 13th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, vol. 1, Bruges, June 6–9, pp. 17–21.

Prem, K.P., Ng, D., Mannan, M.S., 2010. Harnessing database resources for understanding the profile of chemical process industry incidents. J. Loss Prevent. Process Ind. 23 (4), 549–560.

Seider, W.D., Seader, J.D., Lewin, D.R., Widagdo, S., 2009. Product and Process Design Principles: Synthesis, Analysis and Design, 3rd ed. John Wiley & Son, Inc., USA.

Taylor, J.R., 2007a. Statistics of design error in the process industries. Saf. Sci. 45 (1), 61–73.

Taylor, J.R., 2007b. Understanding and combating design error in process plant design. Saf. Sci. 45 (1), 75–105.

Tixier, J., Dusserre, G., Salvi, O., Gaston, D., 2002. Review of 62 risk analysis methodologies of industrial plants. J. Loss Prevent. Process Ind. 15, 291–303.