Department of Biotechnology and Chemical Technology

Process Safety Enhancement in Chemical Plant Design by Exploiting Accident Knowledge

Kamarizan Bin Kidam

Aalto University

DOCTORAL
DISSERTATIONS

Aalto University publication series
DOCTORAL DISSERTATIONS 168/2012

Process Safety Enhancement in Chemical Plant Design by Exploiting Accident Knowledge

Kamarizan Kidam

Doctoral dissertation for the degree of Doctor of Science in Technology to be presented with due permission of the School of Chemical Technology for public examination and debate in Auditorium (Forest Products Building 2) at the Aalto University School of Chemical Technology (Espoo, Finland) on the 14th of December, 2012, at 12 noon.

Aalto University
School of Chemical Technology
Department of Biotechnology and Chemical Technology
Plant Design

Supervising professors
Professor Dr. Markku Hurme
Professor Dr. Jukka Koskinen

Preliminary examiners
Professor Dr. J. P. Gupta,
Rajiv Gandhi Institute of Petroleum Technology,
India.

Dr. David W. Edwards,
Senior Safety Consultant,
Granherne - KBR, UK.

Opponents
Professor Dr. Ilkka Turunen,
Lappeenranta University of Technology,
Finland.

Dr. Anna-Mari Heikkilä,
Senior Scientist,
VTT Technical Research Centre of Finland, Finland.

Aalto University publication series
DOCTORAL DISSERTATIONS 168/2012

ISBN 978-952-60-4909-0 (printed)
ISBN 978-952-60-4910-6 (pdf)
ISSN-L 1799-4934
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)
http://urn.fi/URN:ISBN:978-952-60-4910-6

Unigrafia Oy
Helsinki 2012

Finland

NORDIC ECOLABEL
441 697
Printed matter

A! Aalto University

Abstract

Aalto University, P.O. Box 11000, FI-00076 Aalto www.aalto.fi

Author
Kamarizan Kidam

Name of the doctoral dissertation
Process Safety Enhancement in Chemical Plant Design by Exploiting Accident Knowledge

Publisher Aalto University School of Chemical Technology

Unit Department of Biotechnology and Chemical Technology

Series Aalto University publication series DOCTORAL DISSERTATIONS 168/2012

Field of research Plant Design

Manuscript submitted 28 August 2012 **Date of the defence** 14 December 2012

Permission to publish granted (date) 30 October 2012 **Language** English

□ **Monograph** ☒ **Article dissertation (summary + original articles)**

Abstract

The accident rate in the chemical industry has not been decreasing although they could be prevented by using the existing knowledge. The aim of this thesis is to enhance the utilization of knowledge from earlier accidents especially in the designing of chemical plants. The experience feedback on accidents is improved by analyzing and disseminating knowledge on accident contributors to design activities. The research was done by analyzing the 364 chemical process accident reports available in the Failure Knowledge Database (FKD).

It was found that the technical contributors (79%) dominated the accidents in the CPI. Deeper analyses were carried out to identify the accident contributors, and design and operation errors for the six most common equipment types of accidents. The other indicators of accidents included in the study were; the contributors share as main contributor (SMC), equipment specific contributors, and the combination of high SMC and frequency.

In design and operation errors analyses, the study found that about 80% of the accident cases were contributed by at least one design error with an average of 2.3 errors per accident. The timing of the errors was analyzed and it shows that about half (47%) of the design and operation errors were made during the process design-oriented stages. Thus, more focus should be given in the making of fundamental decisions such as process conditions, chemicals and reactions during the early phases of the design.

The corrective actions proposed in accident reports employed typically the outer layers of protection such as procedural changes (53% of cases) even though the design errors are generally dominant. The inherently safer design proposed was only 18% of cases; and these were based on the most used principles which were ’error tolerance’ and ‘moderate’.

Current design oriented safety methods do not fully utilize knowledge from earlier accidents and therefore do not facilitate learning. For example, HAZOP is often employed only as a final check and do not support the designer during the work. Therefore the thesis proposed a method for identification of accident contributors and design errors throughout the design stages by utilizing knowledge from earlier accidents. The method is based on information obtained from accident contributors and design errors discovered which will be presented in the first part of this thesis. The aim is to show also their mechanisms and time of creation. The proposed method would support the design process by having an early design error detection and elimination through design changes. Therefore, cost and safety benefits can be achieved by undergoing changes in the earlier stages of plant design. The Bhopal tragedy is used as the case study to demonstrate and test the method. The proposed method could be used to predict an average of up to 85% of accident contributors.

Keywords experience feedback, accident contributor, plant design, process lifecycle

ISBN (printed) 978-952-60-4909-0 **ISBN (pdf)** 978-952-60-4910-6

ISSN-L 1799-4934 **ISSN (printed)** 1799-4934 **ISSN (pdf)** 1799-4942

Location of publisher Espoo **Location of printing** Helsinki **Year** 2012

Pages 170 **urn** http://urn.fi/URN:ISBN:978-952-60-4910-6

Preface

First and foremost, I would like to raise my thanks to God, the Most Gracious, the Most Merciful.

This work was carried out between August 2007 and September 2012 in the Plant Design research unit, Department of Biotechnology and Chemical Technology, Aalto University. The financial support from the Ministry of Higher Education, Malaysia and Universiti Teknologi Malaysia, as well as the research supports from Aalto University, Ella and Georg Ehrnrooth Foundation and The Finnish Work Environment Fund are gratefully acknowledged.

I would like to thank my supervisors, Professor Markku Hurme and Professor Jukka Koskinen, for their support, guidance and encouragement during this study. Without their contribution, this work would not have been possible. I am also grateful to Professor Dr. J. P. Gupta and Professor Dr. David W. Edwards for reading the thesis manuscript and I appreciate their valuable comments. I would also like to thank all of my colleagues and the laboratory staff for providing a positive and pleasant working environment.

Finally, I would like to thank my parents and family for their unconditional support and encouragement. My work is dedicated to my beloved wife, Hariyani Mohamed and my daughters for their love, patience and understanding. Thank you very much.

Espoo, November 2012

Kamarizan Bin Kidam

List of Publications

The thesis is based on the compilation of the following publications, which are referred by the corresponding numbers:

I. Kidam, K., Hurme, M., Statistical analysis of contributors to chemical process accidents, *Chemical Engineering & Technology*, ***accepted for publication.***

II. Kidam, K., Hurme, M., Analysis of equipment failures as contributors to chemical process accidents, *Process Safety and Environmental Protection*, ***In Press,*** *Available online 18 February 2012,* doi:10.1016/j.psep.2012.02.001

III. Kidam, K., Hurme, M., Design as a contributor to chemical process accidents, *Journal of Loss Prevention in the Process Industries*, Volume 25, Issue 4, July 2012, Pages 655–666.

IV. Kidam, K., Hurme, M., Origin of equipment design and operation errors, *Journal of Loss Prevention in the Process Industries*, Volume 25, Issue 6, November 2012, Pages 937–949.

V. Kidam, K., Hurme, M., Method for identifying contributors to chemical process accidents, *Process Safety and Environmental Protection*, ***In Press****, Available online 20 August 2012, doi.org/10.1016/j.psep.2012.08.002*

VI. Kidam, K., Hurme. M. and Hassim, M.H., Inherent safety based corrective actions in accident prevention. In *Proceedings of 13th International Symposium on Loss Prevention*, Bruges, Belgium, Jun 6 – 9th, 2010, Vol. 2, pp 447-450.

Author’s Contribution

I. The author carried out the accident analysis and wrote the paper with the co-author

II. The author carried out the equipment accident analysis and wrote the paper with the co-author.

III. The author carried out the design error analysis and wrote the paper with the co-author.

IV. The author carried out the process lifecycle analysis of the accident cases and wrote the paper with the co-author.

V. The author developed the safety method and wrote the paper with the co-author.

VI. The author carried out the corrective actions analysis and wrote the paper with the co-authors.

Abbreviations

CBR	Case-based reasoning
CBS	Chemical Safety and Hazard Investigation Board
CCPS	Center for Chemical Process Safety
CEI	Dow Chemical Exposure Index
CIMAH	Control of Industrial Major Accident Hazards Regulation 1999
CPI	Chemical process industry
ETA	Event Tree Analysis
EU	European Union
F&EI	Dow Fire and Explosion Index
FACTS	Failure and Accidents Technical Information Systems
FKD	Failure Knowledge Database
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
H&O	Human and organizational
HAZOP	Hazard and Operability Study
HSE	Health and Safety Executive
IRIS	Accident Reporting Information System
ISD	Inherently safer design
JST	Japan Science and Technology Agency
LOP	Layer of protection
LOPA	Layer of Protection Analysis
MARS	Major Accident Reporting System
MC	Main contributor
MHIDAS	Major Hazard Incident Data Service
MIC	Methyl isocyanate
NRC	National Response Center
OECD	Organization for Economic Co-operation and Development
PUPAD	Pondicherry University Process-industry Accident Database

QRA	Quantitative Risk Assessment
R&D	Research and Development
SMC	Share as main contributors
SMS	Safety management system
TNO	Netherlands Organization for Applied Scientific Research

Table of Contents

1 Introduction

1.1 Background

In the last decade, considerable resources have been used for creating accident reporting systems. The aim of these systems was to collect accident information that would provide a better understanding on the causes of accidents and to create lessons learned as well as make recommendations for accident prevention. However, major accidents still occur in the chemical process industry (CPI). The accident rate in the CPI has been increasing or is still a constant phenomena in the USA (Prem et al., 2010), in Asia (Hasegawa, 2004; He et al., 2011) and also in Europe (Niemitz, 2010). It seems that the current safety management and design methods are insufficient to prevent accidents in the CPI. Further improvements in the process safety and design are still needed.

The safety problems are related to the *changes in the industry*. The level of risk has increased in the CPI in the last decade due to the complexity of operations (Qi et al., 2011). At the same time, the problems could be due to the economic downturn and tight competition, major restructuring and cost cutting programs which are being implemented for the companies/plants to remain competitive. These factors have led to outsourcing and increased workload. At the same time, the safety knowledge within the organization is drained-off due to staff restructuring, retirement etc. All of these factors influence the safety performance by eroding the safety margins which were in the design and operation in the beginning. The capability of process to maintain functioning in a safe state after a disturbance can be called 'resilience'. The gradual changes are slowly eroding this capability (Pasman, 2010). The term resilience was originally introduced by Hollnagel et al. (2006) as well as the approach called 'resilience engineering' to provide methods for measuring and improving the resilience.

At the same time, as the organizations are potentially losing their safety knowledge and experience due to the lack of the application of knowledge *lessons learnt* from accidents i.e. safety databases are inefficient. It has been claimed that the accidents occur or recur due to poor dissemination of accident information and learning from these accidents due to fact that many did not know how to prevent the accidents from recurring (Kletz, 1993). 95% of accident causes are known, foreseeable and could have been prevented by using the existing knowledge (Drogaris, 1993a). However, similar accidents tend to recur within a five-year interval (Mannan et al., 2010).

The third issue discussed in the thesis is the shift in *risk management approach* used for loss prevention. In the early years of industrialization, loss prevention was based on technical safety. In 1960s and 1970s, several technical/design-based safety methods were implemented such as Hazard and Operability Study (HAZOP) and Quantitative Risk Assessment (QRA). However, in the late 1970s and till today, the approach for loss prevention shifted from technical oriented to human and management oriented such as safety management systems (SMS) (Knegtering and Pasman, 2009). The focus on the outer layers of protection (LOP) is based on the assumptions that the chemical plant is well designed, existing process hazards are accepted and humans have been asked to be more careful at the workplace. Although the SMS approach is effective in improving the overall safety awareness at work, it doesn't reduce process hazards. Relying on SMS is also problematic when the organization does not have enough safety knowledge (Kletz, 2003; Paradies, 2011).

The outer layers of LOP (the active engineered and procedural strategies) do not control process hazard in comparison to inner layers an inherently safer strategy. However, due to its conceptual/general approach, the process developers/designers often ignored the inherently safer strategy (Kletz, 1999). They believed that the process hazard is unavoidable and can be controlled effectively through add-on safety protection systems (Hendershot, 2011).

As the number of accidents in the CPI has not decreased, the issue to be addressed is if the current safety promotion approaches are sufficient. The option of should the technical and design related reasons of accidents be reviewed since they seem to be dominant based on earlier studies (Drogaris (1993ab) and Taylor (2007ab). There is also the question of should the focus be more on the hazard reduction through inner layers of LOP concerning the more fundamental design oriented aspects. Then, there is the consideration as to what should be done to promote the usage of existing safety information such as the lesson learnt from earlier accidents.

There is a lack of studies on this area and little is known about the technical and design reasons of accidents, e.g. what are the typical design errors made and in which process lifecycle stages do the errors take place. The rationale for this study is to understand the reasons of accidents from the perspectives of technical, design and operation error throughout the process design lifecycle. Deeper understanding of the root causes of accidents would facilitate early detection of accidents which may prevent similar accidents from taking place in the CPI.

1.2 Aim of the study

The purpose of the study is to identify the accident contributors and analyze their frequency. Deeper analyses are carried out to find out their root reasons, interdependence and characteristics of different types of equipment. The aim is to create a hazard identification approach based on frequency of accident contributors by locating the common errors made during the plant design and operation lifecycle stages. The following tasks carried out are as follows:

i. Statistical analysis of main and sub contributors for various accident elements and the root causes.
ii. Analysis on interdependence of main and sub contributors causing accidents.
iii. Identification of high-risk contributors to accidents.
iv. Identification of typical design errors in the CPI.
v. Identification of time of occurrence of design errors in a typical plant design lifecycle.
vi. Development of a design oriented safety method for accident contributor identification.

The thesis is organized into four main sections, which include introduction (Chapters 1 – 4), research approach (Chapter 5), statistical analysis of accident cases and dissemination of accident information into design (Chapters 6 – 11), and discussion and conclusion (Chapter 12).

The introduction section comprises the chapters 1-4. Chapter 1 provides the background of the research work. In Chapter 2, the fundamental elements of process safety are introduced. Chapter 3 discusses the current issues in lessons learnt from accidents and experience feedback system. The learning cycle is reviewed and their weaknesses are identified. Chapter 4 summarizes the usual plant design phases, design tasks and decisions for typical chemical process plant design. The basic safety and design considerations throughout process lifecycle are discussed.

The section on research approach or chapter 5 describes the methodology used and how the accident information is disseminated into design process. Chapters 6, 7, 8, and 9 present the analysis of accident contributors with reference to technical and human and organizational contributors. In Chapter 10, discussion on how accident knowledge gathered is incorporated into the design of an oriented safety method. Enhancement of inherent safety measures based on corrective actions taken by the CPI is presented in Chapter 11. Discussion and conclusion are in Chapter 12.

2 Process Safety

2.1 Definitions for safety terms

A number of process safety terms used in this work is defined to support the understanding of the thesis:

- ***Accident***: the occurrence of a sequence of unwanted events that produced unintended injury, death or property damage (CCPS, 1999).
- ***Accident contributor***: an agent that is responsible in causing an accident.
- ***Accident main contributor***: an agent that is responsible for triggering the accident.
- ***Accident sub contributor***: a supporting or co-agent in causing an accident.
- ***Design technical contributor***: any design related error (technical or human) made during design activity: including designed procedures and operator-technical interface errors.
- ***Design error***: a design error is deemed to have occurred, if the design or operating procedures are changed after an incident has occurred (Taylor, 1975).
- ***Hazard***: a chemical or physical condition that has the potential to cause damage (Crowl and Louvar, 2011).
- ***Human and organizational contributor***: purely operation-based human and organizational fault in the *operation stage* of process lifecycle.
- ***Operator-technical interface error:*** the error that is not strictly design error but can cause operators to make a mistake.
- ***Origin of error***: time of occurrence of design error during design activity when the final decision is made.
- ***Risk***: a measure concerning both the likelihood and magnitude of loss (Crowl and Louvar, 2011).
- ***Safety or loss prevention***: the prevention of accidents through appropriate hazard identification, risk assessment and control strategies (Crowl and Louvar, 2011).

2.2 Legal requirements on process safety

The case histories of Seveso and Flixborough had a great impact on the current legal requirements of the CPI operations. Seveso Directive I was gazetted in the EU in

1982 and improved further in 1996 as Seveso Directive II. The legislation clearly states that the plant owner is responsible for controlling the process hazards. Through this legal requirement, every chemical facility is required to furnish the process safety information and demonstrate that appropriate action has been taken to prevent major accidents. With regards to Seveso II Directive, for a new establishment, a safety report must be sent to a Competent Authority within a 'reasonable period of time' prior to the start of construction or operation.

However, current safety and health framework such as OSHA 29 (OSHA, 1993) does not have the requirements to recognize, avoid or control hazards during the early phase of plant design project (Wincek, 2011). As a result of this requirement, most of the companies conduct full safety evaluation at the detailed design phase. Furthermore, a late formal safety evaluation makes the fundamental or major design changes difficult to be carried out.

2.3 Hazard, risk and layers of protection

Losses can be reduced by diminishing risks. The level of risks can be reduced by decreasing or managing hazards through having add-on or administrative systems within the layer of protection (LOP) approach as illustrated in Figure 1.

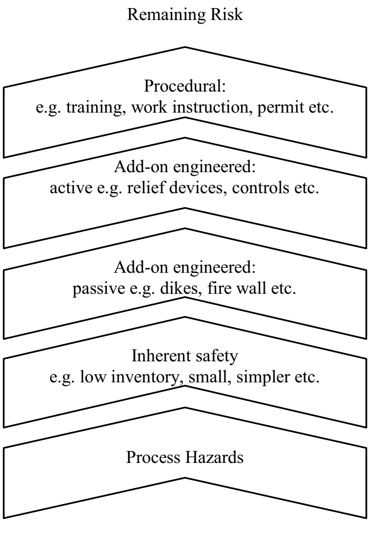

Remaining Risk
Procedural:
e.g. training, work instruction, permit etc.
Add-on engineered:
active e.g. relief devices, controls etc.
Add-on engineered:
passive e.g. dikes, fire wall etc.
Inherent safety
e.g. low inventory, small, simpler etc.
Process Hazards

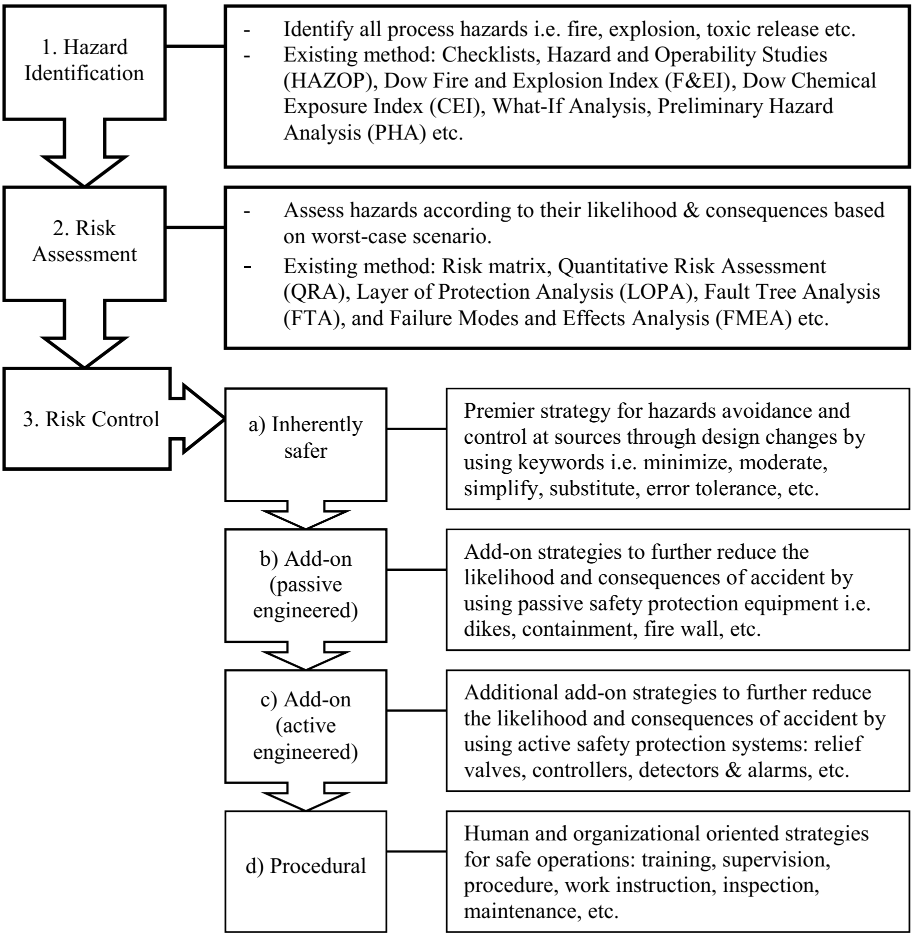
Figure 1: Layers of protection (LOP).

As seen from Figure 1, hazards refer to the hazard potential such as fire, explosion and toxic release which are typically found in chemical processing plants. Process hazards are managed by an inherently safer design (ISD) such as process intensification, inventory reduction, etc. Add-on layers can be divided into passive and active engineered categories. Passive engineered strategy employs systems that do not perform any fundamental operation and remain static in default condition such as dikes and blast or separation walls. Meanwhile, the active engineered strategy utilizes safety devices that respond to the process changes such as process controls, alarm systems and pressure relief valves. The outer layer of LOP involves procedural strategies. Procedural strategy focuses on organizational and human control by establishing work instructions and use of personal protective equipment.

The process hazards at chemical facilities need to be managed effectively and must be in accordance with the legislation, social responsibility, company image, and cost factors as unsafe operations would not be profitable in the long run. The steps in risk management and safety promotion include the hazard identification, risk assessment and control. Firstly, all possible process hazards need to be identified. Secondly, the risks of an accident should be estimated based on its likelihood and consequence. Subsequently, appropriate actions should be taken to eliminate and control the process risk as much as possible.

An overall approach to managing the process risks in hierarchical order would be inherently safer as well as having add-on protection and procedural system as summarized in Figure 2. In loss prevention, the main strategy is to implement inherent safety for process hazards avoidance and control at source. This is in contrast to the traditional risk reduction strategy that relies on engineered add-on protection systems. However, the opportunity to implement inherent safety decreases as the design proceeds. The best time to implement ISD is during the research and development, and preliminary engineering because many of the decisions are conceptual and fundamental during these stages (Hurme and Rahman, 2005).

The layer of protection acts on three functional factors of chemical plants: technical/design, operation related human factors and management factors (Figure 3). These factors have interfaces, which are operator technical interface, inspection-maintenance programs and safety promotion in operation. Statistical analyses confirm that the accidents in the CPI are contributed by organizational, human and technical faults (Sales et al., 2007; Jacobson et al., 2010). Technical contributors include equipment/component failures, lack of analysis, design related errors, etc. Figure 3 presents the main classification of accident contributors and the responsible parties.



- Identify all process hazards i.e. fire, explosion, toxic release etc.
- Existing method: Checklists, Hazard and Operability Studies (HAZOP), Dow Fire and Explosion Index (F&EI), Dow Chemical Exposure Index (CEI), What-If Analysis, Preliminary Hazard Analysis (PHA) etc.

- Assess hazards according to their likelihood & consequences based on worst-case scenario.
- Existing method: Risk matrix, Quantitative Risk Assessment (QRA), Layer of Protection Analysis (LOPA), Fault Tree Analysis (FTA), and Failure Modes and Effects Analysis (FMEA) etc.

Premier strategy for hazards avoidance and control at sources through design changes by using keywords i.e. minimize, moderate, simplify, substitute, error tolerance, etc.

Add-on strategies to further reduce the likelihood and consequences of accident by using passive safety protection equipment i.e. dikes, containment, fire wall, etc.

Additional add-on strategies to further reduce the likelihood and consequences of accident by using active safety protection systems: relief valves, controllers, detectors & alarms, etc.

Human and organizational oriented strategies for safe operations: training, supervision, procedure, work instruction, inspection, maintenance, etc.

Figure 2: The design approach in risk management in CPI.

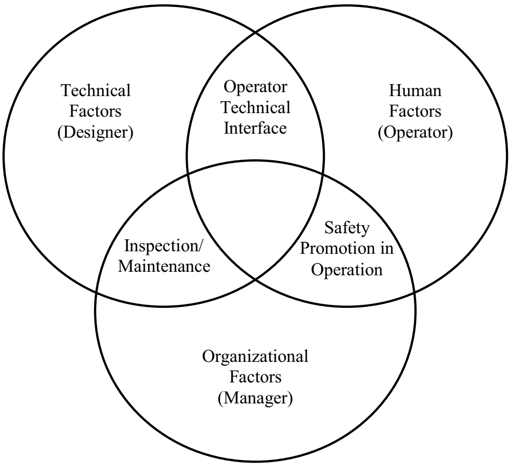

Technical Factors (Designer)
Operator Technical Interface
Human Factors (Operator)
Inspection/ Maintenance
Safety Promotion in Operation
Organizational Factors (Manager)

Figure 3: Accident contributors in CPI.

3 Accident Databases and Learning from Accidents

3.1 Accident databases

Reporting of abnormal main events is encouraged (Meel et al., 2007) and it is part of the requirements in the Seveso Directive II as a result of catastrophic accidents such as Flixborough, Seveso, Bhopal, Piper Alpha, etc. Several national and international accident databases have been created for dissemination of accident information such as Major Accident Reporting System (MARS) managed by EU; Failure Knowledge Database (FKD) managed by Japan & Science Technology (JST) Agency, Japan; and Major Hazard Incident Data Service (MHIDAS) managed by Health Safety Executive (HSE), UK. Recently, a new and available accident database has been developed called Pondicherry University Process Industry Accident Database (PUPAD) (Tauseef et al., 2011) which contains nearly 8000 accident cases collected from 41 existing open source accident databases.

Accident databases have some limitations in terms of accessibility, contents and accuracy. Although some of these accident databases are open-source and accessible through the Internet, their use is subject to certain terms and conditions. A number of these databases are developed and maintained by a service provider are not freely accessible such as MHIDAS. Besides that, a database is not perfect as there are some accidents that had been wrongly investigated, reported or classified (Kletz, 2009; Tauseef et al., 2011). This will affect the analysis results and accuracy of the generated lessons learnt from these accidents.

3.2 Learning from accidents

As mentioned in Chapter 1, accidents recur due to not addressing the lessons learnt from the earlier accidents. Many efforts have been done to analyze the cause of accidents and to generate corrective actions for effective accident preventions in the CPI. As a result, many journal papers, books and accident databases have been produced to support lessons learnt from accidents. However, a recent study found out that only one third of the accident cases studied is considered to provide lessons learnt on a broader basis (Jacobsson et al., 2010).

The level of learning depends very much on the quality of accident reports i.e. the raw data used for the analysis. Good accident data are essential for correct accident knowledge creation that would enhance process safety knowledge. Based on the knowledge management hierarchy of Ackoff (1989), the accident knowledge generated using the analyses of the number of accident cases give a better understanding of why accidents occur and how they can be prevented compared to the use of a report of single accident cases. The hierarchy of knowledge applied to accident analysis is presented in Figure 4.

In this thesis, focus is on the selection of a suitable accident database and how to carry out a deeper analysis on the causes of accident to create useful accident knowledge for better understanding of the causes of accidents. The causes were analyzed by calculating the frequency and general knowledge obtained about the causes of accidents for several types of equipment. The outcome of the research would be an approach to identify accident contributor which would be used to propose a method to enhance chemical process safety.

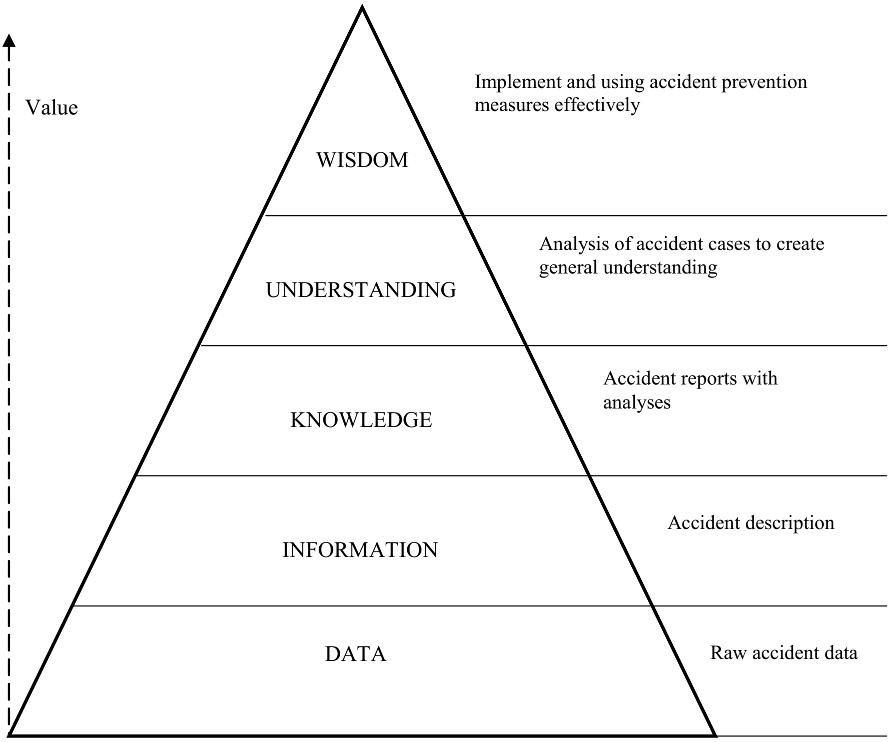

Value
WISDOM
Implement and using accident prevention measures effectively
UNDERSTANDING
Analysis of accident cases to create general understanding
KNOWLEDGE
Accident reports with analyses
INFORMATION
Accident description
DATA
Raw accident data

Figure 4: Knowledge hierarchy based on accident prevention perspective

3.3 Experience feedback system

In recent years, more studies on learning from feedbacks based on experience have been conducted in the CPI; however, most of them were related to lessons learnt from accidents (Jacobsson et al., 2010; Kletz, 2004) or from near miss cases (Prem et al., 2010). The circle of experience from the feedback system (Figure 5) consists of several elements namely: (a) accident, (b) accident investigation and reporting, (c) data collection, (d) data analysis/ processing, (e) lesson learnt, (f) information dissemination/distribution, (g) solution/decision on prevention measures, and (h) implementation (Kjellen, 2000).

The current cycle of learning system is not sufficient to prevent accidents due to poor input quality, lack of analysis, poor dissemination and insufficient use of information to prevent accidents (Kletz, 2009; Lindberg et al., 2010). The weakest link of feedback based on experience in the process learning cycle is related to dissemination of accident information (Lindberg and Hansson, 2006). Majority of the research on experience feedback is related to accident investigation and not much on dissemination of information (Lindberg et al., 2010). Therefore, the main challenge is how to disseminate the accident information effectively and translate the current knowledge into practice (Bell and Healey, 2006).

There are several approaches to actively disseminate accident information into the CPI which include the use of physical means (i.e. accident reports, journals); electronic means (accident report in databases); and the development of accident-based safety/design tools. Disseminating accident information through physical means is less effective, compared to accident databases which have a good data retrieving system (He at el., 2011; Tauseef et al., 2011). However both these approaches represent lower level information in the knowledge hierarchy compared to analyzed knowledge which is proposed in the thesis.

3.4 Dissemination of accident information

Although accident analysis using accident databases is an active research agenda in the CPI, the utilization of the lessons learnt to prevent accidents is slow. The format of accident information (e.g. accident reports) is not user-friendly to the practitioners especially process engineers and designers. The search for a safer design option by using the current format of accident information is very demanding and time consuming.

Currently, the only method on accident analysis would be to search relevant accident cases found in the literature or databases during design work. On the contrary, past accident-based design approaches for detecting and eliminating design errors are not available (Taylor, 2007a). Past experience can be introduced in safety studies through HAZOP, which can indirectly draw upon lessons learnt from earlier related accidents. The results of the lessons learnt from these accidents are dependent on the expertise of the team members.

The current experience feedback system needs to be modified, so that it can be systematically integrated with risk analysis methods (Lindberg et al., 2010; Jorgensen, 2008). Therefore in this thesis, the information dissemination part of experience feedback system was implemented by creating a design oriented safety tool in Paper V. Figure 5 illustrates the design-based experience feedback system for a safer design and operation of chemical process plants.

Dissemination and utilization of accident information into a design oriented safety tool development is placed at a higher level of knowledge management hierarchy (Figure 4) in comparison to accident reports or databases. At this level, the tools do not present only case studies, but contain deeper knowledge and understanding of accident causes and their interdependence which is done by analyzing many accident cases. The potential methods of reusing accident knowledge are:

- Case-based reasoning: retrieval of similar database data and its adaptation to current problem (Heikkilä et al., 1998).
- Human experience based utilization through HAZOP study.
- Analysis of database information and its representation as a higher level knowledge and method is discussed in Papers I-V.

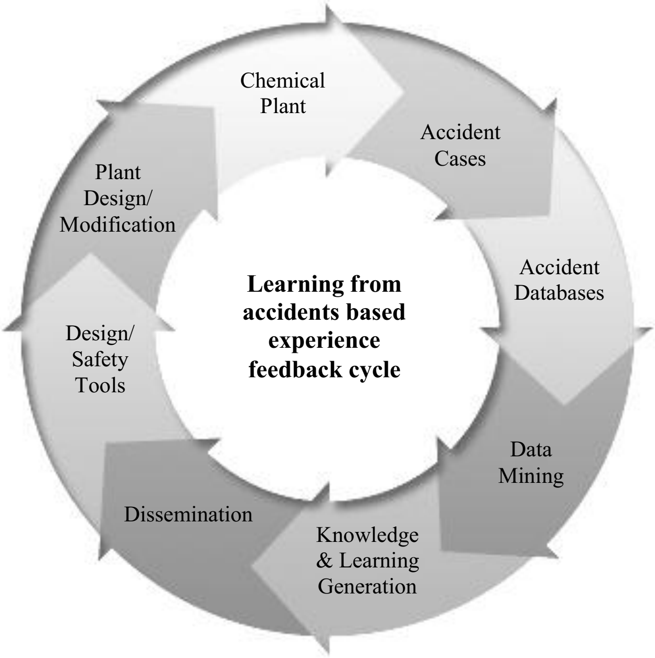

Chemical Plant
Accident Cases
Accident Databases
Data Mining
Knowledge & Learning Generation
Dissemination
Design/ Safety Tools
Plant Design/ Modification
Learning from accidents based experience feedback cycle

Figure 5: Learning from accidents based experience feedback system.

4 Safety Considerations in Design

4.1 Plant design phases

A chemical plant design undergoes a series of phases. Usually, the design of the plant starts from research and development, followed by preliminary process design, basic engineering, detailed engineering, construction and start-up, plant operation, retrofit, and decommissioning. Each design phase has specific design objectives, tasks, and decisions as presented in Table 1 (Refer Paper III).

As the project starts, the chemical process route is either acquired or developed during the research and development phase which is based on experimental and modeling data. In this step, the process concept from laboratory to pilot plant is developed. In the preliminary design, the process concept is defined, process alternatives are identified, material and heat balances are calculated, and flow sheet diagrams are generated.

In the basic engineering phase, details of the process package are determined. Process package contains process flow sheet, piping and instrumentation diagrams (PID), equipment specifications, and process description. Process data for all the equipment, piping, control system, and utilities needed are decided and provided as input information for the detailed engineering phase. The detailed PID is developed and the detailed equipment and instrument specifications are finalized. Then, HAZOP is carried out.

Detailed engineering phase includes the design for construction comprising engineering disciplines such as mechanical, electrical, civil etc. Three dimensional plant layouts are developed and full process safety analyses are carried out. The process designer prepares the operating manual of the process which includes work procedures and instructions, safety and emergency guidelines of the process. The operation manual is prepared for process operation, process start-up and operator training.

Table 1: Typical characteristics of the design stages in the CPI (Paper III)

Phase	Target	Main tasks and decisions	Main safety issues
Research and development	Development of process concept and scale-up to industrial scale.	- Idea generation and process creation/innovation. - Laboratory and simulation studies on reaction mechanism and kinetics. - Examination of raw materials (pure and industrial grade). - Laboratory & reaction calorimeter tests. - Process alternatives generation - Bench and pilot scale tests. - Market survey. - Legal and patent check.	- Use of hazardous material as feedstock. - Fail to choose the safer state of feedstock. - Incorrect data on the reaction kinetic and reaction behavior. - Incorrect data on runaway reaction potential. - Overlook the chemical reactivity and incompatibility. - Underestimate the effect of impurity, by-product and contaminants. - Unclear mechanism to control the unwanted/runaway reaction. - Inaccurate scale-up.
Preliminary engineering	Preliminary process design for the feasibility study.	- Process concept selection and flow sheet development. - Selection of unit operations. - Preliminary sizing of equipment. - Preliminary selection of construction material. - Site selection. - Final feed/product specifications. - Feasibility study.	- Complicated and extreme routes selection (high temperature and pressure). - Unsuitable types of unit operations. - Unsafe operating conditions. - Overlook the chemical reactivity and incompatibility at process equipment level. - Lack of safety analysis on the chemical contaminations.
Basic engineering	Creation of the process data for detailed engineering.	- Detailed process design and optimization. - Process design of equipment and piping system. - Basic automation and instrumentation engineering. - Preliminary layout design. - Utilities design. - Waste minimization. - Hazard and operability study.	- Inappropriate layout, positioning and physical arrangement. - Incompatible heat transfer medium. - Incorrect heating/cooling sizing. - Inadequate safety and process protection. - Wrong or inaccurate process data for equipment - Unsuitable material of construction. - Failing to consider corrosive environment. - Inappropriate mechanical/ physical and chemical resistance specification. - Incorrect material flow set-up. - Lack of safety analysis.
Detailed engineering	Design of the physical process (equipment, piping etc.) for acquisitions and construction.	- Detailed piping design. - Detailed layout design. - Instrumentation and automation design. - Mechanical design of the equipment. - Structural and civil engineering. - Electrical design. - Design of utilities/services.	- Inappropriate piping layout and protection. - Inappropriate internal shape of equipment/component. - Incorrect location and positioning of support/ attachment/ venting of process equipment. - Inadequate electrical, mechanical and structural/ foundation specification. - Inadequate static, lightning and ignition sources control. - Inadequate detection, automation and instrumentation. - Inadequate operating, start-up, shutdown and emergency manuals. - Wrong specification of 'buy item'. - No back up for utilities failure.
Procurement, fabrication, commissioning and start-up	Acquisitions, construction and installation of the process. Starting up the process and make it to meet the specification.	- Contracting and bidding. - Contractor selection. - Procurement. - Installation. - Inspection. - Testing. - Field changes.	- Part or components miss-match. - Wrong installation or poor work quality. - Incorrect positioning of sensor/ instruments. - Accessibility. - Lack of monitoring and supervision of contractor. - Miscommunication between designer, contractors and plant owner.
Operation/ Plant modification	Safe operations within design specifications and capacity. Improvement of the process.	- Selection of safe operation and maintenance principles. - Gathering experience. - Process optimization. - Process improvement - Record keeping on plant histories and technological up-date.	- Poor planning. - Lack of safety analysis. - Lack of technical and reaction knowledge. - Poor safety culture. - Poor inspection and maintenance. - Poor management of change.

In the construction phase, the chemical plant is built as designed. In the start-up phase, the process starts and the test runs are made. In the operation phase, the plant is operated and maintained according to guidelines. Since the plant requires improvement or capacity increase, modifications are made. The management of change is important during this stage of design.

4.2 Safety evaluation during design

A number of safety and design reviews are carried out throughout the process lifecycle. Their timing and techniques used may vary because engineering companies have a quality system which defines what is done and when it is done. In the literature, several publications discussed the methods used for hazard identification and risk assessment during chemical process plant design (Crawley and Tyler, 2003; Deshotels and Zimmerman, 1995; Kletz, 1991). They also listed the common methods used to evaluate the safety aspects at each plant design phase.

The most common methods used in chemical plant design were checklists, HAZOP and hazard surveys such as Dow F&EI, and safety review (Crowl and Louvar, 2011; Seider et al., 2009). A checklist can be used throughout the process lifecycle, however, the other methods are intended mainly for the later stages of plant design; i.e. at basic and detailed engineering stages due to their need for information (Hurme and Rahman, 2005; Kidam et al., 2008a). In some firms, these checklists were used earlier but in an abridged form. Consequently, the safety evaluations are usually intervened quite late in the design (i.e. at basic or detailed design) where major design decisions on the process have already been made (Schupp et al., 2006).

The existing safety review methods eliminate 80-95% of design errors (Taylor, 2007a) but there is still a design element present in most (80%) of accidents in the chemical industry (Refer Paper III). Therefore, it is obvious that the current safety and design reviews have limitations. HAZOP is a typical method used for tens of years for finding safety and operational weaknesses in process plant design. It is based on the P&I diagrams and does not cover mechanical design errors. Dimensioning errors and problems arising during start-up & shut down are not well covered, as well as human or procedural errors (Duguid, 2001; Taylor, 2007b). The coverage has an average of

85% in those aspects which HAZOP should take into account but the average is only 60% when it includes human errors and mechanical hazards (Taylor, 2007b).

HAZOP is rather effective in removing process engineering related faults, but the problem is that HAZOP is done at a later stage, when all the process design is quite ready. One of the expectations is that HAZOP would not point out any need for process design related changes because the costs related to these changes made at a late stage are expensive. Therefore HAZOP does not support the process designer during the design work but acts as a final check. From the mechanical engineering point of view, HAZOP is done too early at the stage where detailed design has not been done or finished. This shows that HAZOP lacks the capability to assist in the changes during the early stages.

It has been identified that most accidents involve design element, and HAZOP has been used for decades as past accident based method for hazard identification to support the existing process safety methods.

5 Research Approach

In this thesis, accident cases from an accident database are analyzed and the findings are used to create a method for improving the process safety in the design of chemical process plants. The research approach of the thesis work is based on the experience feedback cycle presented in Figure 5. The aim is to incorporate the accident information directly into design, where effective accident prevention can be done on the design and these changes are made during the early stages of design.

5.1 Accident database selection

As mentioned in Chapter 3.1, there are several accident databases available that can be used for the accident analysis. The Failure Knowledge Database (FKD, 2011) was selected for the study to minimize the problems related to insufficient and inaccurate data as pointed out by Kletz (2009). This accident database contains a total of 549 accident cases. 364 are chemical industry related and 95% of the accidents happened in Japan from the years 1964 till 2003 The database is managed by experienced academia in Japan under the close monitoring of the Japan & Science Technology (JST) Agency. The accident reports are carefully reviewed by a nominated committee and they have compiled extensive information on the accidents. The availability of quite detailed technical and engineering information enables the analyses of accident contributors to be made. The basic structure and case expression of the database are discussed by Hatamura et al. (2003).

5.2 Retrieval and analysis of accident data

Accident information on 364 cases was retrieved and transformed into MS Excel format for frequency analysis aimed at identifying the following:

a) the overall accident contributor categories such as technical, design, human and organizational (Paper I),
b) the equipment types that are frequently involved in accidents (Paper II),
c) the main contributors that trigger the accidents as well as the sub contributors that co-exist (Papers I and II),
d) design errors and their origin during design activities (Papers III and IV),
e) corrective actions taken to prevent similar accidents (Paper VI).

In Papers I and IV, all the 364 accident cases were used in the analyses. Papers II - IV discussed in detail the six major equipment types involving 284 accident cases.

5.3 Dissemination of accident information into design process

The approaches to utilize and disseminate accident information to design can be grouped into three categories: heuristic, case-based and statistical approaches (Figure 6). Heuristic approach is experience based trial and error technique. Heuristic approaches include design checklists, standards and good engineering practice utilized by practicing engineers.

Case-based reasoning (CBR) is a method of reusing information by retrieving the most similar cases and adapting them for solving the current problem. CBR has been utilized by Heikkilä et al. (1998) for evaluating the inherent safety level of process configuration. This was done by using a database comprising good and bad cases; i.e. design recommendations and accident cases. Hatakka and Reniers (2009) developed and used a CBR tool for accident databases for marine safety.

In this work, the statistical approach was used to discover the most common contributors of accidents and their relationship. The analyses included frequencies of accident contributors from different points of views such as

a) frequent accident contributors,
b) frequent main-contributors,
c) specific contributors
d) contributors which often act as main contributors (SMC),
e) contributors in the high risk cluster.

The potential accident mechanism was identified through the interconnection of contributors. Based on usual design tasks and decisions, the time of occurrence of design and operation errors in the typical design project stages were identified. The findings were used for creating a design oriented safety method to support hazard identification activities during the design. The method aims to present the accident information based on a higher level of knowledge hierarchy (i.e. understanding as shown in Figure 4).

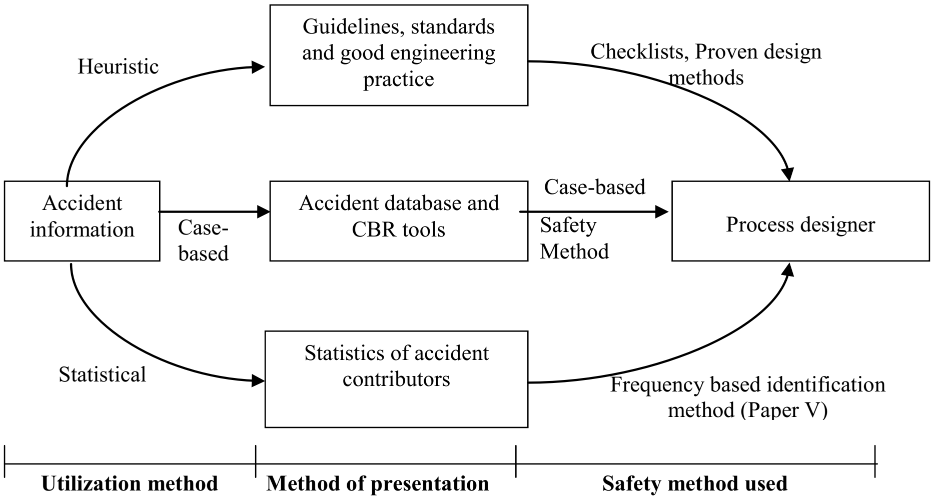

Guidelines, standards and good engineering practice
Heuristic
Checklists, Proven design methods
Accident information
Case-based
Accident database and CBR tools
Case-based
Safety Method
Process designer
Statistical
Statistics of accident contributors
Frequency based identification method (Paper V)
Utilization method
Method of presentation
Safety method used

Figure 6: Integration of approaches for learning from accidents into design.

6 Statistical Analysis of Accidents

Statistical analysis of accidents is an active research agenda in the CPI (Prem et al., 2010; He et al., 2011; Lisbona et al., 2012). Accidents are caused by organizational, human and technical faults (Sales et al., 2007; Jacobson et al., 2010) and a majority of the research focused on organizational and human failures. Detailed statistical studies on technical contributors to accidents are scarce. Thus, this study relies on the 364 CPI-related accident cases available in the FKD database which are based on the analysis of technical contributors (Paper I).

6.1 Accident contributors

In Paper I, 364 accident cases were studied based on 15 categories of accident contributors. These included categories such as human & organizational faults (in operation), external factors and 13 sub-categories of technical faults. The technical category includes design and operator-technical interface related faults. Table 2 lists the descriptions of the accident contributors. 806 accident contributors based on multiple causes of accidents were identified and, the average was 2.2 contributors per accident. Figure 7 presents the distribution of the 806 accident contributors in this study.

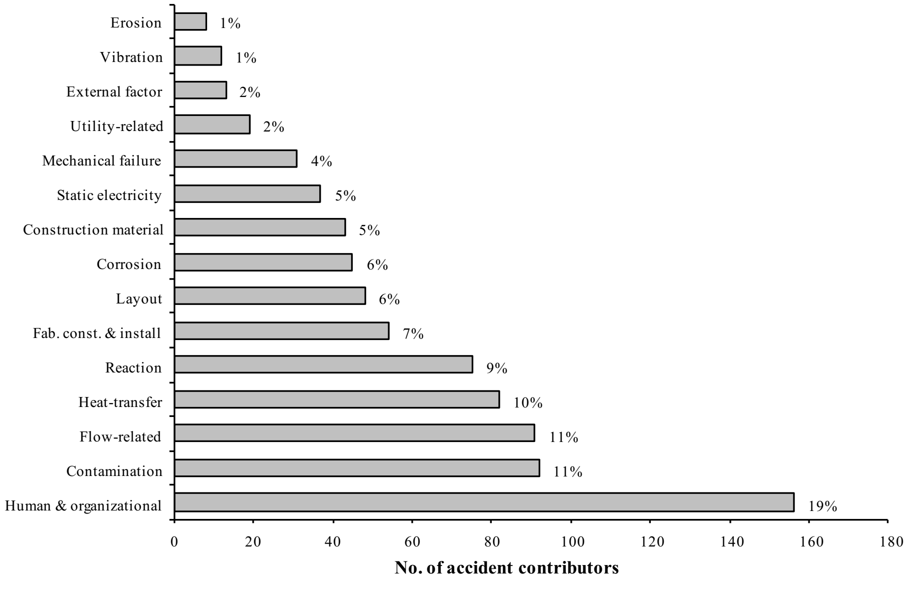


Figure 7. Distribution of the accident contributors (% of all contributors)

Table 2: The classification of accident contributors

Contributors	**Description**
Human & organizational faults in operation (a)	Operation related human error and organizational failures. Design and operator-technical interface related human errors are classified into technical contributors.
Contamination* (b)	Traceable amount of unwanted chemicals such as impurities, recycle accumulation, residues, by-products formation, moisture etc.
Flow related* (c)	Contributors related to fluid flow and transfer such as velocity, viscosity, liquid hammer, reverse flow, leakages etc.
Heat transfer* (d)	Cooling, heating and their effects to physical changes in equipment and process conditions.
Reaction* (e)	Chemical reaction related contributors: unfinished, runaway and unwanted chemical reactions due to chemical reactivity and incompatibilities.
Fabrication, construction and installation* (f)	Faults in design specification, fabrication and installation concerning work planning, quality of work, welding, support arrangements, reconditioning and reusing items.
Layout* (g)	Plant layout, physical arrangement, positioning, equipment accessibility, visual obstacles, signage and color-coding etc.
Corrosion* (h)	Excessive corrosion attacked due to wrong design specification, construction, equipment and piping aging, lack of protection and water proofing etc.
Construction material* (i)	Inappropriate physical, mechanical and chemical specification of construction material for equipment, piping and components.
Static electricity* (j)	Electric charges generation, accumulation and discharge due to wrong material selection, isolation, lack of earthting and protection when handling process fluids, particulates, dust and powders.
Mechanical failure* (k)	Structural and wall failures due to crack, fatigue, rotation, moving object/parts, stress, wear and tear, etc.
Utilities related* (l)	Inappropriate design, decision and selection of utility systems and their equipment, availability of utilities as well as back-up system for emergency.
Vibration* (m)	Vibration resulting from fluids flow, pumping, poor installation, support etc.
Erosion* (n)	Result of fluid movement and flow pattern, gas/liquid phases, particulates, velocity, bubble ruptured and internal equipment layout etc.
External factor (o)	Physical and natural events such as bad weather, earthquake, floods, tsunami, lightning, land slides, and some random effects.

*Note: * classified as technical contributors*

19% of accident contributors were classified as ‘purely’ human and organizational failures in the plant operation stage (without design or operator-technical interface faults). Similar results were reported by Drogaris (1993), who found 18% of accident causes were operation related human & organizational faults. Meanwhile, 79% of causes were classified as technical which included design, analysis and also operator-technical interface errors. In this category, the most common accident contributors were process contamination (11%), flow related faults (11%), heat transfer (10%), and reactions (9%). In addition, approximately 2% of the accidents were caused by external factors e.g. weather, earthquake and random events. Causes of these contributors are further elaborated in Appendix 1 of Paper I.

6.2 Operator-technical interface induced causes

Paper I reviewed on the contribution of the operator-technical interface faults to accidents which was significant as it was 11% of the contributors (Refer Table 2 in Paper I). The operator-technical interface errors were not strictly design errors but they caused operators to make mistakes which led to accidents. Typical examples of these technical interface induced human failures include problems caused by wrong equipment or component labeling or positioning, confusing control panel display, and poor visibility or accessibility.

The most critical category in interface errors was the flow related accident contributors (33% of flow related accident contributors). The value corresponded to 1/3 of the interface-induced causes. The other frequent interface-affected contributors were contamination and heat transfer. These three contributors made up 2/3 of all the interface-related causes. Utility-related contributors were also greatly affected by interface problems (26%) but their frequency was small. Typical examples of technical interface induced human failures included wrong equipment or component labeling or positioning, confusing control panel display, poor visibility and accessibility caused problems.

6.3 Main and sub contributors of accidents

In Paper I, an analysis of the main and sub contributors of accidents and their interdependency was carried out. The main-contributor was considered to be the main factor that immediately initiated or triggered the accident. In some cases, the main contributor had solely initiated or triggered the accident. The sub-contributors also were significant in causing the accidents; however their roles were minor and considered as supporting factor only. If the main contributor were to be removed, the accidents would not happen at all or would have had a lower probability of happening.

Table 3 presents the frequencies of the contributors and the main contributors to accidents. The *main contributors* to accidents are 83% technical, 16% human and organizational and 1% external factors. To compare, technical aspects were 79% as contributors but even more (83%) as main contributor. The most common main contributors to accidents are human and organizational aspects (16%), followed by process contamination (14%), flow related aspects (13%), heat transfer (12%), layout (10%) and fabrication / construction / installation (10%).

6.4 Importance study on accident contributors

The importance of the analysis of accident contributors in accident prevention was carried out based on their share as main contributors (SMC) and being part of the four quadrants analysis in Paper I. The SMC of an accident contributor means how often it is identified as the main contributor compared to its presence in general as an accident contributor. For example, layout is the main contributor with 38 times of occurrences meanwhile as an overall contributor with 48 times. Therefore, the SMC for layout is calculated by 38/48 = 79%. The SMC represents the potential of an accident contributor to be the main contributor to an accident.

In Table 3, the highest SMCs among all the contributors are: layout (79%), unsuitable construction material (67%) and errors in fabrication, construction and installation (65%). The average value of SMCs is 45%, which can be used as a benchmark for comparison purposes.

Since SMC does not represent absolute frequency, a four-quadrant analysis was made for the contributors based on the SMC and frequency to estimate the importance of the accident contributors. In the four-quadrant analysis, the risky contributors are: contributors that tend to be frequent contributors to accidents and have a high SMC. As seen from Figure 8, the figure is divided into four-quadrants according to SMC values and frequency of occurrence. The analysis shows that the accident contributors could be grouped into 3 main clusters. However reaction (e) and human & organizational (a) do not fit into any of the clusters. The clusters are summarized in Table 4.

Table 3: Frequency and percentage according to main contributors (SMC)

Contributing Factors	Frequency				SMC
	As contributor		As main contributor		
Layout (g)	48	6%	38	10%	79%
Construction material (i)	43	5%	29	8%	67%
Fabrication, construction & installation (f)	54	7%	35	10%	65%
Corrosion (h)	45	6%	25	7%	56%
Contamination (b)	92	11%	50	14%	54%
Flow related (c)	91	11%	48	13%	53%
Heat transfer (d)	82	10%	43	12%	52%
Reaction (e)	75	9%	29	8%	39%
Human & organizational (a)	156	19%	60	16%	38%
External factor (o)	13	2%	3	1%	23%
Utilities related (l)	19	2%	3	1%	16%
Static electricity (j)	37	5%	1	0.3%	3%
Mechanical failure (k)	31	4%	0	0%	0%
Vibration (m)	12	1%	0	0%	0%
Erosion (n)	8	1%	0	0%	0%
TOTAL	806	100%	364	100%	average: 45%

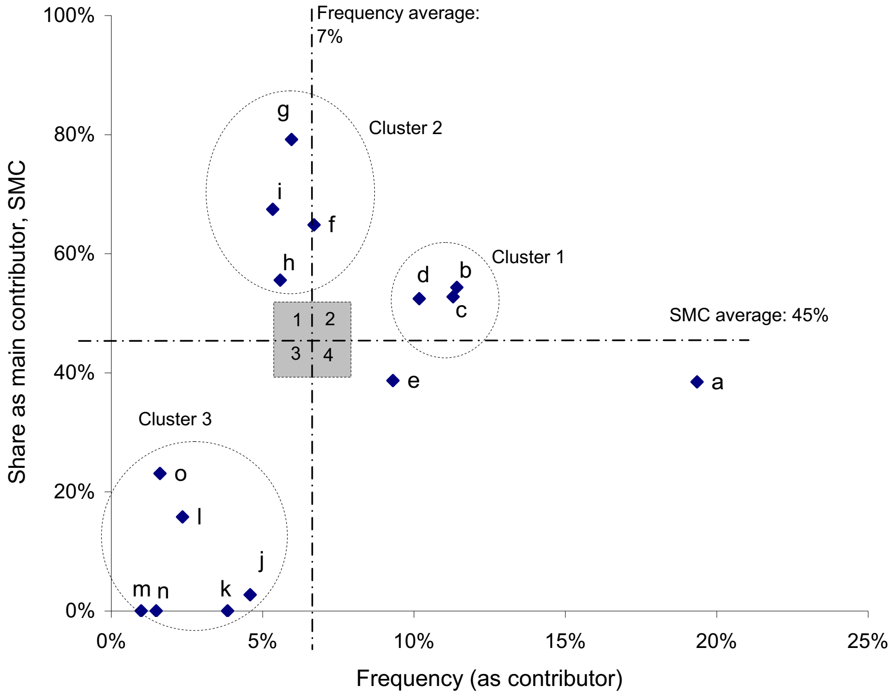


Figure 8: Percentile of main contributor (SMC) vs. frequency as accident contributors (for notation see Table 3)

Table 4: Clusters of main contributors and frequency as a main contributor

Cluster 1	%	Cluster 2	%	Cluster 3	%	Outside clusters	%
Contamination (b)	14	Layout (g)	10	Utility related (l)	0.8	Hum & org. (a)	16
Flow related (c)	13	Fab./const/inst (f)	10	External factor (o)	0.8	Reaction (e)	8
Heat transfer (d)	12	Const. material (i)	8	Static electricity (j)	0.2		
		Corrosion (h)	7				
Total	39	Total	35	Total	2	Total	24

Referring to Figure 8 and Table 4, cluster 1 (b-contamination, c-flow related, and d-heat transfer) has the highest frequency of occurrence and a high SMC, and therefore, is the most likely factor for causing accidents in the CPI.

The second cluster consists of faults in the layout, construction material, fabrication-construction-installation, and corrosion. This cluster is higher in SMC but is less frequent compared to the ones in cluster 1. The third cluster is made-up of less common and low SMCs contributors. Contributors outside the clusters (human & organizational and reaction) have lower than the average SMCs but their frequency is high.

Since a contributor with a high SMC has a higher probability of causing accidents and not only contributing as a sub-factor, thus accident prevention should focus on the high SMC contributors as they have a high frequency. Therefore, the importance based on ranking as the most likely contributors to accidents are: cluster 1 comprising process contamination, flow related & heat transfer, followed by cluster 2 which contains layout, fabrication/construction/ installation, construction material & corrosion, and outside cluster; human & organizational and reaction.

6.5 Interconnection of accident contributors

Some main accidents and sub-contributors have a strong relation to one another. Therefore, a correlation study was carried out by using interconnection matrix (Refer Table 5 in Paper I). The correlation study investigates the probability of accident contributor act together to cause an accident. The finding helps for early accident scenario prediction. The main interconnections of accident contributors are illustrated in Figure 9. A thick line represents the strongest correlation between two accident contributors, while a thin line shows a strong correlation and a dotted line indicates a medium correlation.

Three functional groups of accident contributors identified from Figure 9 are as follows:

- *Human and organizational* failures group. This is specifically related to flow oriented problems (such as transfer and handling of chemicals), heat transfer activities, layout issues, static electricity control and construction materials.
- *Reaction, heat transfer*, *contamination* oriented group. Process contamination is created or caused by unwanted chemical reactions, which could be prevented by identifying possible routes and sources of the contaminants (i.e. layout and flow related factors) and by reducing operating errors (i.e. the human aspects). Heat transfer and reaction are very closely related and their effects on the process safety should be considered mutually.
- *Mechanic*al *& material* contributors group. Mechanical faults are affected by fabrication/construction/installation and by corrosion which are affected by construction materials.

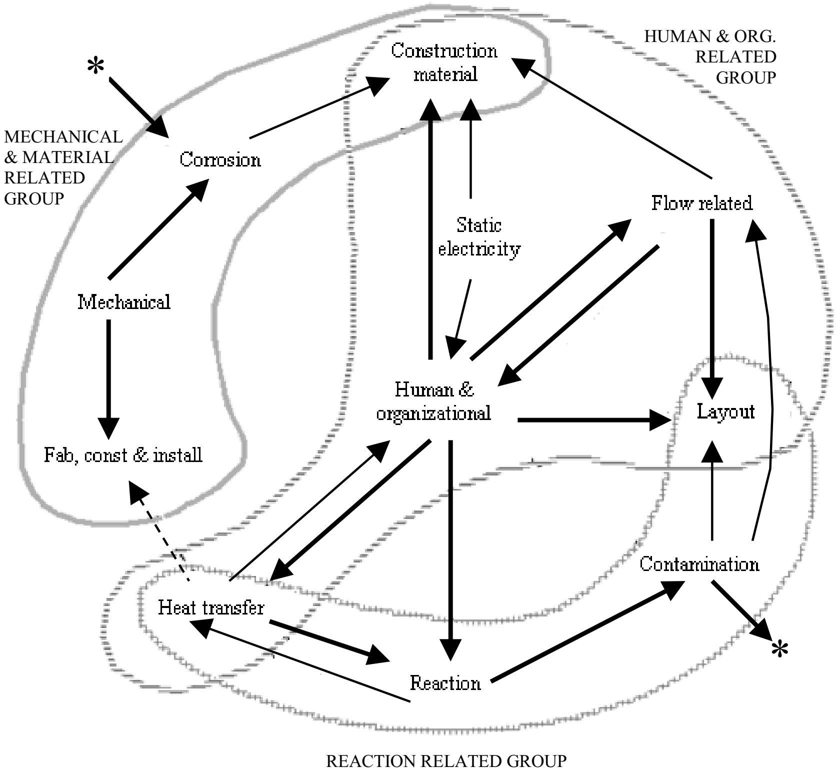


Figure 9: Diagram of Interconnection between accident contributors with functional groups (the thicker the line the stronger the interconnection). The arrows show the direction from sub to main contributor.

7 Process Equipment Accidents

The focus of this chapter (Refer Paper II) is to identify the reasons behind process equipment failures. Several studies on equipment failures have been carried out in the CPI. However, equipment failures were considered as only sub-topics in the accident cause analysis (Duguid, 2001; Gunasekera and Alwis, 2008; He at el., 2011; Hou and Zhang, 2009; Prem at el., 2010). Therefore, a study to identify the reasons for equipment based accidents was done and presented in Paper II.

Identification of equipment based accidents was done by analyzing 364 CPI-related accident equipment type cases in the FKD database. The results for the most frequently involved type of equipment are shown in Figure 10. The most common ones are piping (25%), reactor (14%) and storage tank (14%). The results are comparable with previous studies (Refer Table 1 in Paper II).

7.1 The contributors to process equipment accidents

The six most commonly accident causing equipment types were selected for a more detailed analysis. The findings showed that 78% of accidents involving 284 accident cases and 623 accident contributors were due to multiple causes of accidents. The accident categories used were the same as the ones used in Table 2.). Table 5 presents the percentiles of the contributors for six types of equipment.

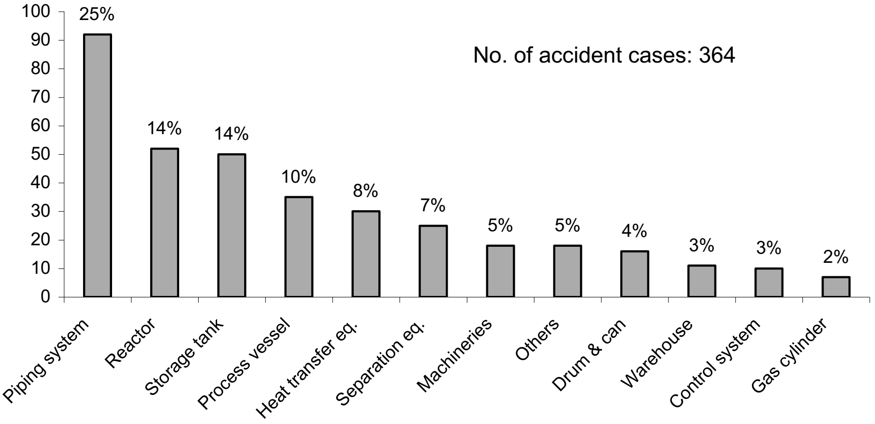


Figure 10: Proportions of accidents caused by specific equipment

Table 5: Number and percentage of contributors in equipment related accidents

Accident contributor	Piping System	Storage Tank	Reactor	Heat Transfer Eq.	Process Vessel	Separation Eq.	Total
Human/organizational (a)	41 (18%)	36 (33%)	12 (16%)	12 (16%)	12 (17%)	9 (15%)	122 (20%)
Contamination* (b)	17 (7%)	6 (5%)	12 (16%)	11 (15%)	14 (19%)	15 (25%)	75 (12%)
Heat transfer* (c)	17 (7%)	10 (9%)	17 (23%)	11 (15%)	8 (11%)	9 (15%)	72 (12%)
Flow related* (d)	23 (10%)	15 (14%)	6 (8%)	9 (12%)	10 (14%)	8 (13%)	71 (11%)
Reaction* (e)	10 (4%)	3 (3%)	17 (23%)	2 (3%)	12 (17%)	9 (15%)	53 (9%)
Layout* (f)	25 (11%)	6 (5%)	1 (1%)	4 (5%)	5 (7%)	3 (5%)	44 (7%)
Fab. const. & inst.* (g)	30 (13%)	5 (5%)	2 (3%)	5 (7%)	1 (1%)		43 (7%)
Corrosion* (h)	22 (9%)	4 (4%)	3 (4%)	8 (11%)	1 (1%)		38 (6%)
Construction material* (i)	19 (8%)	4 (4%)	3 (4%)	8 (11%)	2 (3%)	1 (2%)	37 (6%)
Static electricity* (j)	2 (1%)	6 (6%)	2 (2%)	3 (4%)	5 (7%)	3 (5%)	21 (3%)
Mechanical failure* (k)	8 (3%)	4 (4%)			2 (3%)	1 (2%)	15 (2%)
External factor (l)	4 (2%)	9 (8%)					13 (2%)
Vibration* (m)	8 (3%)			1 (1%)			9 (1%)
Erosion* (n)	6 (3%)						6 (1%)
Utility related* (o)	2 (1%)					2 (%)	4 (1%)
Total contributors	234 (37%)	108 (17%)	75 (12%)	74 (12%)	72 (12%)	60 (10%)	623
Contributors per accident	2.5	2.2	1.4	2.5	2.1	2.4	2.2

*Note: *) classified as technical contributors*

In Table 5, the operation related human & organizational causes are the largest percentile of contributors (20%). However, the main portion of 78% refers to technically oriented causes including design and operator interface errors. External causes such as earthquake, bad weather, lighting, etc. are 2%. An accident has typically 2.2 contributors. Piping has the largest number of contributors per accident which is 2.5 and this is the same for heat transfer equipment whereas the reactor accidents have only 1.4 contributors.

At the process equipment level, piping is the most common and risk prone part of the chemical process. The typical accident contributors are related to human and organization aspects (18%), fabrication/construction/installation (13%), layout (11%), and flow (10%) related causes. Piping accidents had more contributors which was 2.5 per accident as compared to other equipment whose average was 2.2.

Reactors were involved in 14% of the accidents. Majority (71%) of the reactor accidents involved batch or semi-batch reactor operations. The higher number of failures in batch reactors is expected due to the dynamic character of batch reactions, variable products, partly manual operations, the reactive materials handled and difficulties in design. The main reasons for accident are inadequate process analysis on heat transfer (23%), reaction problems (23%) and process contamination (16%).

Storage tanks were responsible for the third highest number of accidents (14%) mainly due to organizational and human failures (33% of contributors), flow related (14%), heat transfer (9%), and external factors (8%). Other major issues were related to poor planning and lack of analysis e.g. in chemical transfer and tank cleaning or maintenance.

Process vessels represent 10% of accidents in the CPI. Typical issues of process vessel operations are their complex interactions with other equipment through piping. Therefore contamination was the most common (19%) accident contributor and followed by unwanted chemical reaction in the vessel (17%) and flow related (14%) causes. The contribution of organizational & human causes to process vessel failures was also significant (17%).

Approximately 7-8% of accidents in the CPI were related to heat transfer and separation equipment failures. The most common accident contributors to heat transfer equipment failure were human and organizational (16%), process contamination (15%) and heat transfer (15%) related causes.

The majority of the separation equipment accidents (80%) involved distillation operations. Common accident contributors were process contamination (25%), heat transfer (15%), human & organizational (15%), reaction (15%), and flow related (13%) aspects. A more detailed analysis of the accident contributors is presented in Appendix 1 of Paper II.

7.2 Accident main contributors

The analysis on main contributors (MC) and shares of main contributors (SMC) for the various equipment types was also carried out by using similar analysis approach as in Chapter 6. The results are summarized in Table 6. The analysis shows that the most frequent main contributors in equipment accidents were operation stage related human & organizational issues (16 %), contamination (14 %), flow related aspects (13%), heat transfer (12%) and layout (11%).

Table 6: Main contributors to accidents and their percentiles

Accident contributors	Piping system		Storage tank		Reactor		Heat transfer eq.		Process vessel		Separation eq.		Overall	
	MC	SMC, %	MC	SMC, %	MC	SMC, %	MC	SMC, %	MC	SMC, %	MC	SMC, %	MC	SMC, %
Layout (f)	19	76	4	67			3	75	3	60	2	67	31	70
Fab. const & inst. (g)	17	57	5	100	1	50	3	60	1	100			27	63
Material const. (i)	13	68	4	100			2	25	1	50	1	100	21	57
Corrosion (h)	9	41	3	75	2	67	6	75	1	100			21	55
Flow related (d)	9	39	12	80	5	83	3	33	5	50	3	38	37	52
Contamination (b)	5	29	1	17	9	75	4	36	13	93	7	47	39	52
Utilities related (o)	1	50									1	50	2	50
Heat transfer (c)	7	41	4	40	12	71	4	36	4	50	3	33	34	47
Reaction (e)			1	33	16	94			2	17	4	44	23	43
Human & org (a)	12	29	13	36	7	7	5	42	5	40	4	44	46	38
External factor (l)			2	22									2	15
Static electricity (j)			1	17									1	5
Erosion (n)													0	
Mechanical failure (k)													0	
Vibration (m)													0	
Total/SMC average	92	39	50	46	52	69	30	41	35	49	25	42	284	46

Notation: MC – count as main contributor; SMC – share as main contributor in percentage, %

The contributors with the largest and most SMCs were poor layout (70%) and fabrication/ construction/ installation (63%) as compared to the average SMC value of all contributors which was 46%. A large SMC shows the capability of the contributor to act as a main contributor to an accident.

Reactor (69%), has the highest SMC average followed by process vessel (49%) and storage tank (46%). Since reactor accidents had only 1.4 contributors per accident

(Table 5), a single contributor was enough to cause an accident for reactors in 56% of the cases, when there was an average 2.2 contributors for all types of equipment. This means that reactors as equipment are quite sensitive to reaction, heat transfer, contamination and flow related accident contributors. Only one fault in the equipment can cause an accident without the presence of other contributors.

7.3 Interconnection analysis

Based on the interconnection technique described in Chapter 6.5, an interconnection study of main and sub contributors was done for the process equipment types in Paper II. Table 7 shows the main interconnections matrix based on Table 5 of Paper II. The interconnections were divided into three groups: human & organizational, reaction & heat transfer, and mechanical & material as described in Figure 9. The shares of the interconnection groups are presented graphically in Figure 11.

Table 7: The interconnections between accident main and sub-contributors to accidents for certain equipment types

Equipment	Interconnection level	
	Largest	Medium
Piping	• Layout to: Human & org., 9%	• Flow related to: Human & org., 7% • Layout to: Contamination, 8%; flow related, 5% • Construction material to: Corrosion, 8% • Fab. cont & inst. to: Vibration, 7%; mechanical failure, 5%
Storage tank	• Flow related to: Human & org., 20%	• Human & org. to: Heat transfer, 9% • Heat transfer to: Human & org., 9% • Const. material to: Static electricity, 9%; human & org., 9% • Fab. const & inst. to: External factor, 9% • Layout: Human & org, 9%
Reactor	• Reaction to: Heat transfer, 10%	-
Process vessel	• Contamination to: Reaction, 14%	• Contamination to: Human & org, 9% • Heat transfer to: Reaction, 9%
Heat transfer eq.	• Corrosion to: Contamination, 9%; construction material, 10% • Human & org. to: Flow related, 10%	-
Separation equipment	• Contamination to: Human & org, 12% • Reaction to: Heat transfer, 12%	-

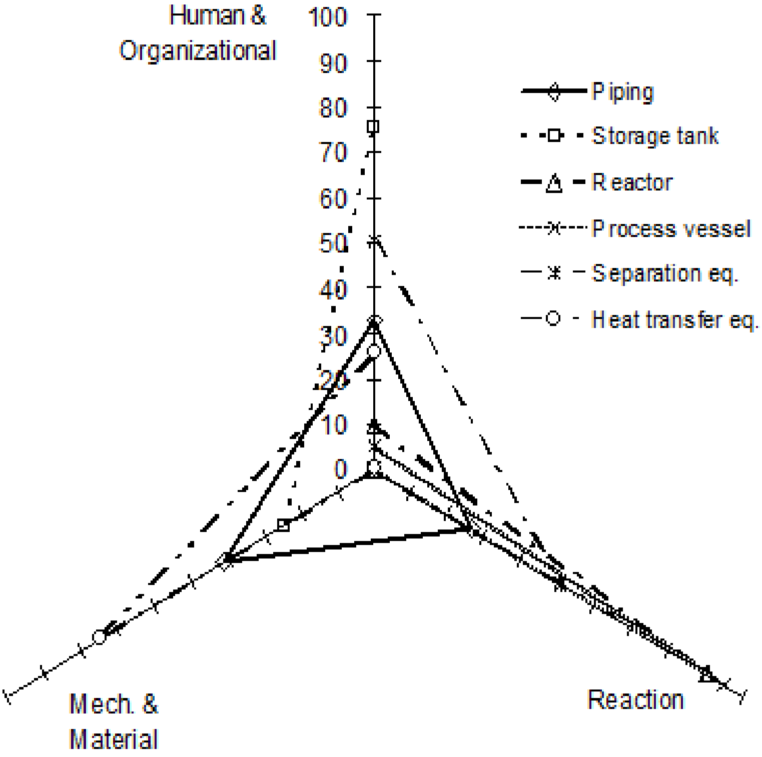


Figure 11: The shares of contributor interconnection groups for equipment.

It was found that different equipment types have characteristic interconnections. Piping accidents had interconnections that were almost equally divided between the three groups of interconnections. Storage tanks had mainly human & organizational interconnections. Reactors and separation equipment were reaction & heat transfer group dominated. Heat transfer equipment had its main interconnections in mechanical and material group, meanwhile, process vessels were equally divided between human & organizational and reaction & heat transfer groups.

7.4 Specific contributors

Equipment types have specific contributors of which they are especially vulnerable and these contributors are more frequent than average in the accidents of particular equipment. The specific accident contributor frequency values in Table 5 were divided by the average frequencies for each equipment type. The results in Table 8 show erosion is relatively 2.7 times more frequent as an accident cause in piping accidents: 3% in equipment accidents as compared on average 1% (see Table 5). On the other hand, it should be noted that some of the contributors have a low absolute frequency; e.g. erosion happened in only 3% of piping accidents. Relative frequency values in Table 8 show a technique to identify specific accident contributors which is not common in general safety analyses.

Table 8: Comparison of frequency among the average accident contributors for certain equipment type (Paper II).

Equipment	Accident contributors	Frequency as contributor, %	Times more common than on average
Piping system	Erosion	3	2.7
	Vibration	3	2.4
	Fabrication, construction & installation	13	1.9
	Corrosion	9	1.5
	Layout	11	1.5
Storage tank	External factor	8	4.0
	Human & organizational	33	1.7
	Static electricity	6	1.7
	Mechanical failure	4	1.5
Reactor	Reaction oriented	23	2.7
	Heat transfer	23	2.0
Heat transfer equipment	Construction material	11	1.8
	Corrosion	11	1.8
Process vessel	Static electricity	7	2.1
	Reaction oriented	17	2.0
	Contamination	19	1.6
Separation equipment	Utility	3	5.0
	Contamination	25	2.1
	Reaction oriented	15	1.8

7.5 Cluster analysis

A four-quadrant analysis was carried out in Paper II for each process equipment type to identify the high risk contributors. The approach is described in Chapter 6.4. Quadrant 1 presents the most risky contributors with high frequency and SMC (Refer Figure 2 of Paper II). Table 9 summarizes these risky contributors for accident contributor identification on specific equipment type.

The characteristics of equipment type can be compared by using the same method as mentioned in Chapter 6.4. Figure 12 presents the four-quadrant analysis for the average values of SMC and frequency for the equipment type. As seen from the Figure 12, the reactor has a very high SMC, therefore the reactor can clearly be considered as the most risky equipment type as most of the cases involved a single contributor that has the potential of causing an accident without sub contributors.

Storage tanks have the average SMC and frequency of the most risky quadrant. Piping has a very high accident frequency but a low SMC, implying that there are a large number of contributors present. Table 6 of Paper II summarizes the main points of the findings in a concise checklist form to support accident contributor identification.

Table 9: Contributors of high risk of accident (Cluster 1)

Equipment	Cluster 1
Reactor	Reaction, heat transfer, and contamination
Storage tank	Flow related
Heat transfer eq.	Corrosion and human & organizational
Process vessel	Contamination, flow related and heat transfer
Separation eq.	Human & organizational, contamination and reaction
Piping system	Layout, fab. const & installation, construction material, corrosion, flow related, and heat transfer

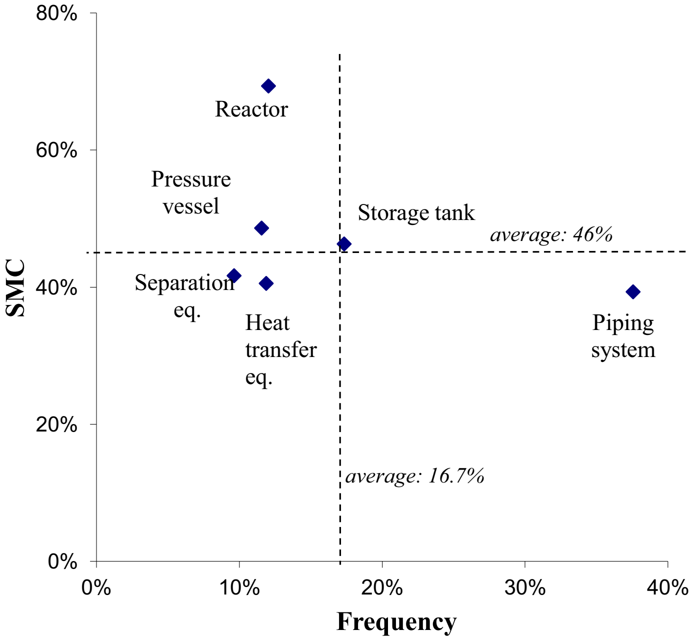


Figure 12: Average SMC and accident frequency for equipment type.

8 Design Errors in the Chemical Process Industry

Research on the design errors has been largely neglected (Bourrier, 2005; Busby, 1998). Only a few statistical data and lessons learnt have been presented (Hale et al., 2007b; Taylor, 2007b). As a result, there is not much design error information available to be used for the detection and elimination of accidents during process development and design. Therefore, in Paper III, an analysis of the design errors was carried out to identify the contribution of design errors to accidents. The timing of the design errors during design project was also studied.

8.1 The contribution of design errors to accidents

284 accident cases in FKD database related to piping, reactors, storage tanks, process vessels, heat transfer and separation equipment were reanalyzed to determine the contribution of design related errors to process accidents. In this study the design error definition by Taylor (1975) is used based on *"a design error is deemed to have occurred, if the design or operating procedures are changed after an incident has occurred".*

Therefore, a design error was committed if the accident report recommended changes in the process or its designed operating procedures. Both technical and procedural errors were included in this study but corrective actions due to human and organizational failures were not included. The errors were divided into 11 categories as described in Table 10. It should be noted that the design errors and the corrective actions proposed in accident reports are not equivalent. The reports tend to propose procedural changes for costing reasons even though there were technical design errors present (Refer Chapter 11).

The study found that approximately 79% (224 out of 284) of accident cases were involved in at least one design error. Majority of these cases (72%) had multiple design errors resulting in 526 errors in total, with an average of 2.35 design errors per accident. 59% of the design errors involved changes in equipment or process such as change in layout, replacement of construction material, re-sizing etc. The remaining

41% were classified as non-hardware related changes including equipment setting, automation, design documentation etc. The results of the analysis are presented in Table 11.

The result on the contribution of design errors on accidents was 79% and this is slightly higher compared to previous studies which were 70% (Drogaris, 1993; HSE, 2003). The difference can be explained by a more detailed analysis where 2.35 design errors per case was discovered as compared to Drogaris' 1.4 and HSE's study with 1.3 design errors per case.

Table 10: Classification of design errors

Design error	Description
Process condition	Inappropriate process condition selection due to lack of knowledge/data, inadequate analysis, wrong assumption/interpretation of process data, environmental/ surrounding input overlook/ignored etc.
Reactivity/ incompatibility	Lack of analysis of chemical reactivity and incompatibility hazard at normal and abnormal process conditions as well as an ignorance of possible process contamination, unintended chemical mix-up and process/environmental changes.
Unsuitable equipment/ part	Unsuitable equipment, components or parts selection that creates operational problems (e.g. wrong application, uneven flow or blockage) or increase the risk of accidents.
Material of construction	Wrong specification of material construction selection in term of physical, mechanical, chemical resistance and environmental/ surrounding characteristics.
Sizing	Inappropriate sizing (oversize or undersize) of process equipment and its piping system that affect their function and reliability during normal and abnormal process conditions (e.g. flow related or two-phase phenomena)
Utility set-up	Wrong utility selection and its realization especially related to maximum heating/cooling capacity, incompatible heat transfer medium and its flow/handling/control mechanism.
Protection	Inadequate design for safety due to lack of analysis and limited process information especially related to thermal safety, relief types and sizing as well as overall mitigation system.
Layout	Errors on plant layout, physical arrangement, positioning, equipment accessibility, visual obstacles, operator/technical interface and color-coding etc.
Automation/ instrumentation	Inadequate automation and instrumentation especially during abnormal process conditions for proactive process deviation/hazard detection, response and mitigation.
Operating manual	Wrong work procedures that jeopardize the safe operation of process equipment such as wrong sequence of work, wrong/unclear direction/ instruction, and wrong hand tool or material used.
Fabrication/ construction/ installation	Design oriented problems related to welding defect, thermal expansion phenomena, stress, and miss-match of process equipment with their connectivity. Some of major equipment has a long delivery time that needs to be ordered early. In some cases, their detailed design is not fit to as built.

Table 11: Distribution of design and operational errors per equipment type

Design errors	Piping system	Reactor	Process vessel	Storage tank	Separation eq.	Heat transfer eq.	Total	%
Layout	44	9	12	14	3	7	89	17
Reactivity/incompatibility	4	17	29	4	22	7	83	16
Process condition	10	16	15	3	25	13	82	16
Protection	9	12	19	17	8	7	72	14
Construction material	37	5	3	11	1	3	60	11
Utility set-up	1	13	4	7	11	4	40	8
Unsuitable equipment/part	3	7	10	13	3	3	39	7
Fab/const/installation	11	2	4	5		7	29	6
Automation/instrumentation		11			3	1	15	3
Sizing		5	3		1	1	10	2
Operating manual	1	3		3			7	1
Total	120	100	99	77	77	53	526	100

8.2 Most common types of design errors

Table 11 summarizes the contribution of various types of design errors to process equipment accidents. The most common design errors are associated with poor process layout (17% of design errors), followed by inadequate analysis of chemical reactivity & incompatibility (16%), incorrect process conditions selected (16%), and lack of protection (14%).

The ranking variation is dependent on the type of equipment. In piping systems, the most common design errors are related to poor layout (44 cases) and unsuitable construction materials (37 cases). Typical errors in reactor design are inadequate safety analysis on chemical reactivity & incompatibility (17 cases) and process conditions selection (16 cases). In many cases, the design errors are inter-correlated with chemical reactivity, stability, incompatibilities, and process deviations.

Design errors of separation equipment and process vessels are very similar to reactors i.e. chemical reactivity & incompatibility, process conditions and protection system. In storage tank designs, the usual errors are lack of protection (17 cases) and poor layout (14 cases). Meanwhile, the most significant design errors associated with heat transfer equipment are inappropriate process condition (13 cases).

The root causes of the design errors are presented in Appendix 1 of Paper III. On average, the most common root causes of design errors are process contamination, (5.1%), physical arrangement (4.0%) and reactions with contaminants (3.8%) (Refer to Table 4 in Paper III).

8.3 Timing of design errors

In Paper III, the design errors were linked with design project stages by determining their time of occurrence in a typical design project based on the usual schedule of plant design activities (Table 1 in Chapter 4). The design decisions give the timing for the corresponding design errors. Since design involves both preliminary and final decisions, the time of design error committed was selected to correspond to the time of *final* design decision (Table 12). The frequency of the design errors in each stage identified was based on Tables 11 and 12. The number of design errors during each plant design stage is presented in Figure 13 and in more detail for each error category in Figure 3 of Paper III. The details of errors in each stage are presented in Appendix 2 of Paper III.

Table 12: Origin of design errors based on final design decisions.

Design errors	Piping system	Reactor	Process vessel	Storage tank	Separation eq.	Heat transfer eq.
Process condition	P	R&D	P	P	P	P
Reactivity/incompatibility	P	R&D	P	P	P	P
Unsuitable equipment/part	D	P/D	P/D	P/D	P/D	P/D
Construction material	B	B	B	B	B	B
Sizing	B	B	B	B	B	B
Utility set-up	B	B	B	B	B	B
Protection	B	B	B	B	B	B
Automation/instrumentation	B	B	B	B	B	B
Layout	D	B	B	B	B	B
Operating manual	D	D	D	D	D	D
Fab/const/installation	C&S	C&S	C&S	C&S	C&S	C&S

Note: *R&D - Research and Development; P - Preliminary Engineering; B - Basic Engineering; D - Detailed Engineering; C&S - Construction & Start-Up.*

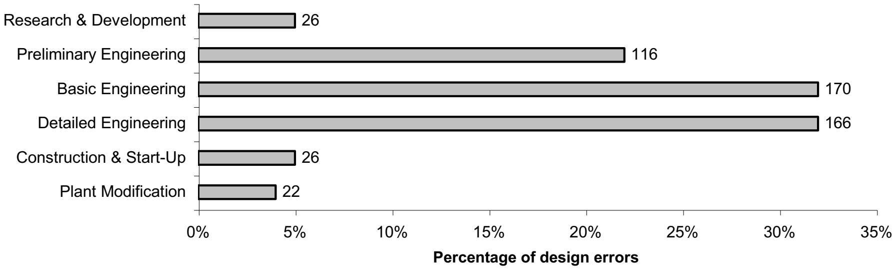


Figure 13: Number and share of the design errors throughout plant lifecycle. (Total of design errors = 526).

According to Figure 13, the majority (59%) of the design errors occurred in the process design related phases: basic engineering (32%), preliminary engineering (22%) and research and development (5%). Errors in detailed engineering were also significant (32%). However, design errors during construction & start-up (5%) and in later plant modifications (4%) were low.

Design errors originating from research and development (R&D) were low but high at the preliminary engineering and highest at the basic and detailed engineering phases. The reason for this is related to the number of design decisions made at each stage. In R&D, few but large conceptual decisions are made on process route and operating conditions. In R&D and preliminary design, almost all of the design errors are related to process condition and reactivity & incompatibility (Refer Figure 3 of Paper III). In the later phases, the number of decision parameter categories increased when more design decisions were made at the equipment level with reference to dimensioning, positioning and processing conditions; which had created a large number of design errors.

8.4 Points to look for in a safer design

Figure 3 in Paper III provides the details on the frequency and timing of design errors. These values represent the importance of each design error category in the design stages. Table 13 summarizes the most frequent design error types, which should be the focus at each design stage. The most frequent design error categories have been marked with five asterisks. The most error prone design aspects are; selection of process conditions and consideration of reactivity & incompatibility issues in preliminary engineering, and the selection of layout and equipment protection in detailed engineering.

Proper consideration should be given to fundamental decisions at the early stages of plant design due to their effect at the later stages. Errors made such as in reaction system specification create more errors at the basic engineering stage and even more in the detailed design. If proper process analysis is carried out at the early phase of process development and design, the combinatorial explosion of effects of erroneous process data can be eliminated at the later design stages.

Table 13: Priority list for design error elimination

Error category	Conceptual & preliminary design	Basic engineering	Detailed engineering	Construction & start-up
Layout		**	****	
Process conditions	*****			
Reactivity & incompatibility	*****			
Protection		*	***	
Construction material		***		
Utility set-up		**		
Fab/const/installation				*
Unsuitable equipment/part			*	

***** = high priority; * = low priority

9 Timing and Origin of Equipment Design and Operation Errors

Although the importance of early safety and design evaluation is known, the lifecycle aspect of process safety has not been given much attention by researchers. Therefore, there is very limited process safety knowledge from lifecycle perspective available in the literature. Thus, the aim of Paper IV is to conduct out deeper analysis on the lifecycle aspects of process safety and design.

9.1 Design and operational errors of process equipment

To study the design and operation errors in process lifecycle, design errors and their origins were studied and presented in Paper III. The paper was extended to include operational and plant modification faults in the operation phase. Table 14 shows the frequencies of accidents causing errors based on the six main types of equipment. In total, 661 errors were found in the 284 accident cases with an average of 2.3 accident contributors per accident.

Table 14: Distribution of design, operational and external causes to process equipment accidents (661 contributors in 284 accidents)

Accident contributors	Piping system		Storage tank		Reactor		Process vessel		Separation eq.		Heat transfer eq.		Total	
	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Layout	44	27	14	11	9	8	12	11	3	3	7	11	89	13
Organizational failure *	26	16	25	20	12	11	10	9	6	7	8	12	87	13
Reactivity/incompatibility	4	2	4	3	17	15	29	26	22	26	7	11	83	13
Process condition	10	6	3	2	16	14	15	14	25	29	13	20	82	12
Protection	9	5	17	14	12	11	19	17	8	9	7	11	72	11
Construction material	37	22	11	9	5	4	3	3	1	1	3	5	60	9
Utility set-up	1	1	7	6	13	12	4	4	11	13	4	6	40	6
Unsuitable equipment/part	3	2	13	11	7	6	10	9	3	3	3	5	39	6
Human failure *	15	9	11	9			2	2	3	3	4	6	35	5
Fab/const/installation	11	7	5	4	2	2	4	4			7	11	29	4
Automation/instrument					11	10			3	3	1	2	15	2
External factors *	4	2	9	7									13	2
Sizing					5	4	3	3	1	1	1	2	10	2
Operating manual	1	1	3	2	3	3							7	1
Total / overall percentage	165	25	122	18	112	17	111	17	86	13	65	10	661	100

**) in plant operation*

80% of the errors are design oriented whereas 18% are organizational and human errors in the operation stages and 2% are external factors. The results correspond to Table 11 and the operation errors and external factors have also been included in the table. Organizational errors in operation stage represent 13% of all errors and rank second. Based on the statistics of equipment type accident, storage tank accidents are due to organizational errors. Human failures at the operation stage represent only 5% of the overall errors; however at specific equipment types, they are a burden for piping and storage tank operation (both 9% of accidents). External factors contribute about 2% of errors, which mainly affect storage tank safety problems caused by earthquakes.

9.2 Design and operation errors of equipment in plant lifecycle

The design and operational faults found for the equipment types in Table 14 were linked to their time of occurrence during the process design and operation lifecycle. To identify the timing of errors, a similar approach is used in Paper III which is described in chapter 8, inclusive of the operating and plant modification stage errors. The results are presented in Table 15.

In Table 15 the average number of errors are divided quite evenly, approximately 20% - 25% each, which are classified as R&D/preliminary, basic, detailed engineering and operation phases. However, separators, process vessels and reactors have the most number of accident leading faults at the early design phases (i.e. research & development; preliminary and basic engineering), while storage tanks, piping and heat transfer equipment have more faults at the later phases (i.e. from detailed engineering onwards).

Each type of process equipment has specific fault characteristics. Storage tanks and piping system are prone to failures with poor operations. Process vessels and separation equipment resemble their fault profile whereby both are sensitive to poor decisions made at the conceptual design stage. Piping, reactors and heat transfer equipment are most sensitive to faults in basic engineering. Reactor design is also affected by the R&D stage data (chemical reactivity, thermal safety etc.) Storage tanks are sensitive to errors in detailed engineering. Heat transfer equipment has a quite even distribution of error sources at the design and operation stages.

Table 15: Time of origin of design and operational faults for process equipment

Design phases	Piping system		Storage tank		Reactor		Process vessel		Separation eq.		Heat transfer eq.		Total	
Research & development *					26	23%							26	4%
Preliminary engineering *	10	6%	8	7%	2	2%	42	38%	41	48%	13	20%	116	18%
Basic engineering *	56	34%	15	12%	31	28%	31	28%	21	24%	16	25%	170	26%
Detailed engineering	45	27%	50	41%	28	25%	21	19%	15	17%	13	20%	172	26%
Construction & start-up	6	4%	7	6%	2	2%	5	5%		0%	6	9%	26	4%
Operations – H&O failures	45	27%	39	32%	12	11%	12	11%	9	10%	12	18%	129	20%
Plant modification	3	2%	3	2%	11	10%					5	8%	22	3%
Total	165	100%	122	100%	112	100%	111	100%	86	100%	65	100%	661	100%
* Share of process development & design	40%		19%		53%		66%		72%		45%		48%	

Note: H&O – human and organizational

Preliminary design (including R&D) is the most important design step for separation equipment and process vessels. On other hand, basic engineering is the most critical part of the design for piping system while detailed engineering is important for storage tanks. For reactors and heat transfer equipment, all the design stages are equally important. In the operation stage, many errors are made during piping and storage tanks operations. Reactors are subject to many design errors in plant modification. Paper IV discusses in more detail the design and operation errors for the six main equipment types in the lifecycle stages. The detailed statistics are in Appendix 1 of Paper IV.

9.3 Most frequent errors and their timings

The most frequent design and operation errors involved in process equipment accidents were identified based on the accident data presented in Tables 14 and 15. The data were plotted to present the frequency of accident-causing faults in process lifecycle phases (Refer Figure 1 in Paper IV). This mapping is useful in identifying the critical accident contributors of equipment design and providing the typical timing of the design errors. The results are summarized in Table 16.

Table 16 presents the most frequent design and operation errors for the process lifecycle stages. The number after the accident contributor presents the frequency showing how often the contributor was present in the accident data. The most frequent general contributors are listed for each stage as well as the same contributors that are present for most of the equipment types.

The R&D and pre-design in Table 16 show the most important contributors which are process contaminants and secondary reactions that had caused unexpected reactions and corrosion problems. These contributors are relevant for nearly all the types of equipment. Therefore, to prevent similar accident related to process contaminants and secondary reactions, it is important to check the reaction chemistry and the actual composition of the feedstock chemicals used during design.

In the basic engineering, the main design errors are mechanical and chemical specifications of equipment as well as the physical arrangement of piping and equipment. Lack of knowledge on process chemistry and chemicals causes a significant amount of design errors in the basic engineering too, such as unsuitable materials for construction.

In detailed engineering, the most common contributors are related to flammability i.e. inert gas blanketing and static electricity prevention. In construction and start-up, the quality of fabrication and prevention of mechanical stress in equipment and piping are important. In the operation phase, lack of physical checking, and lack of inspection & maintenance are the most critical faults causing a significant amount of equipment failures. In later modifications, there are various contributors to accidents especially regarding reactors. Details are provided in Appendix 1 of Paper IV.

Information given in Table 16 can be used for supporting design by identifying the aspects commonly overlooked in design projects and current risk analyses.

Table 16: List of most frequent design and operation errors per lifecycle stage for chemical process equipment

Equipment	Piping system	Storage tank	Reactor
Process R&D and Pre-design	- Process contaminations, 6		- Reaction with contaminants, 4 - Process contaminations, 3 - Uneven flow/dry condition, 3 - Reactive heat transfer medium, 3
Basic Engineering	- Mechanical specification, 13 - Chemical specification, 11 - Physical arrangement, 9 - Sizing/ Thickness, 7 - Shared piping, 4 - Single valve, 3	- Physical arrangement, 3 - Friction/ impact, 3 - Flammable sealing/ cleaning agent, 3	- Extreme heating/ cooling source, 4 - Physical arrangement 4 - Chemical resistance spec, 3 - Lack of detection by automation, 3
Detailed Engineering	- Physical arrangement, 9 - Dead end, 8 - Support arrangement, 5 - U-shape, 5 - Flow restriction, 3	- Spark-generating parts, 9 - No nitrogen blanket, 8 - Static electricity, 7 - Non-conductive part, 6	- Setting error, 4 - No nitrogen blanket, 4 - Feeding mechanism, 4 - Maintenance/repair (operating manual), 3
Construction & start-up	- Bolt tightening related, 2 - Poor fabrication/ construction quality, 2	- Stress concentration3	- Welding defect, 2
Operation	- Contractor mgt/ control, 5 - Lack of maintenance, 5 - No double & physical check, 4 - Work permit related, 3 - Poor mgt system, 3 - No problem-reporting system, 3	- Poor planning, 5 - Lack of maintenance, 5 - Lack of analysis, 4 - Misjudgment, 4 - Not following procedure, 4 - No double & physical check, 4	- Lack of analysis, 3 - No double & physical check, 2
Modification			Various, 11

Note: The numbers show the frequency of the accident contributors

Table 16: *cont…*

Process vessel	Separation eq.	Heat transfer eq.	**All**
- Reaction with contaminants, 6 - Secondary reaction, 6 - Process contaminations, 6 - Hazardous material generated, 4 - High temperature, 3 - Waste handling, 3	- Process contaminants, 7 - Reaction with contaminants, 7 - Secondary reaction, 7	- Process contaminations, 3	**- Process contaminants, 26** **- Reaction with contaminants, 17** **- Secondary reaction, 13**
- Friction/impact, 3 - Physical arrangement, 3	- Incompatible heat transfer medium, 3 - Utility set-up: various	- Incompatible heat transfer medium, 3 - Single valve, 2	**- Mechanical & chemical spec., 27** **- Physical arrangement, 19** **- Sizing, 7** **- Incompatible heat transfer medium, 6**
- Non-explosion-proof, 4 - Static electricity, 4 - No nitrogen blanket, 3	- Static electricity, 3 - No nitrogen blanket, 2 - Sensor failed, 2	- No nitrogen blanket, 2 - Static electricity, 2	**- No nitrogen blanket, 19** **- Static electricity, 19**
- Poor fabrication / construction quality, 3		- Stress concentration, 4	**- Mechanical stress, 7** **- Poor fabrication/ construction quality, 5**
- No double & physical check, 3 - Lack of analysis, 2	- No double & physical check, 2 - Not following procedure, 2	- Not following procedure, 3 - Lack of inspection/testing, 2	**- No double & physical check, 15** **- Lack of maintenance / inspection/testing, 12** **- Lack of analysis, 9** **- Not following procedure, 9**
		Various, 5	

10 Method for Accident Contributor Identification

Papers I - IV show that design is a major contributor to accidents. Nearly 80% of accidents have design as a contributor and based on other studies (Duguid, 2001; HSE, 2003) in 50% - 60% of these cases, it is the primary cause (Paper III). As discussed in the previous sections (Section 1 and 3), earlier utilization of existing knowledge can prevent most of these accidents. In other words, available accident knowledge was not fully utilized to recognize the risks. The accident databases were not usable in practice for the normal engineering work, since the compiled information was scattered and not in a user-friendly format as discussed in Chapter 3. Therefore, in Paper V, a design oriented accidents contributor identification method is proposed. The aim is to disseminate existing accident knowledge into a design for hazard identification in a practical way.

10.1 Limitations of current design oriented methods

There are several well-accepted safety analysis methods available for design as discussed in Chapter 4. Since most of the current safety and design review methods have limited applicability at the early phase of plant design project, the benefits to detect and eliminate the accident contributors at an early stage of plant design cannot be done.

The existing safety review methods eliminated 80-95% of design errors (Taylor, 2007a) but there is still a design element present in most (80%) of accidents in industry (Refer Paper III). Besides that, the applicability of many existing safety/design methods (i.e. HAZOP, F&EI etc.) were limited in the early phases of plant design due to lack of process information (Hurme and Rahman, 2005; Kidam at el., 2008a).

HAZOP is rather effective in removing process engineering related faults but the problem is that HAZOP is applied typically at a time when it was too late. HAZOP is used when all the process design is quite ready and any process design related changes will be expensive. From the mechanical engineering point of view, HAZOP is done too early, since detailed design has not been done or completed. For this reason, HAZOP lacks the lifecycle point of view. Therefore, an additional lifecycle based approach for enhancing process safety is needed.

10.2 Method development

The method for accident contributor identification of chemical processes is illustrated in Figure 14. The purpose of the method is to identify the accident contributors throughout the process lifecycle and evaluate their importance in causing accidents. The method consists of five main steps and the evaluation is based on process equipment types. Detailed description of the method is in Paper V.

In Step 1, equipment type is selected. Then in Step 2, the relevant accident contributors and their root causes are identified. This is based on the most *frequent accident contributors* of the equipment identified as well as their frequency of occurrence in the earlier CPI accidents. These include both main and sub contributors with their root causes as presented in Table 5 (Chapter 7.1). A detailed accident ranking is provided in Appendix 1 of Paper II. Next, the most *frequent main contributors* (MC) to accidents are identified by using Table 6 (Chapter 7.2). The main contributor of an accident is the one that triggers and plays a major role in the accident. Besides that, the less frequent but *specific contributors* are also identified. This identification is based on the contributors, which are much more frequent than average in the accidents of certain equipment types. Table 8 (Chapter 7.4) gives the more frequent than average contributors for each equipment type.

The *share as main contributor* (SMC) to accident is also identified and ranked in Table 6. The SMC presents the capability of a contributor to cause an accident possibly by itself (Refer Paper I). These contributors are obviously crucial in accident prevention. Since SMC does not present the frequency because some of the high SMC contributors may rarely occur. Therefore, Paper II 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. These high-risk contributors, which are frequent and often act as main-contributors are summarized in Table 9 (Chapter 7.5).

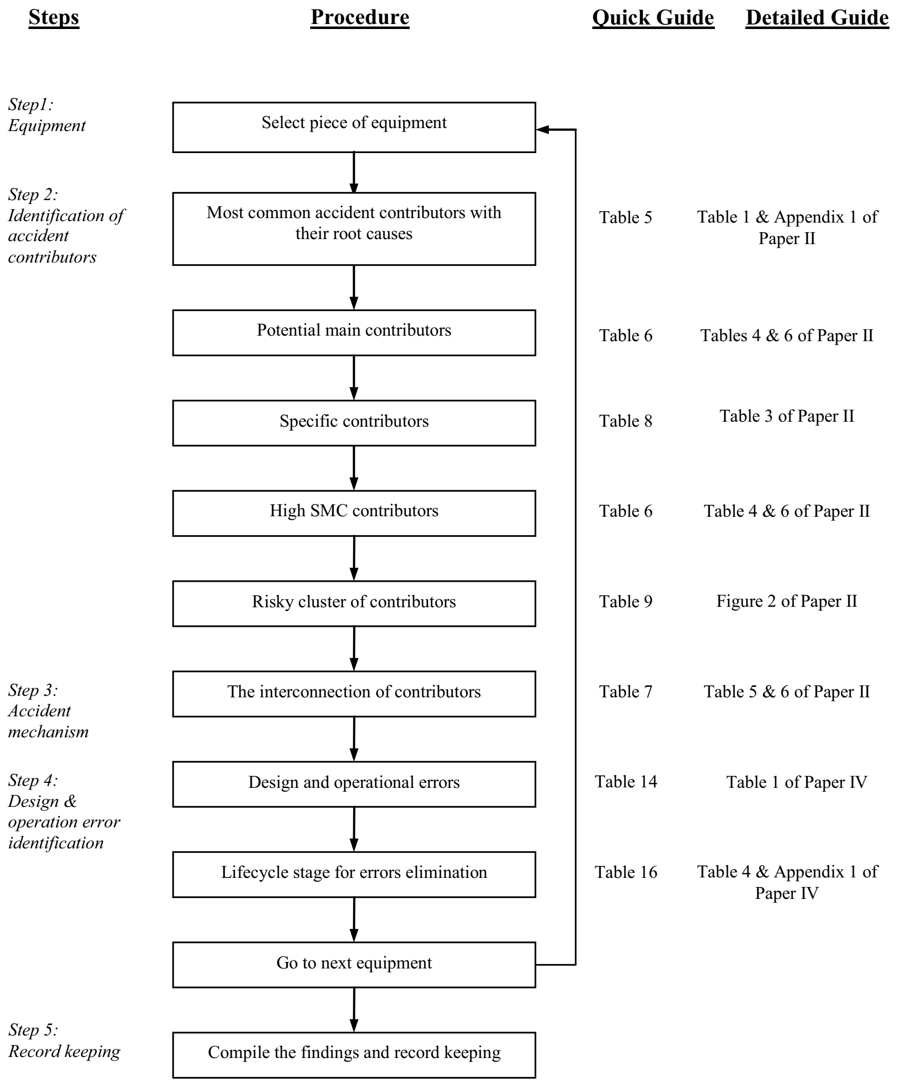

Steps
Procedure
Quick Guide
Detailed Guide
Step1:
Equipment
Select piece of equipment
Step 2:
Identification of accident contributors
Most common accident contributors with their root causes
Table 5
Table 1 & Appendix 1 of Paper II
Potential main contributors
Table 6
Tables 4 & 6 of Paper II
Specific contributors
Table 8
Table 3 of Paper II
High SMC contributors
Table 6
Table 4 & 6 of Paper II
Risky cluster of contributors
Table 9
Figure 2 of Paper II
Step 3:
Accident mechanism
The interconnection of contributors
Table 7
Table 5 & 6 of Paper II
Step 4:
Design & operation error identification
Design and operational errors
Table 14
Table 1 of Paper IV
Lifecycle stage for errors elimination
Table 16
Table 4 & Appendix 1 of Paper IV
Go to next equipment
Step 5:
Record keeping
Compile the findings and record keeping

Figure 14: Flow chart of the accident contributor identification methodology (Refer Paper V).

In Step 3, the detection of potential accident *mechanism* is carried out. As mentioned in Paper I and illustrated in Figure 9, (Chapter 6.5) certain accident contributors have a tendency to act together in accidents. At equipment level, the interconnection data are summarized in Table 7 Chapter 7.3) and the details are in Paper II (see Tables 5 and 6).

Next, in Step 4, the possible *design and operation errors* are identified by using Table 14. (Chapter 9.1). Identification is based on the statistical frequency of errors for different equipment types as presented in Appendix 1 of Paper III. Later, the design errors are linked to the process design lifecycle by identifying their *time of occurrence* during design and operation activities. This can be done based on the statistics on the frequency and time of the error, as shown in Table 16 (Chapter 9.3). The aim is to prevent the same errors from being repeated. In this case, the design error timing points out the time in the plant lifecycle when accident contributor elimination should be done.

In the method presented in Figure 14, continuous evaluation for each design stage is done 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 provide ideas on appropriate hazard elimination and risk reduction strategies. This can be done by using a hierarchy of controls such as inherently safer, add-on engineered and procedural levels.

10.3 Method demonstration and test

The method of identifying accident contributors throughout the process lifecycle is demonstrated and tested using the Bhopal tragedy case study presented in Paper V. The Bhopal gas tragedy was the worst industrial accident in the world killing over 2000 persons immediately and injuring more than 200,000 persons in 1984 in Bhopal, India.

In the process, methyl isocyanate (MIC) was an intermediate to produce 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 reacted with the water in an exothermic way. The reaction was catalyzed by rust and other compounds. 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, a large amount of MIC gas leaked. The leaked gas spread towards the city zone covering residential areas and causing the casualties (Chouhan, 2005; Mannan, 2005).

The method of identifying accident contributors was applied to the MIC storage tank T610. Although T610 is a storage tank, its function, structure and operation resemble more than a process vessel. Therefore, the equipment types selected in Paper V to represent tank T610 were 'pressure vessel' and 'storage tank'. Besides that, the piping system was also analyzed. Paper V presents the assessment steps for T610 as a 'process vessel'.

The result of the method test for pressure vessel is summarized in Table 17. In the contributor category, contamination (14 cases) was the largest accident contributor identified. The next contributor was the reaction contributor (12 cases) with its root cause as unwanted reaction, due to contamination. These were largely the main contributors, relatively high contributors and SMCs aspects. The mechanism of accident proposed by the interconnection study (Step 3) was therefore: human & organizational – contamination – reaction – heat transfer problems.

Table 17: Results of Bhopal T610 analysis as a pressure vessel

Steps	Parameters	Findings
1	Equipment types	Process vessel
2a	Accident contributors (Table 5)	a. Contamination, 14 cases – flow-in, 8 cases; human/technical interface, 4 cases. b. Human & organizational, 12 - organizational failure, 10; no procedure/check, 3. c. Reaction, 12 – unwanted reaction, 9; contamination, 3. d. Flow related, 10 - human/technical interface, 3.
2b	Main contributors, MC (Table 6)	a. Contamination, 13 b. Flow related, 5 c. Human & organizational, 5 d. Heat transfer, 4
2c	Specific contributors (Table 8)	a. Static electricity, 2.1 times more than average b. Reaction, 2.0 c. Contamination, 1.6
2d	High share as main contributor, SMC (Table 6)	a. Corrosion, 100% b. Fabrication/construction/installation, 100% c. Contamination, 93%
2e	Cluster analysis (Table 9)	a. Contamination b. Flow related c. Heat transfer
3	Accident mechanism (Table 7)	a. Contamination – reaction, 5 b. Heat transfer – reaction, 4 c. Contamination – human & organizational, 3
4a	Design and operation faults (Table 14)	a. Reactivity/incompatibility, 29 – reaction with contaminants, 6 b. Protection, 19 – lack of ignition source control, 11 c. Process condition, 15 – reaction with contaminants, 6.
4b	Lifecycle location (Table 16)	a. R&D, preliminary – reaction with contaminants, 6; secondary reaction, 6; contamination, 6; hazardous material and heat generation, 4; high temperature, 3 b. Basic design – physical arrangement, 3 c. Detailed design – non-explosion proof, 4; static electricity, 4

Based on the findings in Table 17, the vessel based assessment strongly shows (Step 2 - 4a) that contaminations was the major accident contributor and had a connection with the unwanted chemical reaction in the vessel. Furthermore, the result shows that these accident contributors should have been identified and controlled at the early stage of design project i.e. at the research & development and preliminary engineering stages (Step 4b).

The accident contributors were also analyzed by using equipment types 'tank' for the T610 as well as piping. The results were compared with the actual Bhopal accident contributors in Table 18. These were extracted from the data from Chouhan et al. (2004) and Chouhan (2005). The critical accident contributors for each piece of equipment were identified from their data and presented as the underlined frequency in Table 18.

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

Piping, the relevant accident contributors and faults were found and shown in Table 18.Following that, the accident mechanism can be predicted. In 'tank' analysis, the contamination was not found as a contributor, neither was the inventory aspect as a design error nor the procedures as the operating errors. For the 'vessel' analysis, all but two of the contributors were found to be weak. Besides that, neither inventory as design error nor procedures as operating error was found. The accident mechanism was only partly predicted in the tank option whereas the vessel option gave a better prediction.

Table 18: Comparison of the method results with the real accident.

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

Note: X = high frequency; (X) = low frequency; - = not relevant; O = did not found; underlined = actual critical contributors

Table 19 summarizes the prediction capability of the method.. Piping can best be predicted with an average of 95% accuracy. The storage tank option has the least prediction capability at approximately 50%, because T610 is not a normal storage tank. The average prediction capability is 86% for piping and vessel, and 75% if the tank is included as an option. The accident contributors are the best predicted aspects with 90% to 100% accuracy.

Table 19: Comparison of predicted accident parameters with the actual parameters (%)

Accident parameters	1) Piping system	2) Process vessel	3) Storage tank	Average 1&2	Average 1, 2 & 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	100	100	50	100	83
Average	95	77	52	86	75

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

11 Corrective Actions Analysis

Paper VI discusses the corrective actions proposed in accident reports after the accidents. The 364 CPI-related accident cases available in the FKD database were studied. 15 cases were classified as unknown because of insufficient information.

11.1 Hierarchy of control

Corrective actions of the accident report was analyzed to find out the risk reduction strategies proposed to prevent accidents. It was found that the CPI normally took several corrective actions due to multiple causes of accident. In this analysis only single corrective actions were counted and the actions were classified according to the priority of risk management strategy: inherently safer > passive > active > procedural (see Chapter 2.4). Analysis of known cases (349 cases) showed that the corrective actions taken were about equally shared between procedural (53%) and engineered (47%). In the engineered strategy, 18% of them were categorized as an inherently safer, followed by active engineered (16%), and passive engineered (13%).

The results can be compared with the work done by Amyotte et al. (2011) who investigated the hierarchy of control by analyzing 62 accident cases from Chemical Safety and Hazard Investigation Board (CSB) database. As shown in Table 20, they found a higher share (36%) of inherently safer category, which is double the result of the present study. The reasons for this difference may be due to the analysis done and the database used. CSB database covers relatively new accidents in the USA whereas FKD database includes both old and new (1964-2003) accidents nearly all from Japan. Since the uptake of the inherent safety was slow in the earlier stage (Gupta and Edwards, 2002), the time of accident may have an effect on the corrective action recommended in the accident report. In the USA, ISD is better known and even required by some counties as an accident prevention strategy.

Table 20: Corrective actions taken by CPI to prevent accidents

Hierarchy of control	Amyotte et al. (2011), %	Paper VI, %	Average, %	Cumulative, %
Inherently safer	36	18	27	27
Passive	8	13	10.5	37.5
Active	14	16	15	52.5
Procedural	42	53	47.5	100

The results reflect the transition from the earlier accident prevention strategies, which are mostly procedural as part of the ISD based strategy. There are increases ranging from 18% to 36%. It is noteworthy that accident reports in FKD database proposed approximately 50% procedural improvements, even though the share of design errors is about 80% of accidents based on Paper III. This could be due to the design changes which are more costly compared to procedural changes.

11.2 Inherent safety keywords

The usage of inherent safety keywords were also analyzed (Refer Paper IV). 18% of accidents were corrected by using ISD strategy. The corrective actions were classified into six main ISD keywords presented in Table 21. The distribution of the keywords used to prevent accidents is presented in Figure 15. The usage of the ISD based on keywords is led by moderation and error tolerance keywords (27% for both); followed by substitute (21%), simplify (13%), minimize (10%), and limitation of effects (2%).

Table 21: Inherent safety keywords used and their strategy to manage risk

Keywords	ISD strategy
Minimize	Design a process or equipment that uses smaller quantities of hazardous substances with limited energy generation capabilities.
Substitute	Avoid hazardous substances or processes and if not applicable, replace with a less hazardous one.
Moderate	Select safer process conditions (i.e. temperature, pressure and concentration) and chemical handling mechanism (i.e. safer physical form and mode of operation).
Simplify	Design a process, equipment or system that is simple, user friendly and easy to operate.
Error tolerance	Designing reliable and robust (i.e. chemically, mechanically and physically) process equipment and its piping system that resist misuse, mal-operation, poor maintenance, and process deviations/changes.
Limitation of effect	Design a process or equipment based on worst-case scenario that protects and mitigates the process hazards by default if an unwanted event occurs.

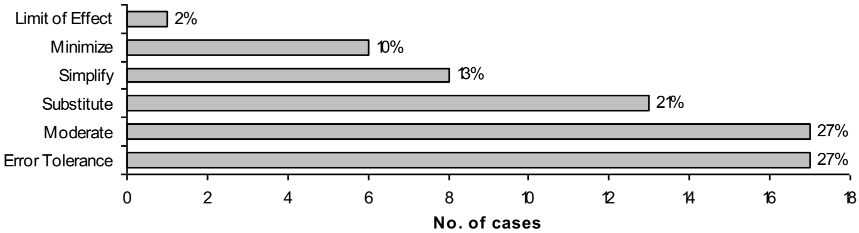


Figure 15: Inherent safety corrective actions taken by the CPI based on ISD keywords.

Based on the results of ISD usage in corrective actions of accidents, a fishbone diagram (Figure 16) was developed to illustrate the accident prevention through ISD keywords (Kidam et al., 2008b). The fishbone can be used as an idea generation for applying ISD principles into practice.

As seen from Figure 16, the error tolerance keyword shows that the majority of actions have been taken to solve the design related errors such as wrong material selections, etc. Another aspect to be considered is the tolerance to operation or maintenance errors and designing a fail-safe system.

Meanwhile, the moderation strategy mainly aims to change the existing processing conditions to milder ones by manipulating the temperature, pressure, concentration and the physical state of the chemicals. Common applications are refrigeration, dilution and decreasing the chemical reactivity by operating at low temperature or low pressure, or introducing the inhibitor and stabilizer agents.

The substitute keyword is to lessen the hazards by using safer or compatible chemicals. Simplification can be achieved by creating highly reliable systems (no redundancy needed) and simpler process (in terms of complexity and interaction between units). Minimization can be achieved by intensifying the operation (low inventory etc.). Limiting the effects would often minimize impacts caused by passive measures (i.e. robust and separate systems).

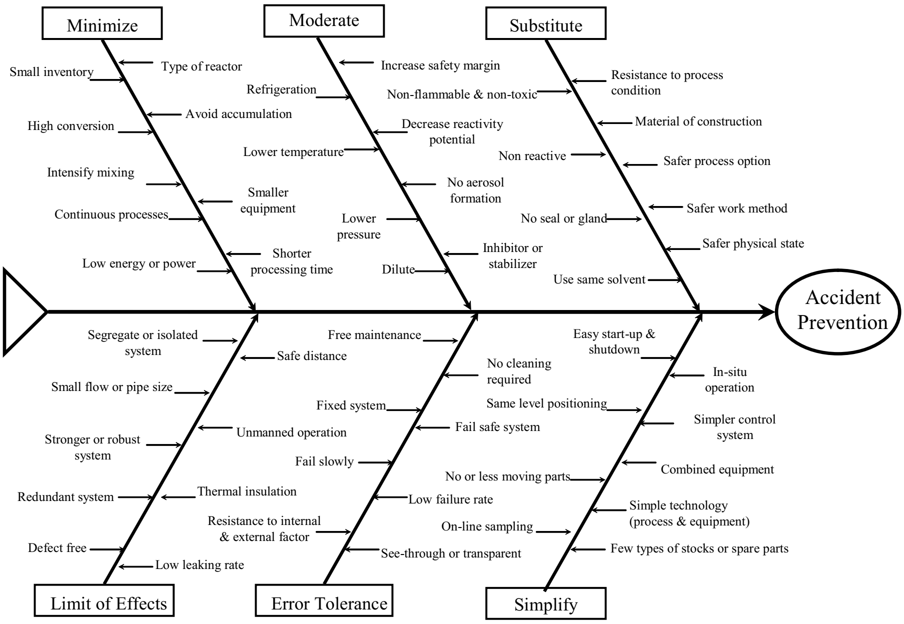


Figure 16: Fishbone diagram of accident prevention through ISD.

12 Discussion and Conclusion

The accident rate has not been decreasing in the CPI. However almost all the accidents (>95%) do have known causes and could have been prevented by using existing knowledge (Drogaris, 1993; Mannan et al., 2010). This shows that the existing knowledge was not used effectively because the same type of accidents recurred.

Learning from past accidents would be a powerful way of reducing accidents. After major accidents that happened in 1970s and 1980s, accident databases were created to disseminate accident information. Their usage has not been effective because of the presentation of accidents as case studies. Their knowledge should be analyzed and presented for higher level general conclusions. This has been done to some extent (e.g. Duguid, 1993) but lacks further analysis e.g. such as contributors on equipment level, their interconnections, presence of design errors and their timing. This should be done especially for the systematic use of accident information in design because this part of the analysis has been neglected.

The *aim of this thesis* is enhance experience feedback on design by increasing the general usability of the accident information. This is done by analyzing further, drawing general conclusions and creating an approach for its utilization during design for enhancement of safety in CPI. The role of design in accident prevention is done by analyzing the FKB database and studying it from four view points: 1) analysis of contributors of accidents and which equipment had the accident and why, 2) design and operating errors and what was designed or operated wrong, 3) timing of the errors, and 4) proposed corrective actions after the accidents.

The *contributors* were divided into three main categories: 1) technical contributors, 2) ‘purely’ human and organizational faults at the operation stage, and 3) external factors. The aim was to see which accident contributors was design related. Therefore the design category included all the contributors, which were related to the design stage and technical aspects, human & organizational faults in design, faults in operator-technical interface, and in designed procedures.

It was found that the share of technical accident contributors was dominant (79% of contributors). The result supported the average result published earlier which was 75% for technical contributors (Sales et al., 2007 and Drogaris 1993), when the same classification was used. The result shows that majority of the accidents could be affected by changes in the design stage. This is more apparent in the main contributors to accidents, which were found to be 83% caused by technical problems.

To utilize accident contributor information in accident prevention, their relative importance needs to be known. This can be based on various criteria; 1) contributor frequency, 2) main contributor frequency, 3) the contributors share as main contributor (SMC), 4) equipment specific contributors, 5) combination of high SMC and frequency (cluster 1 contributors). This is based on the idea that the role of main contributors is essential and they are capable of causing accidents by themselves although there are typically several contributors to an accident. The sub-contributors have a supportive role only.

The thesis is able to identify the contributors in general and specifically for each of the six most common equipment types studied. These six equipment types represented approximately 80% of all accidents. The most common contributors found in general were human & organizational (19%), process contaminations (11%), flow-related aspects (11%), and heat transfer (10%).

In addition, the mechanism of accident needs to be eliminated. The interconnection of main and sub-contributors can be used for this purpose. These interconnections were analyzed in general as compared to the six equipment types which were specifically studied in the thesis.

Another point to be reviewed is the *design and operation errors* by looking at what was designed or operated wrongly and when the error was done. A broad definition of design error was used here whereby if the accident report proposed changes in process or its designed procedures, the design error would be considered to have occurred.

The study found that about 80% of the accident cases were contributed by at least one design error. This finding was higher than the ones found in the earlier studies which was 70% (Drogaris, 1993 and HSE, 2003). This could be due to the design oriented point of view of the study and the depth of the analysis. Majority of the accidents have more than one design error and the average design errors was 2.3 errors present per accident. The most common design error classes found were related to poor layout, followed by poor consideration of chemical reactivity & incompatibility and wrong process conditions selected. The most common underlying causes were process contaminations, physical arrangement, and reactions with contaminants.

The *timing of the errors* was analyzed by determining the time of the design decision, which caused the accident in a typical design project time schedule. It was found that nearly half (47%) of the *design and operation errors* were made in process design-oriented stages, one fourth (26%) in detailed engineering, and one fifth (20%) in operation. Process contaminants, reactions with them and secondary reactions were the most significant accident contributors in the early phase for nearly all types of equipment. The number of design errors done per design aspect was the largest in the preliminary design indicating that many errors were done in the fundamental process design decisions such as process conditions, chemicals and reactions involved. This clearly indicates that more focus should be given on these decisions at the early phase of the design to enhance safety. The most frequent errors and their timing were identified for each equipment type. This knowledge can be utilized by focusing on the hazard analysis in each stage of the most error-prone features of design. A points-to-look list was created for this purpose.

The *corrective actions* in accident reports were studied by analyzing which risk management strategy was proposed. It was found that the current approach of loss prevention mainly utilized the outer layers of protection, which were organizational and human-oriented. The most commonly proposed corrective actions after an accident were procedural changes (53% of cases) even the analysis of the background reasons showed that the design errors were generally dominant (80% of causes of accidents). The inherently safer design was proposed in 18% of the cases. More recent results by Amyotte et al. (2011) from CSB database found a higher share (36%) of ISD and less procedural corrective actions (42%). This may be because of the wide spread knowledge of ISD in USA lately. Generally, procedural corrective actions

were probably proposed because of their lower cost as compared to the engineering changes.
The ISD corrective actions proposed were studied in more detail based on which inherent safety keyword was adopted. It was found that the most used principles were ’error tolerance’ and ‘moderate’ (27% each). Keywords ‘substitute’, ‘simplify’ and ‘minimize’ were not commonly used. This is probably because of the late application of ISD i.e. after the accident. Therefore, it was not possible to do large changes to the process at this stage. This is based on the results of ISD usage as a corrective action illustrated in the fishbone diagram that was created to aid in the hazard reduction through ISD keywords.

The aim of the thesis is to transform the accident report information into practical applications by analyzing it and creating an approach that can be used for supporting the design activities. This transformation is needed, since the current design-oriented safety methods have limitations in their capability. They have not utilized the knowledge available from the earlier accidents and therefore did not enable knowledge cycle. As a result, similar accidents recur. The previous methods do not support the designer during the design work, since they lack the design lifecycle point of view. For example, HAZOP is typically utilized as a final check after the process design is completed. No significant design changes can be made at this point due to economic factors. Therefore, the cost benefits of making early changes are lost and most of the risk reduction is achieved by using add-on safety systems, which tend to complicate the process.

The restrictions in the traditional method pointed out the need for a new method to support the design process. The thesis presents a method for identifying accident contributors as well as design and operation errors. The method includes their causes and the timing of creation. The identification is done by using several techniques based on accident contributor and design error statistics presented earlier in the thesis. The identification is based on the most frequent accident contributors, main contributors and uncommon but specific contributors, which are capable of causing accidents by themselves. The accident mechanism is analyzed through the interconnection of contributors. Statistically, the most potential design and operation errors and their lifecycle timing are pointed out and shown in the design stage, where action should be taken to eliminate the accident contributor. The method should be used to complement existing methods such as HAZOP and not as an alternative.

The proposed 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. The proposed method can predict up to 85% of accident contributors, and design and operation errors if the type of equipment is selected correctly. Selection of equipment may be the main problem with the method especially when the process includes unconventional or novel types of equipment as there is no an earlier accident information available.

In conclusion, the thesis has presented new knowledge on the statistics of equipment based accident contributors, their background, the design errors involved and their timing and proposed a method for extended experience feedback to improve the dissemination of accident knowledge. The results confirmed that there is a high number of design based errors in accidents (approximately 80%), which can be removed (about 50%) by improved process design. The proposed method utilizes knowledge on accident contributors from earlier accidents by presenting a new method to eliminate accidents since the accident based information was not utilized systematically in earlier designs. Besides that, the design lifecycle point of view is novelty which makes it possible to start hazard identification in the early stages. The proposed method would lead to cost and safety benefits that can be achieved as a result of early process design changes. Figure 16 summarizes briefly the characteristics of chemical process design and their connections to accident contributors in the process lifecycle.

The limitation of the research presented is related to the source of accident knowledge, i.e. the database used. Even though the number of cases is large, there may have been distortion dues to the origin of accidents, which are mostly from one country. The Japanese chemical industry may not represent the world CPI average. Most of the study focused on to the six most common equipment types in accidents, which correspond to 80% of accident cases. Focusing on these equipment types may to a certain extent affect the generalization of the results. It is recommended that similar studies using other databases be carried out. Besides that, the effect of time of accidents on the contributors involved should also be studied since many safety efforts on this aspect have been taken in CPI during the last decade.

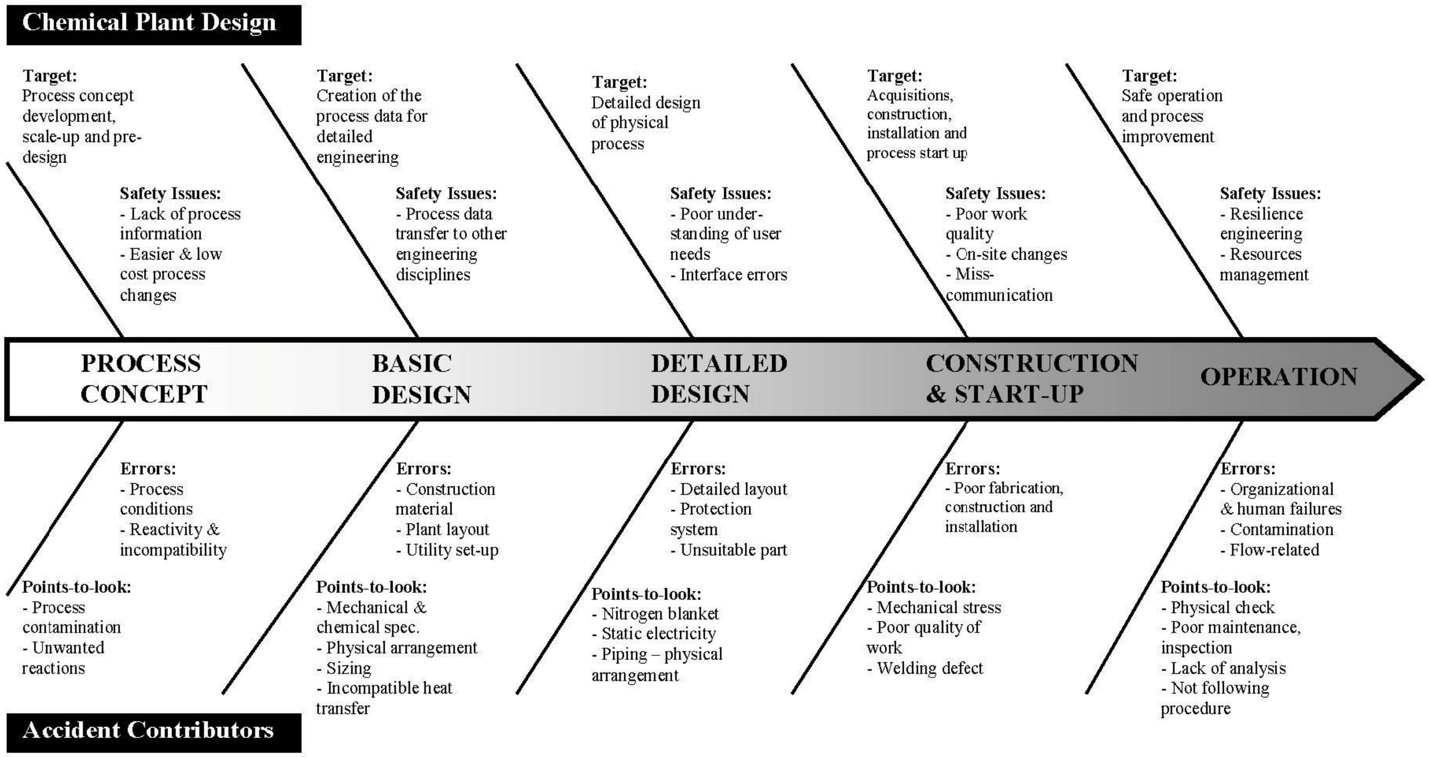


Figure 16: Chemical plant design and accident characteristics throughout process lifecycle.

References

Ackoff , R. L. (1989). From data to wisdom, *Journal of Applies System Analysis*, 16, 3-9.

Amyotte, P.R., MacDonald, D.K., & Khan, F.I. (2011). An analysis of CSB investigation reports concerning the hierarchy of controls, *Process Safety Progress*, 30(3), 261–265.

Bell, J., & Healey, N. (2006). *The Causes of Major Hazard Incidents and How to Improve Risk Control and Health and Safety Management: A Review of the Existing Literature*, Health and Safety Laboratory/Health and Safety Executive, UK. (HSL/2006/117).

Bourrier, M. (2005). The contribution of organizational design to safety, *European Management Journal*, 23(1), 98-104.

Busby, J.S. (1998). The neglect of feedback in engineering design organizations, *Design Studies*, 19(1), 103-117.

CCPS (1999). *Guidelines for Consequence Analysis of Chemical Releases*, Center for Chemical Process Safety, AIChE, New York.

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 Bhopal disaster. *Journal of Loss Prevention in the Process Industries*, 18(4–6), 205-208.

Crawley, F. & Tyler, B. (2003). *Hazard Identification Methods*, European Process Safety Centre (EPSC), Institution of Chemical Engineer (IChemE), Rugby.

Crowl, D. A. & Lauvar, J. F. (2011). *Chemical Process Safety – Fundamentals with Applications*, 3rd Ed, Pearson Education Inc, New Jersey.

Drogaris, G. (1993b). Learning from major accidents involving dangerous substances, *Safety Science*, 16, 89-113.

Drogaris, G. (1993a). *Major Accident Reporting System: Lessons Learned from Accidents Notified*. Amsterdam: Elsevier Science Publishers B. V. p. 16.

Duguid, I.M. (2001). Take this safety database to heart, *Chemical Engineering*, 108 (7), 80-84.

Deshotels, R.D. & Zimmerman, R. (1995). Cost-Effective Risk Assessment for Process Design, McGraw-Hill, New York.

FKD (2011). Failure Knowledge Database, <www.sozogaku.com/fkd/en/>, available online 26th June 2012.

Gunasekera, M.Y., & Alwis, A.A.P. (2008). Process industry accidents in Sri Lanka: Analysis and basic lessons learnt. *Process Safety and Environmental Protection*, 86(6), 421-426.

Gupta, J.P. & Edwards, D.W. (2002). Inherently safer design - present and future, *Process Safety and Environmental Protection*, 80(3), 115-125.

Hale, A., Kirwan, B. & Kjellen, U. (2007). Safe by design: where are we now? *Safety Science*. 45(1), 305-327.

Hasegawa K. (2004). Data-Base of Hazardous Materials Accidents in Japan and its applications - Hazardous Materials Safety Techniques Organization, *In 3rd NRIFD International Symposium on Safety in the Manufacture, Storage, Use, Transport, and Disposal of Hazardous Materials*, Tokyo, March 2004.

Hatakka, T.V. & Reniers, G.L.L. (2009). A case-based reasoning safety decision-support tool: Nextcase/safety, *Expert Systems with Applications*, 36(7), 10374-10380.

Hatamura, Y., Ilno, K., Tsuchlya, K., & Hamaguchi, T. (2003). Structure of failure knowledge database and case expression, *CIRP Annals - Manufacturing Technology*, 52(1), 97-100.

He, G., Zhang, L., Lu, Y. & Mol, A.P.J. (2011). Managing major chemical accidents in China: Towards effective risk information, *Journal of Hazardous Materials*, 187(1-3), 171-181.

Heikkilä, A.-M., Koiranen, T. & Hurme, M. (1998). Application of case-based reasoning to safety evaluation of process configuration. Rugby, IChemE Symposium Series No 144, pp 461-473.

Hendershot D. C. (2011). Inherently safer design: An overview of key elements, *Professional Safety*, The American Society of Safety Engineers', 1st February 2011, <www.*findarticles.com/p/articles/mi_hb5618/is_201102/ai_ n57036565 /?tag =content;col1>.*

Hollnagel, E., Woods, D. D. & Leveson, N. (Eds.) (2006) Resilience engineering: Concepts and precepts. Aldershot, UK: Ashgate.

Hou Y. & Zhang T. (2009). Evaluation of major polluting accidents in China—Results and perspectives, *Journal of Hazardous Materials*, 168(2-3), 670-673.

HSE (2003). *Out of Control – Why Control Systems Go Wrong and How to Prevent Failures*, HSE Books, 2nd Ed, Sudbury, UK.

Hurme, M. & Rahman, M., (2005). Implementing inherent safety throughout process lifecycle, *Journal of Loss Prevention in Process Industries*, 18, 238-244.

Jacobsson, A., Sales, J. & Mushtaq, F. (2010). Underlying causes and level of learning from accidents reported to the MARS database, *Journal of Loss Prevention in the Process Industries*, 23(1), 39-45.

Jørgensen, K. (2008). A systematic use of information from accidents as a basis of prevention activities, *Safety Science*, 46(2), 164-175.

Kidam, K., Hassim M.H. & Hurme, M. (2008a). Enhancement of inherent safety in chemical industry, *Chemical Engineering Transactions*, 13, 287-294.

Kidam, K, Hassim M.H. & Hurme, M. (2008b). Accident prevention: Practicing inherent safety, In 1*5th Regional Symposium on Chemical Engineering (RSCE)*, Kuala Lumpur, 2-3 December, Vol. 1, 789-792.

Kletz, T. A. (1991). *Plant Design for Safety: A User-Friendly Approach*. Hemisphere Publishing Corporation, New York.

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

Kletz, T. A. (1999). The origins and history of loss prevention, *Process Safety and Environmental Protection*, 77(3), 109-116.

Kletz, T. A. (2003). Inherently safer design—Its scope and future, *Process Safety and Environmental Protection*, 81(6), 401-405.

Kletz, T. A. (2004). Learning from experience, *Journal of Hazardous Materials*, 115(1–3), 1-8.

Kletz, T. A. (2009). Accident reports may not tell us everything we need to know, *Journal of Loss Prevention in the Process Industries*, 22(6), 753-756.

Kjellen, U. (2000). *Prevention of Accidents through Experience Feedback*, CRC Press, London.

Knegtering, B. & Pasman, H.J. (2009). Safety of the process industries in the 21st century: A changing need of process safety management for a changing industry, *Journal of Loss Prevention in the Process Industries* 22 (2), 162–168.

Lisbona, D., Johnson, M., Millner, A., McGillivray, A., Maddison, T., & Wardman, M. (2012). Analysis of a loss of containment incident dataset for major hazards intelligence using story-builder, *Journal of Loss Prevention in the Process Industries*, 25(2), 344-363.

Lindberg, A.-K. & Hansson, S.O. (2006). Evaluating the effectiveness of an investigation board for workplace accidents. *Policy and Practice in Health and Safety*, 4 (1), 63–79.

Lindberg, A.-K., Hansson, S.O. & Rollenhagen, C. (2010). Learning from accidents – What more do we need to know? *Safety Science*, 48(6), 714-721.

Mannan, M. S., Prem K. P. & Ng, D. (2010). Challenges and needs for process safety in the new millennium, In *Proceeding of 13th International symposium on loss prevention and safety promotion in the process industries*, Bruges, June 6-9, Volume 1, 5-13.

Mannan, M. S. (2005). *Lee's Loss Prevention in Process Industry*, 3rd Ed., Vol. 1, Elsevier-Butterworth Heinemann, Burlington, USA.

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, *Journal of Loss Prevention in the Process Industries*, 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, 2010.

OSHA (1993). *Process Safety Management of Highly Hazardous Chemicals*, Code of Federal Regulations, OSHA 29*,* 1910.119.

Pasman, H.J. (2010). Will a safe process be sufficient or do we have to do a bit more? In *Proceeding of 13th International symposium on loss prevention and safety promotion in the process industries*, Bruges, June 6-9, Volume 1, 17-21.

Paradies, M. (2011). Has process safety management missed the boat?, *Process Safety Progress,* 30(4), 310–314.

Prem, K.P., Ng, D. & Mannan, M.S. (2010). Harnessing database resources for understanding the profile of chemical process industry incidents, *Journal of Loss Prevention in the Process Industries*, 23(4), 549-560.

Qi, R., Prem, K.P., Ng, D., Rana, M.A., Yun, G. & Mannan, M.S. (2011). Challenges and needs for process safety in the new millennium, *Process Safety and Environmental Protection*, doi:10.1016/j.psep.2011.08.002.

Sales, J., Mushtaq, F., Christou, M.D. & Nomen, R. (2007). Study of major accidents involving chemical reactive substances: Analysis and lessons learned, *Process Safety and Environmental Protection*, 85(2), 117-124.

Schupp, B., Hale, A., Pasman, H.J., Lemkovitz, S. & Goossens, L. (2006). Design support for the systematic integration of risk reduction into early chemical process design, *Safety Science*, 44(1), 37-54.

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.

Tauseef, S.M., Abbasi, T. & Abbasi, S.A. (2011). Development of a new chemical process industry accident database to assist in past accident analysis, *Journal of Loss Prevention in the Process Industries,* 24(4), 426-431.

Taylor, J. R. (2007a). Understanding and combating design error in process plant design, *Safety Science*, 45(1), 75-105.

Taylor, J. R. (2007b). Statistics of design error in the process industries, *Safety Science*, 45(1), 61-73.

Taylor, J. R. (1975). *A Study of Abnormal Occurrence Reports*. Report RISØ-M-1837, Risø National Laboratory, Roskilde, Denmark.

Wincek, J.C. (2011). Two safety reviews before formal PHAs, *Process Safety Progress*, 30(3), 212–215.

The accident rate has not been decreasing in the chemical process industry although almost all the accidents (>95%) do have known causes and could have been prevented by using existing knowledge. This shows that the existing knowledge was not used effectively to prevent accidents. The aim of the thesis is to transform the accident report information into practical applications by analyzing it and creating an approach that can be used for supporting the design activities.

The thesis has presented new knowledge on the statistics of equipment based accident contributors, their background, the design errors involved and their timing and proposes a method for extended experience feedback to improve the dissemination of accident knowledge. The proposed method utilizes knowledge of earlier accident cases and a design lifecycle point of view. This makes it possible to start hazard identification in the early stages of plant design that lead to cost and safety benefits as a result of early process design changes.

Aalto-DD 168/2012

9 789526 049090

ISBN 978-952-60-4909-0
ISBN 978-952-60-4910-6 (pdf)
ISSN-L 1799-4934
ISSN 1799-4934
ISSN 1799-4942 (pdf)

Aalto University
School of Chemical Technology
Department of Biotechnology and Chemical Technology
www.aalto.fi