Jurnal Teknologi

Full Paper

# LESSONS LEARNED FROM PROCESS EQUIPMENT FAILURES IN THE CHEMICAL PROCESS INDUSTRY

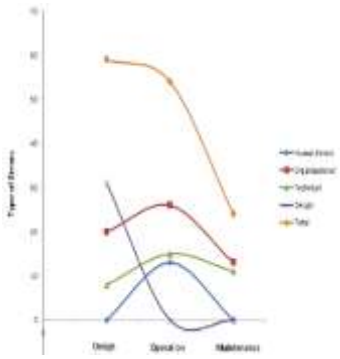
Nor Afina Eidura Hussin,[a] Kamarizan Kidam,[a,*] Siti Suhaili Shahlan,[a] Anwar Johari,[a] HaslendaHashim[b]

[a]Centre of Hydrogen Energy, Faculty of Chemical Engineering, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia
[b]Process System Engineering Centre (PROSPECT), Faculty of Chemical Engineering, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia

**Article history**
Received
*15 April 2014*
Received in revised form
*24 December 2014*
Accepted
*26 January 2015*

*Corresponding author
kamarizan@cheme.utm.my

## Graphical abstract



## Abstract

Process equipment failures play significant roles in most accidents that occur and recur in the chemical process industry (CPI). In this study, 50 equipment comprehensive accident investigation reports, extracted from the U.S. Chemical Safety and Hazard Investigation Board (CSB) and U.S. National Transportation Safety Board (NTSB) were analyzed to generate lessons learned. Based on the analysis, the synergy between major hazards i.e. fire, explosion, and toxic release has resulted in catastrophic accidents in the CPI. The emphasis on procedural equipment failure prevention does not provide sufficient hierarchy of controls in the CPI. Balance and integrated accident prevention is required to solve human unreliability that often leads to improper problem-solving, inappropriate actions, and ill-timed responses. To minimize losses, facilities and equipment should be designed and prepared for the worst-case scenario. Moreover, occurrence and recurrence of the accidents could be prevented using inclusive and updated communication systems through cooperation between various governmental agencies, industry players, and the public to disseminate lessons learned and promote safety in the industry.

*Keywords*: Accident prevention; equipment failure; hierarchy of controls; lessons learned

## Abstrak

Kegagalan peralatan pemprosesan adalah penyumbang utama kepada kemalangan yang berlaku di industri pemprosesan kimia. Kajian ini menganalisa 50 laporan penuh penyiasatan kemalangan daripada pusat data CSB dan NTSB. Berdasarkan analisa yang dibuat, kejadian kebakaran, letupan, dan pembebasan bahan kimia megakibatkan impak kemalangan peralatan yang sangat teruk. Pergantungan kepada kawalan kemalangan yang bersifat prosedur tidak mampu mengekang kejadian kemalangan ini. Sewajarnya, pihak industry mewujudkan kawalan kemalangan yang bersifat seimbang dan menyeluruh untuk mengelakkan kebergantungan kepada manusia yang terdedah kepada kesilapan dan ketidakcekapan. Kemudahan dan peralatan hendaklah direka untuk menghadapi situasi paling kritikal. Kemalangan ini juga boleh dielakkan dengan mempertingkatkan system komunikasi dan kerjasama dengan pelbagai pihak bagi menyebar maklumat berkaitan dan membudayakan keselamatan dalam industri.

*Kata kunci*: Pencegahan kemalangan; kegagalan peralatan; hierarki kawalan, pengajaran

## 1.0 INTRODUCTION

Nowadays, employing accident databases for accident analysis is becoming an active agenda. But, little effort has been made to harness the information in improving the safety systems and adopted risk mitigation measures to prevent future accidents in the chemical process industry (CPI) [1]. The application or utilization of the lessons learned is progressing slowly in the CPI [2]. The slow lessons learned utilization is a result from poor accident investigation, analysis and reporting [3].Knowledge from these data mining studies is poorly disseminated since majority of the research on the experience feedback system is related to accident investigation only, not on the dissemination of information [2-3]. A study by Jacobsson *et al*. reported that only one-third of the accident cases were considered as lessons learned on a broader basis. Most of the accident analyses provide very case specific information and are generally difficult to apply. Therefore, accident analyses that provide new findings on general knowledge and understanding on accident prevention are still greatly lacking, particularly on equipment failures [4].

Lack of focus is made on technical aspects of the equipment since the industry is aiming for cheaper procedural accident prevention [3]. As the complexity and technologies of the CPI advance, the tendency for equipment failures to occur is high. The high production and extreme operating conditions in chemical process plant tend to damage the equipment. This poor operation may lead to disasters. These accidents would not only damage the industry in terms of the financial losses but also in terms of major regulatory restrictions, societal losses and irreversible environmental damage.[1]The capital and operating costs required for equipment design modifications at the earlier stages are cheaper due to their less complex changes compared to the latter stages. Moreover, the reliability is also higher during the earlier stages [5]. Thus, this paper analyses recent accident data to identify the major hazards, root causes, and corrective actions for equipment failure incidents of the industry; and establishes lessons learned for better process equipment failure prevention.

## 2.0 HISTORY OF LOSS PREVENTION IN THE CPI

The history of accident prevention in the CPI shows that different approaches of risk reduction strategies have been implemented. Previously, accident prevention emphasizes either on design, technical, or procedural strategies. In the 1800s, a CPI plant with little instrumentation and means of protection only emphasized on procedural aspects for accident prevention. One of the procedural risk reduction examples is the one-legged stool strategy in nitroglycerin production. In this case, the operators had to sit on one-legged stools while watching over the production of highly exothermic nitroglycerin in large-stirred pots. If the heat was not removed by cooling and stirring, the reaction became uncontrollable and may lead to an explosive decomposition of the nitroglycerin. Hence, the operators had to watch the temperature closely. If they fell asleep, they fell off and injured themselves or at worst, could lead to fatality [6].

In 1960s, a great change in CPI occurred with process operating conditions (e.g. temperature, pressure etc.) became more severe; the energy stored in the process increased; problems in areas such as material construction and process control became more taxing; and the plants grew in size with a factor of about 10, and were often single stream. Relatively sophisticated instrumentation provision was developed to run a process under extreme conditions and close to the limits of safety thus causing high accident rates [7]. The focus of accident prevention shifted to technical and design-oriented [8].

Later, from 1980s onwards, the trend in accident prevention was mostly utilizing the outer layers of protection by adding add-on engineered either passive or active; and procedural control strategies. However, the risk reduction approaches were only effective to a certain extent. Nowadays, the focus of loss prevention is human and organizational-related which emphasis on the safety management system and safety culture to overcome fluctuating accident rate issues as shown by the study conducted by Amyotte *et al*. with 42% of the recommended corrective actions was procedural safety. In the study, 258 risk reduction strategies were identified. Inherently safer was the second highest (36%), followed by active-engineered and passive-engineered controls which represented 14% and 8% of the overall hierarchy of controls, respectively. The accident rates however remain persistently high [9].

## 3.0 RESEARCH APPROACH

In this study, 50 comprehensive accident investigation reports from 1998 to 2012 were extracted from U.S. Chemical Safety and Hazard Investigation Board (CSB) and U.S. National Transportation Safety Board (NTSB) database [10-11]. The baseline of the study was 2005. These accidents were related to equipment failures. Among the identified equipment were piping systems (32%), storage tanks (20%), process vessels (16%), separation equipment (10%), reactors (8%), and heat transfer equipment (8%). Others equipment such as conveyor and batch-off equipment only led to 6% of the reported accidents.

Piping systems include piping and piping components such as flanges, expansion joints, gaskets, bolts, etc. In this study, the types of vessels considered were process vessels and storage tanks. Process vessels are used for processing tasks in a plant. Meanwhile, storage tanks are used to contain raw materials, products, by-product, waste, etc. and commonly

located outside the process plant area. Reactors are a unique subset of vessels since they are specifically designed to contain chemical reactions. Heat transfer equipment are shell and tube exchanger, air cooled exchanger, and direct contact exchangers. Meanwhile, centrifuges, filters, dust collectors, cyclones and electrostatic precipitators are considered as separation equipment [5].

### 3.1 Major Hazards

The industry has been known with its highly hazardous environment compared to other industries. Many accidents happen in the CPI due to the existence of reactive/toxic chemicals and state-of-the-art technologies. The accidents commonly risk life and damage physical assets and its surrounding. Three major hazards in the CPI are fire, explosion and toxic release. Commonly, multiple major hazards occur resulting from an incident, leading to catastrophic disaster. In this study, consequence analysis was conducted to identify major hazards of equipment failure accidents and their severity in terms of fatality, injury, exposure, shelter-in-place and evacuation.

### 3.2 Accident Contributors

Root causes for the accidents were identified and classified as nature, human, organizational, technical, and design errors. Nature is an external factor in leading to accidents such as bad weather, earthquake, floods, lightning, tsunami, and landslides. Human errors are of four types; (1) errors due to slip or momentary lapse i.e. unintentional action, (2) errors due to poor training or instructions, (3) errors due to mismatch between the ability of the person and the requirement of the task, and (4) errors due to a deliberate not to follow instructions or accepted practice. Organizational errors are often related to management system. Design error is a part of technical errors.

However, due to its significant contribution in leading to accidents, a separate class for design errors was established. A design error is deemed to have occurred if the design or operating procedures are changed after an incident has occurred. Design errors are related to process condition, reactivity/incompatibility, unsuitable equipment/parts, and material of construction, sizing, utility set-up, protection, layout, automation /instrumentation, operating manual and fabrication/construction / installation [12].

Then, the origins of accident contributors were determined using root cause failures analysis by Antaki [13]. Root causes are originated from four major phases of a plant lifecycle; (a) risk reduction in materials, (b) risk reduction in design, (c) risk reduction in operation, and (d) risk reduction in maintenance. Risk is reduced in materials by selecting a good quality and compatible material. Risk reduction in design can be applied during process engineering and detailed engineering stages. To reduce risk in design, the basic control strategy should be established and all conditions such as start-up, normal operation and emergency shut-downs have to be considered. Risk reduction in operation comprises of safety and environmental management systems, controls of the safety management system, accident and investigation, and operating procedures. Meanwhile, risk reduction in maintenance deals with permits to work, maintenance programs, and modification controls. In these categories, human resources and management are required to eliminate human errors by giving education and training, and improving communications among the personnel in the CPI [14].

### 3.3 Accident Contributors

Finally, the recommended corrective actions were analyzed to identify the applied hierarchy of controls in the industry i.e. inherently safer, passive-engineered, active-engineered, or procedural. Ideally, accident preventive approach framework recommends inherently safer approach to deal with design errors and nature. For human and organizational causes, procedural approach is usually applied. Meanwhile, add-on engineering controls (i.e. passive and active-engineered) are recommended for technical-related accidents. Based on the findings, several lessons learned are established for better accident prevention for the industry.

## 4.0 RESULTS AND DISCUSSION

In this study, the analyses are divided into three major sub-sections; (1) consequence analysis, (2) root cause failures analysis, and (3) hierarchy of controls analysis. Root cause failure analysis was used to identify various types of accident contributors and determine their origins in process plant lifecycle.

### 4.1 Consequence Analysis

In the analysis, there were seven types of incidents resulted from 50 equipment failure-related accidents; fire (14%), explosion (22%), toxic release (26%), fire and explosion (32%), fire and toxic release (2%), explosion and toxic release (2%), and fire, explosion, and toxic release (2%). In total, 126 fatalities, 590 injuries, 260 exposures, four shelter-in-place, and 13 evacuations were reported. Fire and explosion incidents were the most common type of incidents in the study with 60 fatalities, 330 injuries, 18 exposures, two shelter-in-place, and four evacuations.

The second major hazards were toxic release incidents which resulted in seven fatalities, 22 injuries, 242 exposures, a shelter-in-place, and four evacuations. Explosion incidents were less than fire and explosion, and toxic release incident but the number of reported fatalities were higher (36 people) and with 161 injuries, and an evacuation. Explosion incidents were followed by fire incidents. In the fire incidents, 21 people were killed, 77 were injured, and two evacuations were resumed. Other incidents i.e. fire and toxic release;

explosion and toxic release; and fire, explosion, and toxic release were less significant. Only two fatalities, a shelter-in-place, and two evacuations were reported for these three types of incidents.

According to Table 1, piping system failures had initiated six fire, three explosion, and seven toxic release incidents. The number of reported fatalities, injuries, and exposures were 35, 150, and 71 people, respectively which were among the severe consequences compared to other failure accidents. The piping system failures also led to a shelter-in-place, and four evacuations.

Piping system failures outnumbered other equipment failures in resulting fire incidents and toxic release incidents. Only one case was reported for fire and toxic release (due to storage tank failure), explosion and toxic release (due to process vessel failure), and fire, explosion, and toxic release incident (due to storage tank failure). Shelter-in-place was commonly associated with piping systems, process vessels, and separation equipment failures.

Meanwhile, evacuation was reported in all equipment failures except others category. The highest evacuation was commenced during piping system failure accidents. The most catastrophic accident was related to separation equipment which occurred on March 23, 2005. The incident involved 16 fatalities, 180 injuries, and a shelter-in-place due to fire and explosion. The root cause of the incident was ineffective oversight of the company's safety culture and major accident prevention programs by the top management. This incident was one of six incidents which occurred due to a single root cause. The identified equipment failures were related to separation equipment (1), reactors (1), piping systems (2), process vessels (1), and heat transfer equipment (1). Most of the incidents were caused by a single organizational or design error as listed in Table 2.

## 4.2 Root Cause Analysis

Based on the root causes analysis, 137 accident contributors were identified with organizational errors as the major accident contributors (43%). Technical errors were identified as the second highest (25%) accident contributors, followed by design errors (23%), and human errors (9%). None of nature caused the accidents. Most of these accidents were contributed by multiple accident contributors. These multiple root causes accidents were classified as accidents with three or less accident contributors (64%) and accidents with more than three accident contributors (24%). Only 12% of the accidents were caused by one root cause. Among equipment failures that caused single accident contributor accidents were piping systems, reactors, process vessels, separation equipment, and heat transfer equipment (Figure 1 and Table 3).

The analysis showed that the average root causes per accident was 2.74. Separation equipment was the most accident-prone since only 2.4 root causes was required for an accident to occur. Although piping systems-related accidents were the highest but their root causes per accident was 2.75, same as for the heat transfer equipment. This indicates that piping systems and heat transfer equipment were less prompted to accident compared to separation equipment (2.4), process vessels (2.5), and reactors (2.5) which had been initiated by less number of root causes. Storage tanks (2.9) and other equipment (3.67) failure accidents occurred less than other accidents since the failures required more accident contributors to initiate (Table 1). Classification of types of root causes and their origins is summarized in Figure 2.

In the study, origins of accident contributors were grouped into three phases; design (i.e. materials and design), operation, and maintenance. At the design phase, most root causes are due to material selection, material quality, basic system design, and detailed integrity design. Instrumentation and controls, procedures and training, and emergency response-related root causes are commonly originated during the operation phase. Finally, during the maintenance phase, risk-bases inspection and fitness-for-service and management of change are considered as the main originated accident contributors.

All the design errors were originated at the design phase meanwhile all the human errors occurred during the operation stage. Other errors such as organizational errors and technical were originated at multiple phases of the plant cycle. Based on the origin cause analysis, critical criteria for accident prevention strategies are established as shown in Table 4. The results can be used to identify and diagnose equipment failure problems before progressing into unexpected downtime or catastrophic accidents as promptly finding the root causes not only save costly damage to the system, but also dramatically reduces operational costs.

### *4.2.1 Piping Systems*

In the research, piping systems caused the highest percentage of accidents. Special considerations for piping systems are blockage in the relief path; deflagration to detonation transition in pipe lines, loss of containment, and thermal stresses.[5] Among the identified piping system root causes were deficient integrity management procedures to detect defected pipe section, inadequate quality assurance and quality control, unreliable maintenance software program, and did not provide a back-up method to ensure timely change-out of piping components. Two piping systems accidents were initiated with only a single design error. This shows the significant of design errors in leading to accidents related to piping systems. Organizational and technical errors contributed to most of the piping systems accidents.

**Table 1** Consequence Analysis based on Equipment Failures

| Type of Equipment Failures | Frequency of Incidents | Root Causes per Incident | Type of Incident | | | | | | | Severity of Incident | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Fire | Explosion | Toxic Release | Fire & Explosion | Fire & Toxic Release | Explosion & Toxic Release | Fire, Explosion & Toxic Release | Fatality | Injury | Exposure | Shelter-in-place | Evacuation |
| Piping Systems | 16 | 2.75 | 6 | 3 | 7 | - | - | - | - | 35 | 150 | 71 | 1 | 4 |
| Storage Tanks | 10 | 2.90 | - | 2 | 2 | 4 | 1 | - | 1 | 17 | 13 | 0 | 0 | 2 |
| Process Vessels | 8 | 2.50 | - | 2 | 1 | 4 | - | 1 | - | 14 | 60 | 16 | 1 | 3 |
| Separation Equipment | 5 | 2.40 | - | 1 | 1 | 3 | - | - | - | 17 | 191 | 19 | 2 | 1 |
| Reactors | 4 | 2.50 | - | 1 | 1 | 2 | - | - | - | 9 | 49 | 154 | 0 | 1 |
| Heat Transfer Equipment | 4 | 2.75 | 1 | 1 | 1 | 1 | - | - | - | 9 | 52 | 0 | 0 | 2 |
| Others | 3 | 3.67 | - | 1 | - | 2 | - | - | - | 25 | 75 | 0 | 0 | 0 |
| **Total** | **50** | **2.74** | **7** | **11** | **13** | **16** | **1** | **1** | **1** | **126** | **590** | **260** | **4** | **13** |

**Table 2** Details on Single Root Cause Equipment Failures

| Single Root Cause Accidents | | | |
|---|---|---|---|
| **Type of Failures** | **Type of Incidents** | **Severity of Incidents** | **Type of Errors** |
| Separation Equipment | Fire and Explosion | 16 fatalities, 180 injuries, shelter-in-place | Organizational |
| Reactors | Explosion | 4 fatalities, 32 injuries | Design |
| Piping Systems | Explosion | 4 fatalities, 11 injuries | Design |
| Piping Systems | Fire | 2 fatalities, 7 injuries | Design |
| Process Vessels | Toxic Release | 16 exposures, evacuation | Design |
| Heat Transfer Equipment | Toxic Release | 7 injuries | Organizational |

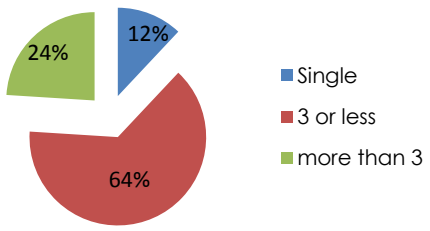



**Figure 1** Type of Root Causes

**Table 3** Single Root Cause Accidents

| Type of Equipment Failures | Type of Errors | Origin of Errors |
|---|---|---|
| Reactors | Design | Design |
| Separation Equipment | Organizational | Operation |
| Process Vessels | Design | Design |
| Heat Transfer Equipment | Organizational | Operation |
| Piping Systems | Design | Design |
| Piping Systems | Design | Design |

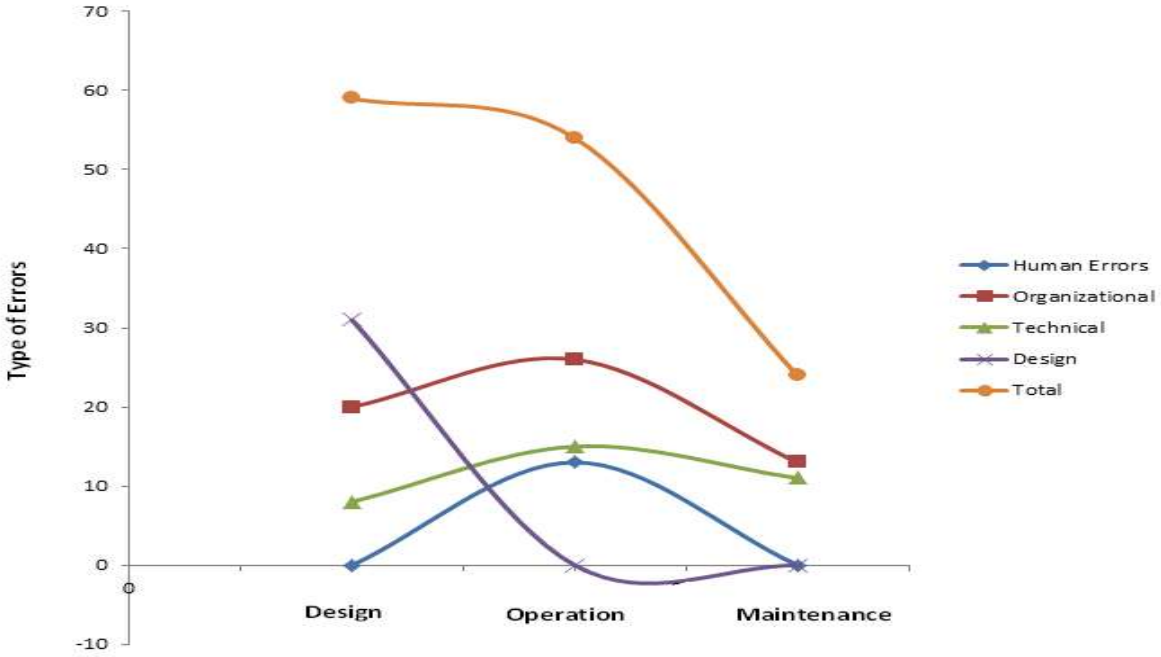



**Figure 2** Origins of Accident Contributors

**Table 4** Distributions of Critical Criteria for Accident Prevention

| CRITICAL CRITERIA FOR ACCIDENT PREVENTION | | | | | |
|---|---|---|---|---|---|
| **Design (43%)** | | **Operation (39%)** | | **Maintenance (18%)** | |
| Hazard analysis | 36 % | Safety culture and accident prevention programs | 35 % | Mechanical integrity | 29 % |
| Design specifications | 21 % | Unsafe practices | 17 % | Maintenance procedures | 29 % |
| Safeguards risk controls | 22 % | Training and experience | 15 % | Management of change | 25 % |
| Inherently safer | 12 % | Public awareness | 13 % | Inspection and auditing programs | 13 % |
| Safe operating limits | 3% | Operating procedures | 11 % | Housekeeping practices | 4% |
| | | Emergency preparedness | 9% | | |

### *4.2.2 Process Vessels and Storage Tanks*

Vessels can be classified into in-process vessels (surge drums, accumulators, separators, etc.) and storage tanks. Common failures involving vessels are regarding ignition of flammable atmosphere; chemical reaction increases pressure; pressure generated by rollover; tank failure under vacuum; and tank failure from heave [5].Storage tanks accidents were higher than process vessels accidents. Storage tanks accidents were caused mainly by organizational errors, followed by design and human errors. Inadequate mechanical integrity management system to prevent and address safety and environmental hazards; and inadequate engineering management and management of change were among the identified organizational errors resulting in storage tank failures. Other storage tank failure factors were inadequate training and practices in determining and handling abnormal cylinders, and employees were unaware of the potential flammability hazard, and inadequate safety measures in place to identify and analyze serious fire hazards that could affect the tanks. Process vessels

failures were also caused by organizational errors related to ineffective process and engineering requirement programs, inadequate hazard analysis systems, and inadequate operating procedures or training programs. A single root cause accidents occurred involving a process vessel which were caused by a design error leading to toxic release. However, no fatalities and injuries were reported.

#### 4.2.3 Reactors

Reactors are a unique subset of vessels since they are specifically designed to contain chemical reactions. However, many of the generic failure modes of vessels such as corrosion-related failures or auto polymerization may also apply to reactors. Reactors can be grouped into three main types: batch, semi-batch, and continuous. To avoid accidents, special emphases of reactor design are on overpressure due to loss of agitation, addition of incorrect reactant, inactive/semi-active or wrong catalyst addition, and monomer emulsion feed breaking during feed [5]. The analysis found out that organizational errors significantly contributed to reactor failures which then led to accidents e.g. top management did not have provide effective oversight of the company's safety culture and major accident prevention programs, and did not have adequate emergency response plan. Other than these management-related errors, design errors also constituted to reactor failure due to ignorance to perform a comprehensive process design and hazard review of the laboratory scale-up to full production before attempting the first chemical production batch. In this study, a single design error had contributed to an occurrence of reactor accident that led to an explosion. The explosion killed four people and injured 32 others.

#### 4.2.4 Separation Equipment

Based on histories, separation equipment is known to lead to explosions such as batch centrifuge explosion, filter explosion, and dust collector explosion. The main issue for this equipment is dust deflagration due to electrostatic spark discharge [5]. Based on the root cause analysis, most separation equipment failures were caused by organizational errors. Others were initiated by technical and design errors. Among the identified organizational errors were due to no formal, documented program to investigate and implement corrective action for incidents, no procedures for identifying and planning of non-routine job situations, no adequate system to identify and evaluate the hazards created by changes to the facility processes and equipment, and insufficient layers of protection to prevent a catastrophic release. A single organizational error originated during the operation phase had caused a separation equipment accident that led to fire and explosion. The incident killed 16 people and injured 180 others.

#### 4.2.5 Heat Transfer Equipment

Past incidents involving heat transfer equipment are ethylene oxide re-distillation column explosion (i.e. Seadrift, Texas chemical facility in 1991), brittle fracture of a heat exchanger, and cold box explosion. Among heat transfer equipment are shell and tube exchanger, air cooled exchanger, direct contact exchanger, and other types including helical, spiral, plate and frame, and carbon block exchangers. Common accident contributors for heat transfer equipment are leak/rupture of the heat transfer surface, fouling or accumulation of non-condensable gases, and external fire [5] In the analysis, the most common root causes of accidents involving heat transfer equipment were organizational-based e.g. inefficient cleaning procedures, incomplete incident investigation program, inadequate management systems for supervision, planning, and execution of maintenance work, and lack of system for monitoring and controlling hazards. A toxic release incident had occurred due to a single organizational accident contributor.

### 4.3 Hierarchy of Controls Analysis

In managing risk, the most reliable layers of protection (LOP) is the inner most layer which is the inherently safer, followed by passive-engineered, active-engineered, and procedural strategies, respectively. The priority in risk management strategy is inherently safer > passive > active > procedural. By changing the design an operation at the earlier stages, the capital and operating costs required are much cheaper than the latter stages. Only, procedural control strategies require low relative costs compared to other stages but the reliability of the strategies is the lowest and the modification is difficult to mark since the complexity increases throughout the process lifecycle [5].The corrective action section of the accident reports was analyzed to determine the applied risk reduction strategies of the CPI. The analysis has showed that the industry normally takes several corrective actions for multiple causation accidents. However, procedural strategies were mostly recommended as the corrective actions. In this study, 590 corrective actions had been suggested by the boards. Out of these 590 corrective actions, 91% were procedural-based. From all the recommended corrective actions, active-engineered was 3%, and followed by inherently safer (3%). Passive-engineered strategies were the least options used with only 3% of the total recommended corrective actions. Further details on the recommended hierarchy of controls are summarized in Table 5.

#### 4.3.1 Inherently Safer

Process hazards and their risks can be managed effectively through layer of protection. The hierarchy controls analysis by the research has showed that procedural strategies were most preferred by the industry. The layer is less reliable than inherent safety, passive-engineered, and active-engineered controls.[5]

Inherently safer is the premier strategy for hazard avoidance and control at its source through design changes. Based on the analysis, 3% of the corrective actions were inherently safer strategies. Inherently safer approach uses material and process conditions that are less hazardous to eliminate and mitigate hazard. Four types of inherently safer used were minimization (44%), moderation (28%), simplification (17%), and substitution (11%). Minimization was used to limit energy generation capabilities by using smaller amount of hazardous substances. Among others recommended inherently safer strategies were replacing a hazardous substance with a less hazardous one such as the use of air or pigging with air instead of natural gas blow for cleaning fuel gas piping (substitution) and sodium hypochlorite as a biocide in cooling water treatment instead of chlorine (substitution); and the use of appropriate materials for wastewater treatment (moderation), and revision of operating conditions to reduce risk of over-chlorination (moderation) for safer process condition.

### 4.3.2 Add-on Engineering Controls

Add-on layers are mainly installed as passive and active engineered safety protection systems. Passive strategy employs systems that remain static and do not perform any fundamental operations. This passive-engineered risk control further reduces the likelihood and consequences of accident by using passive safety protection such as dikes, containment and fire wall. The passive-engineered modifications are mostly related to layout, mechanical/physical aspects, design specification changes,

**Table 5** Classifications for the Recommended Hierarchy of Controls

| HIERARCHY OF CONTROLS (%) | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Inherently Safer (3%)** | | **Passive-Engineered (3%)** | | **Active-Engineered (3%)** | | **Procedural (91%)** | |
| Minimization | 44 | Protective system | 60 | Instrumentation | 55 | Communication | 23 |
| Moderation | 28 | Design changes | 13 | Mitigation system | 30 | Safety regulations and guidance | 15 |
| Simplification | 17 | Layout | 7 | Protective system | 15 | Training and education | 13 |
| Substitution | 11 | Sizing | 7 | | | Inspection | 11 |
| | | Equipment modification | 7 | | | Management system | 10 |
| | | Additional equipment | 7 | | | Emergency preparedness | 5 |
| | | | | | | Work mechanism | 5 |
| | | | | | | Documentation | 3 |
| | | | | | | Enforcement and implementation | 3 |
| | | | | | | Cooperation | 2 |
| | | | | | | Expertise and consultation | 2 |
| | | | | | | Management of change | 2 |
| | | | | | | Maintenance | 2 |
| | | | | | | Monitoring and supervision | 1 |
| | | | | | | Research | 1 |
| | | | | | | Contractor safety performance | 1 |
| | | | | | | Cleaning and housekeeping | 1 |

additional equipment, equipment modification, and friendlier design. Active add-on engineered strategies use active systems that depend on timely hazard detection and initiation (i.e. utilizes safety devices that respond to process changes) to further reduces the accidents using relief valves, controllers, detectors and alarms. For controlling risk, active-engineered control requires additional devices to sense and indicates process variables, valves, etc. either by adding or removing the instrumentation and automation of the equipment [12].

In the study, 3% passive-engineered controls were used and 3% were active-engineered controls. For passive-engineered, protective system (60%), design changes (13%), layout (7%), sizing (7%), equipment modification (7%), and additional equipment (7%) were recommended. Passive-engineered controls further reduced hazard and risk by using firewalls and blast-resistant construction; adding protective fireproofing for fire rack support steel near process unit containing highly pressurized flammables; and ensuring that penetrations of partitions, floors, walls, and ceiling were sealed dust-tight. Meanwhile, instrumentations were mostly used as active-engineered controls (i.e. 55%). Other active-engineered controls were mitigation system (30%), and enhanced protective system (15%). Active-engineered controls established adequate layers of

protection system by using additional interlock and shutdown, air monitoring devices, automated audible alarms, level indicators, automatic controls, post-ignition deflagration detection, and damage control devices.

#### *4.3.3 Procedural*

Procedural or human and organizational-oriented risk control usually focuses on safe operation including training, supervision, procedure, work instructions, inspection and maintenance. This operator and maintenance procedures should be the last resort, especially for control and mitigation where the chance of errors or failure is high [12]. In the study, procedural safety systems were commonly related to administrative controls that include standard operating procedures, safety rules and procedures, operator training, management systems, and emergency response procedures. The procedural strategies were 91% of all the corrective actions suggested. Communication was the highest strategies recommended by the boards (22.9%), followed by development or amendment of safety regulations and guidance (15.3%). Training and education (12.7%), inspection (11.5%), and management system (10.1%) were also parts of these implemented corrective actions. Other less prioritized procedural strategies were emergency preparedness (5.4%), work mechanism (4.8%), documentation (3.2%), enforcement/implementation (2.6%), cooperation (2.4%), expertise and consultation (2%), management of change (1.9%), maintenance (1.5%), monitoring/supervision (1.1%), research (1.1.%), contractor safety performance (0.9%), and cleaning and housekeeping (0.6%). In the study, communication issues were commonly addressed to ensure timely transmission of critical safety information to responding personnel. Therefore, safety alerts and health bulletin were published to warn owners and operators on potential hazards and risks of the industry. The safety alerts advised them on their responsibilities for accident prevention such as recommending the use of inherently safer design features, describing sufficient security measures, and recommending the use of hazards signs to identify the fire and explosion hazards.

## 5.0 LESSONS LEARNED

From the analyses, the contribution of process equipment failures in leading to accidents of the CPI is significant. Many lessons learned can be established based on the analyses of major hazards, root causes, and the recommended corrective actions. Among the lessons learned are:

### 5.1 Worst-case Scenario Design

Equipment process failures result in major hazards and their severity is beyond limitations. It is infrequently reported that only a type of incident happened per equipment failure i.e. only fire or explosion or toxic release incident occurs. In most accident cases, fire, explosion, and/or toxic release incidents occur simultaneously. The synergy between major hazards results in catastrophic accidents with severe consequences in numbers of fatalities, injuries, exposures, shelter-in-place, and evacuations. To minimize the losses, plant and equipment should be designed and prepared for the worst-case scenario, not just adapting to any 'applicable' standards or guidance.

### 5.2 Hierarchy of Controls Implementation

In the study, the required Management Preventive Actions (MPA) was 52.6% whereby human errors and organizational errors constituted 9.5% and 43.1%, respectively. Based on technical and design errors identified, 47.5% of the root causes required Engineering Preventive Actions (EPA). Although the amounts of both preventive actions were almost balanced, the Boards only recommended 9% of the corrective actions in terms of technical and design aspect. Most often procedural strategies were applied. These results show the need for more balanced accident prevention strategies for the CPI. The industry should shift its accident prevention approach towards technical and design, not just emphasizing on procedural aspects. Integrated accident prevention should be the focus of the industry nowadays to eliminate hazards and reduce risks. In general, the emphasis on procedural accident prevention strategies does not provide adequate hazard elimination and risk reduction. The human reliability is not high enough and often leads to improper problem-solving, inappropriate actions, and ill-timed responses. Thus, the CSB and NTSB suggested various procedural corrective actions with the involvement of governmental agencies, industry players, research institutes, and other non-governmental agencies. Thus, the industry should reconsider the implementation of the inner most layers of hierarchy of controls to prevent accidents thus resulting in safety and cost benefits of the CPI. The importance of implementing a comprehensive hierarchy of controls includes,

- To comprehensively control all potential ignition sources and continuously monitor hazards at appropriate locations and elevations;
- To train and certify emergency response personnel;
- To publish the technical guidance addressing the safe operating procedures;

- To avoid occurrence and recurrence of accidents by analyzing the key findings, cause, recommendations of the reports to shareholders, membership, and workforce; and
- To establish a timely notification community procedures in the event of chemical release that save life and public properties.

### 5.3 Communication and Cooperation

Communication is the major factors to prevent occurrence and recurrence of accidents. Any miscommunications among responsible agencies and the industry players should be avoided especially during emergency response procedures. Moreover, good community notification systems for any emergencies would also save near-by public life and properties. Accident knowledge generated from accident investigations should be communicated thoroughly for better accident prevention of the industry. Additionally, the establishment of safety regulations and guidance are also important in preventing accidents. Several governmental agencies such as the Occupational Safety and Health Administration (OSHA), the Environmental Protection Agency (EPA), National Fire Protection Association (NFPA), and other regulatory bodies are responsible for developing, revising, and regulating safety regulations of the CPI. At the industry level, top management and middle management are in-charged for establishing and enforcing these safety regulations and guidance. Cooperation between the agencies, industry players, and the workforce are needed to ensure comprehensive regulations and standards are adapted in the CPI.

## 6.0 CONCLUSION

As a conclusion, most accidents due to equipment failures could be prevented by incorporating worst-case scenario design, balanced and integrated hierarchy of controls, and comprehensive communication systems in the industry. Cooperation between various agencies, industry players, and the public is required to disseminate lessons learned and promote safety in the CPI.

## Acknowledgement

Special thanks to Zamalah Scholarship of Universiti Teknologi Malaysia and RU grant Q.J130000.2544.08H04 for supporting the research work .

## References

(1) Prem, K. P., Ng D., and Mannan, M.S. 2010. Harnessing database resources for understanding the profile of chemical process safety incidents.*J Loss Prevent Process Ind*. 23(4): 549-560.
(2) Lindberg,A. K., Hansson, S. O., and Rollenhagen, C. 2010. Learning from accidents – What more do we need to know? *J Saf Sci.* 48(6): 714-721.
(3) Kletz, T. A. 2009. Accident reports may not tell us everything we need to know. *J Loss Prevent Process Ind*. 22(2): 162-168.
(4) Jacobsson, A., Sales, J., and Mushtaq, F. 2010. Underlying causes and level of learning from accident reported to the MARS database. *J Loss Prevent Process Ind*. 23(1): 39-45.
(5) CCPS. 1998. *Guidelines For Design Solutions For Process Equipment Failures*. Center for Chemical Process Safety, AIChE.
(6) Kletz, T.A., and Amyotte, P. 2010. *Process Plant – A Handbook For Inherent Safer Design.* CRC Press.
(7) Lees, F.P. 1996. *Loss Prevention In The Process Industries.* Butterworth Heinemann.
(8) Kidam, K., and Hurme, M. 2012. Origin of equipment design and operation errors. *J Loss Prevent Process Ind*. 25: 937-949.
(9) Amyotte, P. R., MacDonald, D. K., and Khan, F.I. 2011. An analysis of CSB investigation reports concerning the hierarchy of controls. *J Process Saf Progress.* 30(3):261–265.
(10) CSB. 2013. *Chemical Safety and Hazard Investigation Board.* Retrieved from www.csb.gov/investigations/completed-investigations
(11) NTSB. 2013. *National Transportation Safety Board*. Retrieved from www.ntsb.gov/investigations/reports.
(12) Kidam, K. 2012. *Process Safety Enhancement In Chemical Plant Design By Exploiting Accident Knowledge.* PhD thesis. Aalto University School of Chemical Technology.
(13) Antaki, G. 2005. *Fitness-For-Service And Integrity Of Piping, Vessels And Tanks*. McGraw-Hill Companies, Inc.
(14) Santamaria Ramiro, J.M., and Brana Aisa, P.A. 1998. *Risk Analysis And Reduction In Chemical Process Industry*. Blackei Academic & Profession, Thomson Science