Peter Okoh

Maintenance Strategies for Major Accident Prevention

Thesis for the degree of Philosophiae Doctor

Trondheim, October 2015

Norwegian University of Science and Technology
Faculty of Engineering Science and Technology
Department of Production and Quality Engineering

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of Science and Technology

Thesis for the degree of Philosophiae Doctor

Faculty of Engineering Science and Technology
Department of Production and Quality Engineering

ISBN 978-82-471-4196-0 (printed ver.)
ISBN 978-82-471-4197-7 (electronic ver.)
ISSN 1503-8181

Doctoral theses at NTNU, 2015:272

Printed by NTNU Grafisk senter

Preface

This thesis is being submitted in partial fulfillment of the requirements for award of the degree of Doctor of Philosophy at the Faculty of Engineering Science and Technology, the Norwegian University of Science and Technology (NTNU).

In a PhD study, one may experience possession by passion, dread of deadlines, weariness from workload, blur from burnout, vivacity of verbal presentations, articulation of arguments, feeling frail in failure, notching of novelty and sounding strong in success - a mix of the good, the bad and the ugly.

Bang! Hitting a blind alley tends to get one discouraged and if consistent tends to lead to frustration. I struggled several times, listened to music to relieve my depression. I listened to Jimmy Cliff's "Struggling man," and "You can get it if you really want." It was scary seeing some colleagues drop by the wayside. I ran to a veteran professor and asked him the reason. We agreed that the fault could be the student's, the supervisor's, the institution's or a combination of these. Then he advised that I must not relax, but continually work hard to get at least three published journal papers. So, I worked each day as though I was going to graduate the following day. It was not an easy road.

Will Durant said that it was all very funny, quoting Arthur Schopenhauer thus: " the life of every individual, if we survey it as a whole...and only lay stress on its most significant features, is really always a tragedy; but gone through in detail it has the character of a comedy." Research is a humbling experience. I betrayed my emotion once, seeing a hard-earned result crumble like a crust of snow being trodden. Scrap the crap! That sucks! But my will kept hope alive and I had faith. Dreaming a PhD without revisions or rejections of costly purchases of sweat is like imagining an omelett without breaking shells.

I wish everyone who reads this thesis a happy reading and the benefit of knowing more.

Trondheim, Norway
October 09, 2015

Peter Okoh

Acknowledgements

To my supervisor, Professor Stein Haugen, I am deeply indebted, for all the time and painstaking efforts he spent to bring me this far. Maybe, I am the PhD student, who "bothered" him the most, with my barrage of meeting requests, which he had always coped with gracefully. I was always eager to learn from him and he encouraged and advised me. He gave room for presentation of my arguments which he viewed with an open mind. I believe that I was most fortunate to have him as a supervisor.

To my co-supervisor, Associate Professor Per Schjølberg, I am profoundly grateful, for his co-operation. Although, he could be busy with administrative work, he exposed me to different aspects of maintenance management.

To my former supervisor, Professor Mary Ann Lundteigen, I extend my heartfelt appreciation, for the initial push she gave me to the "front line." She scheduled frequent meetings, which helped to hasten my development, and she was also a good counselor.

To Professor Marvin Rausand, I pay glowing tributes, for all I have learnt from him. He is one of the pioneers of my development in Norway and encouraged me a lot. I used to turn to him like a father whenever I fell into "trouble." He reminds me of Democritus, the laughing philosopher, for his sense of humor which served as a relief valve to burnout.

To Professor Jørn Vatn, I express my sincere appreciation, for all he has taught me over time which has contributed to my development. Even though my experience with him had been more of a struggle, it was necessary for the best end.

To colleagues and friends, I give my kind regards: Erik Faarlund, Abraham, Alvaro, Emrah, Geir-ove, Harald, HyungJu, Pavan, Tara, Sverre, Tørstein, Vegard, Xue, Yiliu etc for their warm relationship, and Eli, Rune, Kjerstin, Kari, Trond, Tonje and Øyvind who facilitated miscellaneous operations.

To my beloved wife and best friend, Amabini, and my children, Raymond and Rayna, I say "thanks" a million times, for all they sacrificed in relation to the PhD study.

Summary

Summary

The overall objective of this PhD thesis has been *to develop new strategies for the prevention of maintenance-related major accidents in the process industries*. By virtue of the new knowledge developed in this PhD project, the decision-makers are expected to gain a better insight into the pros and cons of maintenance, how maintenance influences major accidents, the maintenance-related major accident trend, the degree and distribution of the causes of maintenance-related major accidents as well as strategies for the prevention of such accidents.

This PhD thesis has been a mix of qualitative and quantitative analysis and synthesis of concepts and theories in relation to major accident causation (e.g. organizational accident perspectives and previous accidents investigation/analysis reports) and preventive initiatives in relation to maintenance-related organizational robustness and resilience as well as maintenance optimization (aimed at minimizing the major accident risk).

This PhD thesis investigates all the aforementioned aspects of maintenance-related major accidents in the hydrocarbon and chemical process industries, and significant results have been achieved as regards a better understanding of the characteristics of maintenance-related major accidents and the most reasonable preventive efforts. The main contributions of this PhD project to the body of knowledge are documented in the form of six articles, five published and one under review in international peer-review publication channels.

Maintenance-related major accidents, like other major accidents, can be caused by technical, human and organizational factors. However, some individuals and organizations may tend to consider the technical and human factors only, while neglecting the organizational. Since accidents are not only products of technical/human failures, it is important to consider all the possible types of influences in order to develop a comprehensive prevention strategy. In this PhD

thesis, a better insight is given into how maintenance influences major accidents with respect to the aforementioned types of influences.

Maintenance-related major accidents may be classified based on existing schemes encompassing maintenance work/management process, threats and error management (TEM) framework and MTO (Man, Technology and Organization), but these fail to explicitly address the accident process itself. In this PhD thesis, how maintenance influences the major accident risk has been analyzed and investigated. The work and accident processes combined into a new scheme called Work and Accident Process (WAP) scheme is being proposed for maintenance-related major accidents classification. This scheme has been tested with maintenance-related major accidents cases from the U.S. Chemical Safety Board (CSB) and the validity has been demonstrated. The PhD thesis also presents a classification approach based on both the accident process and the maintenance management process.

Statistics on maintenance-related major accidents are important for decision-making, most especially, in relation to the prioritization of preventive efforts. However, most of the statistics identified on maintenance-related accidents are about 25 years old. The validity of such statistics is constrained by the uncertainty associated with the assumption that future failure will continue at the same rate as immediate previous experience. Besides, some of the statistics were a mixture of major accidents, occupational accidents and serious incidents and this also adds to uncertainties in relation to maintenance-related major accidents. This PhD thesis provides a current update on the trend of maintenance-related major accidents in the 21st century and the degree and distribution of the causes. The thesis also proposes WAP-FMEA (Work and Accident Process Failure Modes and Effects Analysis), i.e. a FMEA which integrates the maintenance work process with the accident process for the purpose of prevention of maintenance related major accidents. As regards the applicability of the statistical findings, the frequencies can be used to determine probabilities which in turn will be useful in maintenance-related, major-accident risk modeling and in the probability column of the suggested WAP-FMEA.

The purpose of maintenance should not be limited to the traditional idea of retaining systems in or restoring them to a functioning state. Maintenance can also contribute to improved system knowledge and interdisciplinary coordination that may benefit the entire organization. The organizational value-adding potential of maintenance has never been investigated. Maintenance can be investigated as a contributor to robustness and resilience of organizations such that the ability to prevent or limit unexpected events is improved. Hence, maintenance-related major accidents (i.e. maintenance-related organizational accidents) can also be viewed from the six perspectives of organizational accidents, i.e. Energy-Barrier model, Normal Accident Theory (NAT), High Reliability Organizations (HRO), the Man-made Disaster (MMD) theory, Conflicting Objectives, Adaptation and Drift (COAD) theory and Resilience Engineering. These perspec-

tives have been studied by several people, but have not been investigated thoroughly by any in relation to maintenance. This PhD thesis systematically investigates the relationship between maintenance and the six perspectives of organizational accidents. This encompasses the significance of the perspectives to maintenance. Finally, recommendations on how to improve the robustness and resilience properties of maintenance within the process industries evolve from the aforementioned investigation. This is an added knowledge for a better insight into the link between maintenance and major accidents.

Increasing or decreasing frequency of maintenance increases the major accident risk when they are off the optimal level. Too much maintenance visits increase the exposure of personnel to risk, the probability of introducing new hazard and failures and the wear-out potential of safety barriers, whereas too little maintenance visits provide an opportunity for failure mechanisms to degrade the major accident barriers. Hence, there is the need to optimize maintenance. However, none of the existing optimization methods has accounted for the exposure of personnel to the major accident risk. This PhD thesis improves maintenance optimization in terms of risk such that the exposure of humans to risk is being adequately accounted for.

Structure of thesis

Structure of the thesis

This PhD thesis has two main parts:

- Part I Main report: This part first presents the background, the challenges and research questions, as well as the objectives and the scope of this PhD thesis, and then proceeds to a discussion of the research methodology and approach. Finally the main results are summarized and the possible areas for future research are indicated.
- Part II Articles: This part includes six articles published or prepared during the PhD project. These articles consist of the main work and achievements during the PhD.

Articles

	Reference
Article 1: Okoh, Peter and Haugen, Stein. The influence of maintenance on some selected major accidents. *Chemical Engineering Transactions*, Volume 31, Pages 493-498, DOI: 10.3303/CET1331083, 2013	[69]
Article 2: Okoh, Peter and Haugen, Stein. Maintenance-related major accidents: Classification of causes and case study. *Journal of Loss Prevention in the Process Industries*, Volume 26, p. 1060-1070, 2013	[68]
Article 3: Okoh, Peter and Haugen, Stein. A study of maintenance-related major accident cases in the 21st century. *Process Safety and Environmental Protection*, Volume 92, p. 346-356, 2014	[70]
Article 4: Okoh, Peter and Haugen, Stein. Maintenance optimization for major accident risk reduction. *Submitted to Journal of Loss Prevention in The Process Industries*	[71]
Article 5: Okoh, Peter and Haugen, Stein. The effect of maintenance seen from different perspectives on major accident risk. *IEEE International Conference on Industrial Engineering and Engineering Management*, Hong kong, 2012	[67]
Article 6: Okoh, Peter and Haugen, Stein. Improving the robustness and resilience properties of maintenance. *Process Safety and Environmental Protection*, Volume 94, Pages 212-226, DOI: 10.1016/j.psep.2014.06.014, 2015	[72]

Declaration of authorship

The first author and Haugen were involved in the conceptual and planning phases of the article projects. The first author gathered data, analyzed the data and wrote the paper, while considering critical comments from Haugen.

Contents

Preface i

Acknowledgements iii

Summary v

Structure of thesis ix

Part I Main report

1 Introduction 3
1.1 Background 3

2 State-of-knowledge of concepts and gaps 7
2.1 Chapter introduction 7
2.2 The major accident concept in the process industries 8
2.3 The maintenance concept 9
2.4 Classification of maintenance-related major accidents 11
2.5 Organizational factors in major accidents 12
2.5.1 Final remarks 20
2.6 The concept of robustness 21
2.7 Pros and cons of changing maintenance intervals 21
2.8 Maintenance optimization 22

3 Research questions and objectives 25
3.1 Research questions 25
3.1.1 How does maintenance influence major accident risk? . . 25
3.1.2 To what extent has maintenance been a cause of major accidents? 26
3.1.3 How should maintenance be optimized in relation to the major accident risk? 26

3.1.4 How can maintenance contribute to the robustness and resilience of organizations? 27
3.2 Research objectives 27
3.3 Scope 28

4 Research methodology and approach 29
4.1 Overview of research 29
4.2 Overview of scientific method 32
4.3 The research content of this PhD project 33
4.3.1 Application of the scientific methodology to this PhD project 33
4.3.2 The bigger picture of the entire PhD research process . . . 37
4.3.3 The detailed picture of the entire PhD research process . 38

5 Main results 41
5.1 Main results 41
5.1.1 "How does maintenance influence major accident risk?" (question 1) - "The realization of a well-structured framework and expanded/modified knowledge about the causal relationship between maintenance and major accident." (objective 1) 41
5.1.2 "To what extent has maintenance been a cause of major accidents?" (question 2) - "Enhanced demonstration of the applicability of the knowledge derived from the causal relationship between maintenance and major accidents" (objective 2) 47
5.1.3 "How should maintenance be optimized in relation to the major accident risk?" (question 3) - "The proposal of novel risk reduction strategies for maintenance-related major accidents" (objective 3) 53
5.1.4 "How can maintenance contribute to the robustness and resilience of organizations?" (question 4) - "The proposal of novel risk reduction strategies for maintenance-related major accidents" (objective 3) 58

6 Discussion and conclusion 65
6.1 Criticisms 65
6.2 Generic tools for measuring quality of research 66
6.3 Quality assurance of this PhD project 67
6.4 Conclusion 68
6.5 Expected benefits of this PhD project to the industry 69
6.6 Future research 70

7 Acronyms and abbreviations 73

References 75

Part II Articles

Article 1 on learning from accidents 87

Article 2 on maintenance-related causes of major accidents 95

Article 3 on maintenance-related major accident statistics 109

Article 4 on risk-based maintenance optimization 123

Article 5 on the relationship between maintenance and various major accident perspectives 139

Article 6 on organizational robustness and resilience 147

Part I
Main report

Chapter 1
Introduction

1.1 Background

Major accidents may be defined as adverse events such as major leaks/releases, major explosion, major fire or major structural failure/loss of stability, leading to serious danger/damage, to human life, the environment or material assets [10, 18, 52, 81, 104].

Most industries that handle or store hazardous substances (e.g. the petroleum and chemical industries) have a major accident potential and several major accidents have also occurred during the last 35 years. Flixborough Disaster (1974), Seveso Disaster (1976), Bhopal Gas Tragedy (1984), Sandoz Chemical Spill (1986), Piper Alpha Disaster (1988), Philips 66 Disaster (1989), Esso Longford Gas Explosion (1998), Texas City Refinery Explosion (2005), and the Imperial Sugar Company dust explosion and fire (2011) are examples of accidents with devastating consequences to personnel, the environment, the companies and the local communities. Efforts have been made to enhance defenses against major hazards based on lessons learnt from the accidents. Despite this effort, it can be argued that the risk of major accident does not always show a positive trend. As shown in Fig. 1.1, the number of major hydrocarbon leaks, a key indicator for major accident risk in the Norwegian oil and gas industry, has for example increased between 2008 and 2010 on the Norwegian continental shelf [81]. There has also been a 50% increase in the number of hydrocarbon leaks in 2013 compared to 2012 [82]. Although this is lower than in 2010, it may still be a source of concern if the goal is continuous improvement.

The industry sectors associated with the aforementioned major accidents are regulated by responsible national authorities. The Petroleum Safety Authority (PSA) in Norway, the Health and Safety Executive (HSE) in the UK, the National Offshore Petroleum Safety and Environmental Management Authority (NOPSEMA) in Australia, the Occupational Safety and Health Administration (OSHA), the U.S. Environmental Protection Agency (USEPA) and the Bureau

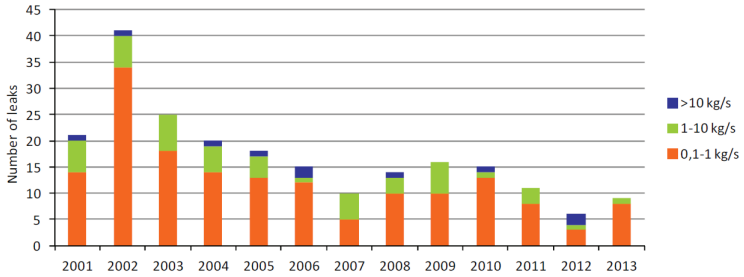


Fig. 1.1 Number of hydrocarbon leaks exceeding 0.1 kg/s, 1996-2013 [82]

of Safety and Environmental Enforcement (BSEE) in the US, are examples of national authorities that regulate the hydrocarbon and chemical process industries.

Major accidents are seldom the result of one failure, but often a combination of failures [75, 102]. High degree of technological and organizational complexity may be mentioned as an attribute of industries with a major accident potential [75, 87]. For this reason, it is common to deploy multiple and independent safety barriers that are capable of preventing or mitigating the consequences of unexpected events. This design philosophy is sometimes referred to as defense-in-depth (in e.g. the nuclear industry) [87] and layers of protection (in the process industry) [36]. Independence among barriers may be achieved by the use of different design principles, such as manual, mechanical and electrical/electronic/programmable electronic systems.

The integrity of barriers cannot be maintained without adequate level of maintenance. Maintenance is therefore a key activity to reduce the risk of major accidents. On the other hand, maintenance may have a negative effect on the system's performance if the execution is incorrect, insufficient, delayed, or excessive. Maintenance can also be the triggering event, for example by operating equipment wrongly. Furthermore, maintenance also exposes people to risk and should be minimized from this point of view. However, it is worthwhile to note that in spite of the aforementioned potential negative effects, maintenance has several other positive effects such as promoting the following: system reliability, production availability, productivity, occupational safety and health, product quality and environmental integrity.

Several investigation reports (e.g. of Health and Safety Executive in the UK and TNO in the Netherlands) have pointed at maintenance as a contributing factor to accidents in the petroleum and petrochemical industries [26, 56, 61, 62, 63, 92, 98]. Overall, the investigations indicate that about 30-40% of all accidents and accident precursor events in the chemical process industry are due to maintenance-related factors. About 30% of all major accidents

in the chemical process industry between 1982 and 1987 were linked to maintenance by UK's Health and Safety Executive (HSE) [26, 98], whereas about 40% of accidents involving chemical releases as reported by Koehorst in 1989 based on the analysis of accidents in FACTS database were linked to maintenance [26]. Hurst et al in 1991, reported that about 40% of 900 accidents associated with piping failures in the chemical industry were linked to maintenance [26]. Reports from the hydrocarbon industry vary in their estimation of how maintenance has contributed, and some studies attribute as much as 80% of all accidents and precursor events in the hydrocarbon industry to maintenance: About 65% of major hydrocarbon leaks on the Norwegian sector of the North Sea were linked to maintenance [114], and about 33% of hydrocarbon topside gas releases between 1985 and 1988 in Australia were linked to maintenance [59]. The significance of these statistics, coupled with the fact that most of the studies are relatively old (needing an update), is a clear sign that the relationship between maintenance and major accident risk is an important topic for further research.

The impact of maintenance on personnel safety has been studied by a number of authorities and research organizations, for example by SINTEF [61, 62, 63], by VTT [49, 50, 74, 117], by TU-Delft [26], and HSE-UK [34]. A number of strategies have been suggested to reduce the chance of personnel injuries and damages, but it is not necessarily the case that the results of these studies apply to major accident prevention [77]. According to Pitblado [77], the idea that battling minor incidents and personnel accidents will improve "safety culture" which will in turn reduce major accidents in the same ratio [4] was refuted by EU and USA data. He reiterated that "the approaches used to enhance personnel safety do not specifically address the barriers which control major accidents and thus it should be no surprise that the two do not correlate well." Furthermore, the study by [26] discusses, for example, the need to balance the trade-off between the risk to the plant, which may be reduced by more maintenance, and the risk to personnel, which is reduced by less maintenance (due to less exposure to major hazards).

In light of the preceding discussions and lessons learnt in relation to recent maintenance-related major accidents, it is reasonable to investigate and analyze maintenance-related major accidents, the implication of maintenance in their causation, how frequent they have manifested over time and how they can be prevented based on an in-depth understanding of the mechanisms of their causation.

Chapter 2
State-of-knowledge of concepts and gaps

2.1 Chapter introduction

The purpose of this chapter is to describe the state-of-the-art of concepts related to maintenance-related major accident risk and the need for increasing the knowledge in this area. The chapter is structured as follows.

First, the major accident concept will be discussed since it is the main problem confronting us that we need to investigate in search of knowledge of possible causes and how to prevent the causes.

Second, the maintenance concept will be introduced, because by having the potential to prevent or cause major accidents, maintenance obviously has a relationship with the major accident risk phenomenon. The PhD project is restricted to maintenance of safety systems, which is an important aspect. The purpose of these systems is to mitigate risk, and developing maintenance strategies with respect to risk reduction in relation to these systems is highly relevant. For other types of systems, there may be different objectives that are equally important (e.g. production availability vs cost), but these are outside the scope of this work.

Third, classification of accidents will be presented. Given that various accident reports indicate that maintenance can be a cause of major accidents and what the maintenance-related causes are, it is important to do some classification to harmonize/standardize the maintenance-related causes. This will make the study of maintenance-related major accidents convenient and will help in the speedy identification of any given maintenance-related cause in the future. It will also avoid duplicity and ambiguity, and will promote the repeatability of the application of classification schemes to accident analysis.

Fourth, organizational factors will be discussed. Attention need to be paid to the factors that guarantee organizational balance, not only the technical protective systems and how they should be maintained to prevent major accidents. A safely organized work environment is also necessary to bring the best out of such protective systems.

Fifth, the concept of robustness will be presented. It would be interesting to investigate how this also fits into making an organization, not only a physical system, to possess characteristics of resistance to accidental events.

Sixth, the effect of changing maintenance intervals will be treated. We need to understand, not only the sudden influence of maintenance in relation to major accidents, but also how changes to maintenance variables may influence risk stepwise until they reach the level associated with major accidents. This will help to promote monitoring in relation to risk control.

Finally, maintenance optimization will be presented. Given that there are several independent maintenance variables that influence risk, it is necessary to balance all of them in order to realize a value of a dependent variable which will offer the most beneficial risk reduction.

2.2 The major accident concept in the process industries

Before embarking on mapping out strategies to prevent maintenance-related major accidents, it is important to investigate and understand how the major accident concept is being perceived within the process industries. “Process accident” is probably more commonly used outside Norway than “major accident.” Besides, there exists variations in its definition across several organizations, which may influence what is being managed by the organizations.

The Norwegian Petroleum Safety Authority (PSA) [81], the European Commission (in relation to Seveso II directive) [18] and the UK government (in relation to the Control of Major Accident Hazards regulations) [103] have quite similar definitions for a major accident, which can be summarized as follows: An acute/adverse event such as emission/discharge/release, fire or explosion resulting in a serious loss with regards to human life/health, the environment or material assets.

The International Association of Oil and Gas Producers - OGP [65] and the Commonwealth of Australia [11] also have similar definitions for a major accident, which can be summarized as follows: Events connected with an installation having the potential to cause multiple fatality/serious damage inside or away from the facility.

The definitions of a major accident by the UK’s Health and Safety Executive (HSE) [33] and the US Occupational Safety and Health Administration (OSHA)/US Environmental Protection Agency (USEPA) [104] also have expressions that imply the potential for serious loss and that the effects may be felt inside or outside the facility. Similarly, the US Department of Energy (DOE) [17] defines an incident as “an unplanned event that may or may not result in injuries and/or loss” and an accident/accident event sequence as “an unplanned event or sequence of events that has an undesirable consequence.”

Terms used to describe major accidents are “adverse”/ “unplanned” and “acute”/ “sudden.” For the hydrocarbon/process industries it is releases of flammable and toxic material which is the main concern, although other types of events may also be relevant.

The main aspect of the accidents which make them “major” is of course the consequences. The exact definitions vary significantly, but for this purpose consequences to life and health, to the environment and to assets are all considered. Further, it is noted that some definitions require an actual consequence to have occurred (“Death or serious injury,” “One or more human fatalities”). However, in other cases, it is sufficient that there is a potential for a serious consequence (“Serious danger to human health,” “Escalation potential for multiple fatalities”). There is some difference in whether the effects should be limited to the facility where the event occurs or not, but this is considered to be mainly a difference between definitions primarily relevant for offshore facilities (which usually are remote and will not affect anyone outside the facility) and onshore facilities.

Although there is no universally agreed definition of a major accident, the various views of the aforementioned authorities may be harmonized to cover both large consequences and the potential to cause them. This is borne from the fact that there is more merit to look at the event from the perspective of its development (causal to consequential) rather than just around its end-state (consequential)[91]. The consequences are usually defined by more or less arbitrary factors, such as whether an ignition source is present at the time of a combustible gas release.

2.3 The maintenance concept

The modern concept of maintenance may be defined as the “combination of all technical, administrative and managerial actions during the life cycle of an item intended to retain it in, or restore it to, a state in which it can perform the required function” [19]. The required function of interest in relation to major accidents is safety function, specifically the mitigation of the major accident risk, whereas the items of interest on same basis are safety-critical systems, which pose a serious risk to the safe operation of the entire installation if they fail, e.g. process containment and ignition control systems [35].

The aforementioned definition of maintenance implies a top level classification of maintenance into two main categories, preventive maintenance and corrective maintenance, corresponding to retentive and restorative actions respectively. These decompose further to more specific types of maintenance as shown in Fig. 2.1. Introductory theories of the elements of the various classes of

maintenance can be found in the European standard on maintenance terminology [19].

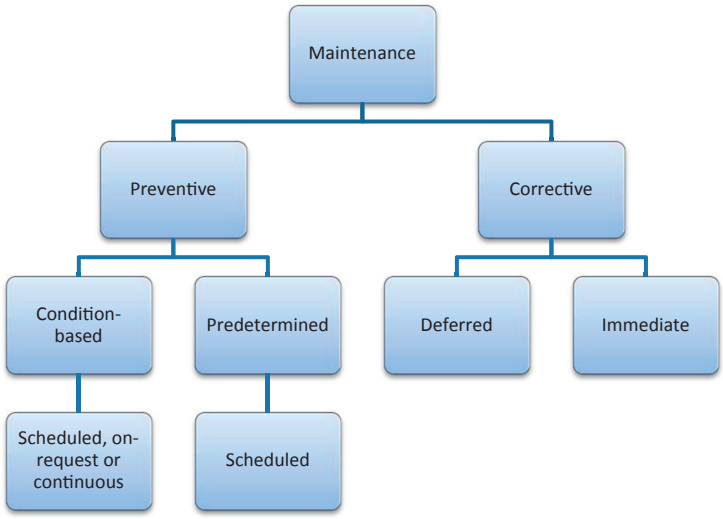


Fig. 2.1 Overall view of maintenance [19]

Furthermore, according to NORSOK Standard Z-008 [60], a generic maintenance concept is "a set of maintenance actions, strategies and maintenance details, which demonstrates a cost-efficient maintenance method for a defined generic group of equipment functioning under similar frame and operating conditions." This is also seen as "a collection of best practices for a company" that "should ensure that all defined HSE, production, cost and other operating requirements are met." It is partly implied that a negation of such best practices in relation to safety-critical equipment increases the major accident potential, thus failing to fulfill the HSE requirements. This is supported by Reason's [87] claim that safety systems require high level of maintenance contact, which implies high level of exposure of personnel to risk.

According to [26], interesting standards such as IEC 706-4 (Guidelines on maintainability) and ISO 9001 (Standard for assessing the quality management of design) exist, but are lacking in important contents with respect to the relationship between safety and maintenance. The former has a section of maintenance management, but does not feature maintenance personnel safety as a key element in developing a maintenance concept. The latter has no clearly stated

requirements for dealing with maintenance at the design stage wherein safety considerations could be incorporated.

Based on the aforementioned knowledge, it is pertinent to investigate maintenance shortcomings that resulted or nearly resulted in major accidents. This is necessary for continuous improvement of the process of maturing, refining and perfecting maintenance strategies. It will go a long way to enrich documents for operational risk control, e.g. standard operating procedures, safe work procedures, etc.

2.4 Classification of maintenance-related major accidents

Having realized the significant implication of maintenance in major accident causation, as revealed in the aforementioned statistics, it is compelling to identify and classify maintenance-related causes based on existing theories and observations from accident investigation reports. The relationship between accident investigation and accident analysis as shown in Fig. 2.2 illustrates that the former is usually done on accidents individually over time, whereas the latter studies a defined group of investigation reports on accidents that have occurred within a given period of time.

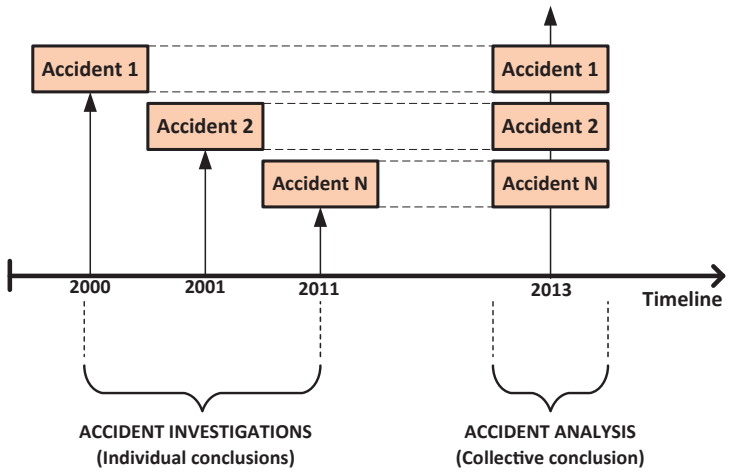


Fig. 2.2 The relationship between accident investigation and accident analysis

Classification may be applied to accident analysis whereby it clearly delineates and tends to standardize causes, the object of prevention. The merit is that prevention efforts become more focused and efficient, instead of wasting time trying to work out directions. Classification of accidents is the assignment of particulars/properties of accidents to groups within a system of categories distinguished by origin of event, end-state of event, mode of occurrence, magnitude of event, physical appearance of event, impact of event, timing of impact, impact location, etc [46, 51]. The origin of the event implies the cause of the accident. This expression has the potential for misinterpretation, hence, it is important to discuss it further. Interesting questions to ask here are "What is a cause?" and "Is ignition the cause of an explosion?" These questions are difficult to answer. Although a scientist would seek to know exactly the mechanisms by which one thing causes another, it is difficult sometimes, as in this case, where there is heterogeneity of causal circumstances. Therefore, it would be more convenient for him/her to say, e.g. that A probably causes B based on statistical correlation between A and B considerably greater than chance [29]. In fact, causal circumstances are broad in nature, covering not only technical circumstances, but also human and organizational circumstances such as complexities, communication gap, conflicting goals, etc. Hence, it is worthwhile to investigate and analyze all of these to see, especially, how they combine to realize a major accident, since "accidents are neither chance events, nor acts of God, nor triggered by a few events and unsafe human acts immediately before they occur" [102]. This will make our preventive measure all-encompassing and more effective. Besides, the way accidents are classified can influence how their preventive measures are developed.

Different studies [25, 26, 32, 62, 92, 98, 113, 115, 116, 119] have explicitly or implicitly classified maintenance-related causes of major accidents in the chemical process and hydrocarbon industries in different ways as shown in Table 2.1. All the classification schemes are relevant, although no single scheme explicitly covers all the relevant perspectives at a time - human, organizational, technical and operational. Some of the researchers may have focused on a particular area based on the prevailing purpose, the boundaries set by some authorities or some other reasons. Overall, most of the work that has been done, has been from a maintenance management perspective rather than the accident process perspective. Besides, some of the aforementioned categorization are coarse, thereby overlooking certain important details.

2.5 Organizational factors in major accidents

Given that accidents are not the product of technical failures only [15], it is important to also include organizational factors in analysis and investigation

Table 2.1 Review of classification of causes of maintenance-related major accidents

Sources	Nature of classification
On the analysis of hydrocarbon leaks in the Norwegian offshore industry [115]	Four main categories based on work process: Planning, preparation, execution and reinstatement. Planning implied "long term and short term planning, including overall schedules, Safe Job Analysis and preparation of the isolation plan, whereas preparation implied "shutdown, isolation and depressurization according to the isolation plan" and reinstatement implied "resetting of valves and controls according to isolation plan, as well as the leak testing and starting up."
Evaluation of the Risk OMT model for maintenance work on major offshore process equipment [25]	Two main categories based on initiating events: Human intervention introducing latent error and human intervention causing immediate release. This was integrated with Reason's classification [87].
Correct Maintenance Prevents Major Accidents [62]	Two categories: Insufficient and poor maintenance.
Analysis of hydrocarbon leaks on offshore installations [114]	Two main categories based on initiating events: Human intervention introducing latent error and human intervention causing immediate release.
Maintenance-Induced Accidents and Process Piping Problems [92]	Two maintenance-related categories: Improper and insufficient maintenance.
Know when to say "When": A Review of Safety Incidents Involving Maintenance Issues [119]	Three categories: Causes present before, during and after maintenance.
Major accidents in process industries and an analysis of causes and consequences [45]	A more general classification of major accidents in the process industries, but did not classify maintenance-related causes specifically.
Evaluating safety in the management of maintenance activities in the chemical industry [26]	Classification of causes in terms of maintenance management shortcomings in management of the preparation of resources, scheduling and work planning, actual conduct of the work, maintainability and external factors. It also featured classification of causes in terms of maintenance-related work phases: Preparation, maintenance itself, handover, startup, shutdown and normal operation).
Managing the Risks of Organizational Accidents [87]	(1) There are two main classes of (maintenance-related) failures: Active and latent conditions, (2) There are two main sources of maintenance causes: Disassembly and reassembly, (3) There are three main classes of (maintenance-related) human error: skilled based slips and lapses, rule-based mistakes and knowledge-based mistakes, and (4) Maintenance-related causes are due to: (i) neglected maintenance and (ii) the likelihood of error of commission or omission.
The role of maintenance management deficiencies in major accident causation [98]	Classification in terms of maintenance management inadequacies in corporate and maintenance objectives, strategy and workload, resources, administrative structure, work planning and work control, and plant reliability control.
Human Error [86]	Three main categories of (maintenance-related) causes based on human failures: Human error, violations and sabotage.
Dangerous maintenance: A study of maintenance accidents and how to prevent them [32]	Classified maintenance-related causes according to timing of incident as follows: Preparation (before maintenance), the job itself (during maintenance) and the return of the plant to operation (after maintenance)
Handbook of human reliability analysis with emphasis on nuclear power plant applications [100]	Classified errors into two: Errors of omission and errors of commission

processes to better understand how to focus management and personnel orientation/training in order to enhance prevention efforts. Organizational factors in relation to major accidents (also called organizational accidents) usually refer to the organizational causes of major accidents.

The organizational accident perspectives include: Energy-barrier model, normal accident theory (NAT), high reliability organizations (HRO) theory, man-made disaster (MMD) theory, conflicting objectives, adaptation and drift (COAD) theory and resilience engineering. The energy-barrier perspective is dominant in the list. However, it is necessary to improve accident analysis with the various other perspectives as technology and organization become more and more complex, since the technically-biased, energy-barrier principle is not sufficient in dealing with organizational deficiencies.

The energy-barrier perspective, which is based on the hazard-barrier-target model of Gibson [23], depicts a linear progression of events from the release of energy (hazard) through interposed barriers to the interaction between the energy (hazard) and the target (See Fig. 2.3). The model is hinged on the concepts of linearity and monocausality, i.e., the transfer of a given energy from the source to the target. This model also forms the basis for Reason's Swiss Cheese Model [87] and the "defense in depth" principle (See Fig. 2.4). An example of how this has been institutionalized in risk management can be found in the Norwegian regulations for offshore installations, where a separate section in the Management Regulations is dedicated to barriers [80].

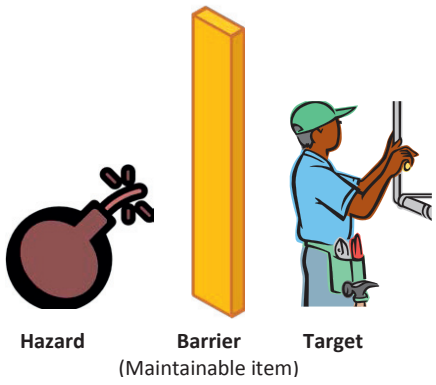


Fig. 2.3 The energy-barrier model [23]

Over time, other organizational accident perspectives evolved and found their way into being accepted as valid major accident theories. These include: Normal accident theory (NAT), high reliability organizations (HRO) theory, man-made

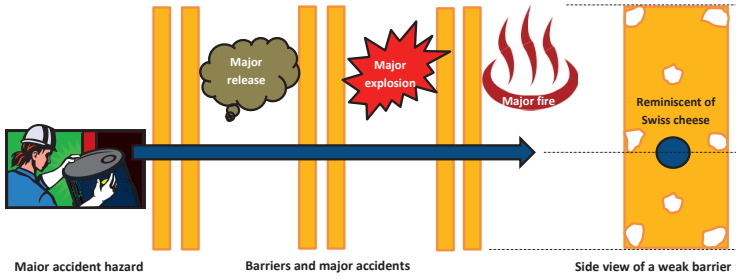


Fig. 2.4 "Defense-in-depth" philosophy with weaknesses represented as Swiss cheese holes [87]

disaster (MMD) theory, conflicting objectives, adaptation and drift (COAD) theory and resilience engineering.

The normal accident theory (NAT), proposed by Perrow [75], expresses the concept of accident proneness (i.e natural tendency towards accidents) owing to the interactive complexities (technological and organizational) and tight couplings that evolve as our world of technologies continue to expand [75]. The Normal accident perspective is hinged on complexity and coupling. Perrow [75] believes that the multiple barriers and redundancies that characterize such high-risk technologies (which are being managed on the premise of the energy-barrier model) could offer some level of safety, but will subsequently increase the system's degree of complexity and tightness of couplings. The policy reversal in Germany (driven by the Fukushima disaster in Japan) that will see all her nuclear power plants abandoned by 2022 [3] may be seen as a logical and necessary result of NAT.

The HRO theory has been developed from studies of organizations which, according to normal accident theory, should experience major accidents, but which still have excellent safety records [48]. The foremost example used to illustrate this is aircraft carriers, but other organizations, like hospital emergency rooms, have also been studied. A number of technologies we have today have great productive potential and at the same time great destructive potential, such that the avoidance of a significant failure is imperative [48]. According to Sagan [90], HRO organizations inherently possess the best safety records of all high-risk technologies. HRO theorists believe that through management commitment to safety, the establishment of safety culture, the maintenance of relatively closed systems, functional decentralization supported by constant training, technical and organizational redundancies, and organizational learning supplemented by anticipation and simulation (trial-and-error process), organizations could achieve the consistency and stability required to support failure-free operations [15, 48, 90, 91]. This is illustrated in Fig. 2.5, where the shaded boxes and red arrows represent HRO elements, whereas the unshaded

boxes and black arrows represent the accident process elements. The idea behind the figure is adapted from the aviation industry [88] which may be seen as an HRO [90]. The figure illustrates that threats and errors can occur separately or at the same time and can cause undesired state of facility (e.g. hazardous state), unless they are properly managed. In addition, the latent conditions, by themselves, can also cause undesired state of facility, unless they are properly managed. In a typical accident, these act together with threats and errors. Information about latent conditions, threats and errors can be fed to the "organizational learning and safety culture" element of the HRO safety management system for analysis and appropriate corrective measures to be fed back to the causal state (i.e. sources of latent conditions, errors and threats). The "organizational learning and safety culture" element can also receive useful information about undesired state of facility, accidental event and consequential outcomes for analysis and subsequent feeding of corrective actions to the causal state. Besides, the "organizational learning and safety culture" element is being supported by other elements such as "failure analysis," "decentralization of failure management authority" and "balancing of safety and production goals" which also influence each other as shown. Furthermore, the failure of redundant safety functions (which influence risk management) can be corrected by the "technical personnel redundancy" element with the help of the "failure analysis" element.

The man-made disaster (MMD) theory considers accidents to be the result of accumulated flaws in information processing between various organizational units, including the administrative, managerial and operational units [102]. Turner [102], the initiator of the theory, calls the period of accumulation an incubation period (i.e. a period of maturity). At the end of the incubation period, the perceived organizational quality is unable to co-exist with the accumulated organizational deviations, thus leading to an accident. A key point in this theory is that there exist warning signs within the organization that could have been used to prevent accidents, if it had been accumulated and communicated in the right way and to the right people as illustrated in Fig. 2.6. This figure (presented according to IDEF0 functional modeling method) illustrates a maintenance management exercise (i.e. the process) that is required to be implemented by maintenance personnel (i.e. the mechanism), by applying a valid method (e.g. Condition Based Maintenance) and maybe together with a "facilitator" (e.g. Computerized Maintenance Management System) - the control. With respect to safety-critical systems, the failure to feed the aforementioned elements with the right information (i.e. the input) leads to an accident (i.e. the output). This perspective is hinged on multicausality and the concept behind it is sociological; it holds that accidents are not just a technological phenomenon [15].

The conflicting objectives/goals (or decision-making) perspective was proposed by Rasmussen [84] and considers major accidents to be the result of organizational objectives clashing with each other (See Fig. 2.7). The result of

this conflict is an organization in a state of dilemma that may drift over time due to lack of information or inability to balance the objectives correctly. Examples of organizational objectives that may come into conflict include production objectives, safety objectives etc. The basic resource used to drive the realization of these objectives is money and the application of this resource must create a balance between objectives to guarantee the survival of the organization. The balance between production (economic objective) and protection (safety objective) was also discussed by Reason [87].

The resilience engineering perspective describes the ability of organizations to achieve ultra-high levels of safety and response to the dynamics of other organizational values (e.g. production, operations, economy etc.) despite complexities, high risks, major accidents, disturbances, disruptions, continuous pressure and change [89, 124]. Accidents, according to this perspective, are not the product of normal system malfunction or breakdown, but rather a breakdown in the adaptive capacity necessary to cope with the real world of complexity [15]. In [31], resilience is defined as "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions." Furthermore, the authors consider anticipation, responding, monitoring and learning as the abilities necessary for engineering resilience into organizations [30, 31]. Resilience, as applied in this thesis, is about being able to adapt to or recover from accidental events, while stability is acquired in a new state [2]. This definition is also associated with the aforementioned abilities of resilience. The resilience engineering perspective encompasses core topics from the five perspectives described earlier [15, 89]. A resilience engineering model based on the aforementioned views is shown in Fig. 2.8.

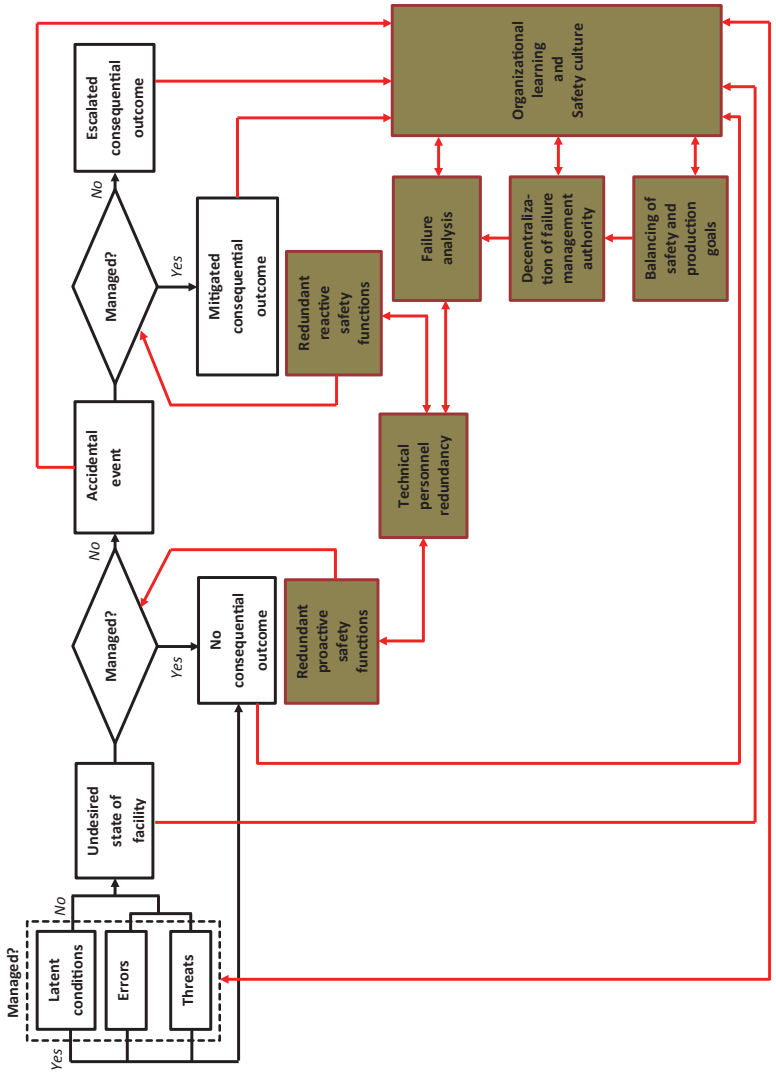


Fig. 2.5 A model illustrating the HRO theory (adapted from the TEM framework [68, 88])

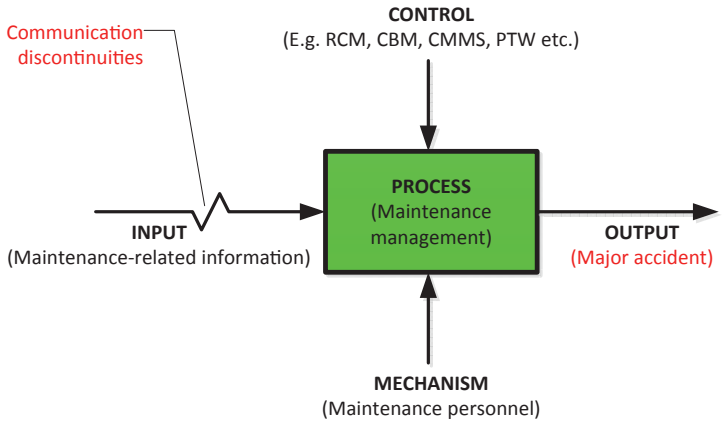


Fig. 2.6 An illustration of man-made (maintenance-related) disaster theory with IDEF0 model

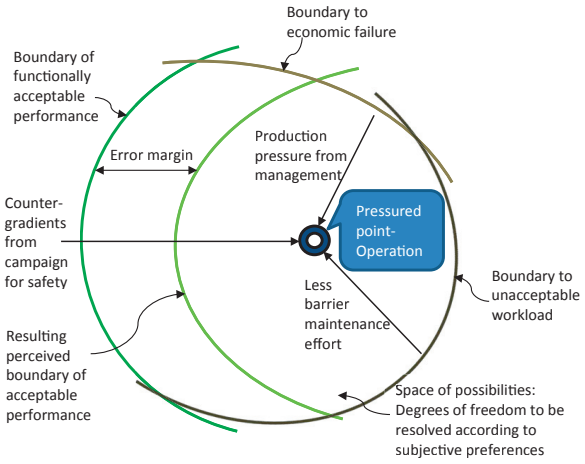


Fig. 2.7 Rasmussen's conflicting objectives model adapted to maintenance [84]

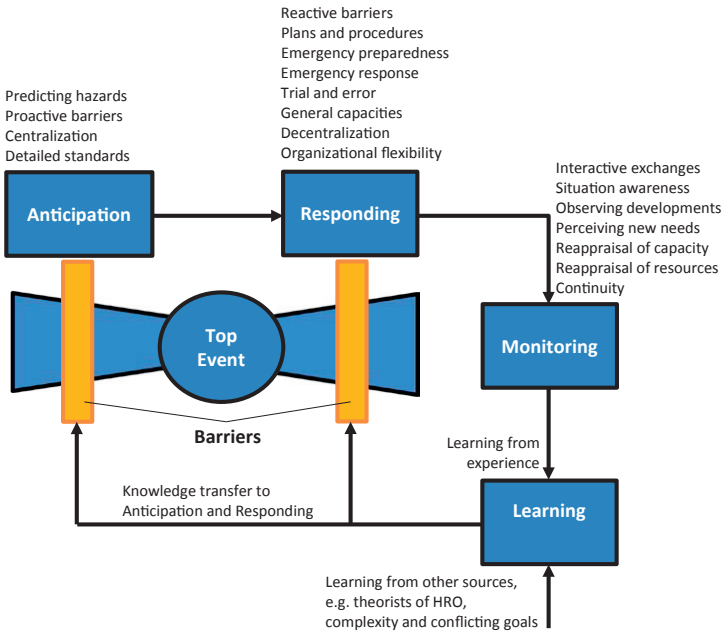


Fig. 2.8 A model illustrating the resilience engineering concept

2.5.1 Final remarks

As mentioned above, a maintenance organization makes efforts to keep major accident barriers functional. This implies that there is an inducement of functionality by the maintenance personnel to the barrier. Yet, we may be tempted to ask: How can the integrity of the maintenance organization itself be maintained in order for it to be effective in inducing functionality to the barriers? This is a problem that the energy-barrier perspective cannot solve alone. It is noted however, that few of the aforementioned perspectives have had significant influence on practical risk management. Although the energy-barrier principle dominates completely, aspects of HRO and resilience are being used in some contexts [16, 89]. Besides the energy-barrier perspective, the other perspectives have no significant evidence of having been sufficiently investigated to uncover all possible relationships with maintenance. The choice of perspective may have important implications for how the management of major accident risk is approached. It may therefore also influence our view on maintenance-related ma-

jor accidents; in other words, how we perceive maintenance, both as a means to reduce risk and as a cause of accident.

2.6 The concept of robustness

Robustness is also an interesting concept that has featured in organizational theories besides resilience. It is sometimes misconstrued for resilience, but they are not the same. The definition of robustness varies from one field of science to the other, and so one has to be careful to apply the definition that is most meaningful to the research depending on his/her field. Robustness, according to Asbjørnslett and Rausand [2], encompasses resistance to accidental events, restoration of functionality and retention of original stability. Chandra and Grabis [9] defines robustness as "the ability to withstand external and internal shocks."

Furthermore, robustness as seen by Pavard [73], is the ability of a system "to adapt its behavior to unforeseen situations, such as perturbation in the environment, or to internal dysfunctions in the organization of the system." Other studies have been done on robustness by Anderies, Nielsen and Boissieres [1, 7, 58]. Few studies have analyzed organizational robustness in relation to major accidents [58] or maintenance [7].

Various industrial settings have different configurations of independent and coordinated units aimed at realizing the set of organizational goals. It is important to address this situation specifically to achieve a better solution for a given industry. One of the organizational goals in the process industries is major accident prevention. To this end, maintenance may be investigated for the properties of robustness by which the organization (not just systems alone) can be further "strengthened." Robustness, as applied in this thesis, is the ability to resist or counteract accidental events.

2.7 Pros and cons of changing maintenance intervals

Beyond the influence of hands-on maintenance practice and its organization on the barriers that prevent major accidents (at the "macro level"), it is also important to investigate in detail all possible causal relationships between major accidents and maintenance, taking into consideration also the amount of maintenance, the maintenance decisions, the visitation frequency of the maintainers, the number of the maintainers, etc (at the "micro level"). This is necessary because it is not only maintenance-related barrier failure that influences the maintenance-related major accident risk, even though the barriers are dedicated to major accident prevention.

With increasing complexity and dependency on technical systems, the need for maintenance also increases. At the same time, maintenance may also represent a risk, because accidents may be initiated by maintenance itself.

As regards the effects of increasing and decreasing maintenance, maintenance when insufficient or excessive involves avoidable risk. With low maintenance frequency (long intervals), it can be expected that the risk associated with equipment failure will decrease as we increase the frequency. However, we may also reach a point where the risk starts increasing again, because the maintenance itself may wear out the equipment. Increasing maintenance frequency in the process industries will also increase the exposure of personnel to existing hazards, increase the potential to introduce new hazards and initiating events, increase error opportunities and increase the potential to bypass/override safety systems, whereas decreasing maintenance will increase the vulnerability of items to failure mechanisms.

Neglected maintenance (an aspect of decreasing maintenance interval), if due to lack of maintainability rather than nonchalance, may encourage technological advancement for improving manufacturing techniques and the intrinsic reliability of materials/components [87]. This is expected to diminish the risk due to maintenance neglect, since the level of maintenance activity (i.e. amount of direct human contact) will decrease [87]. However, there is a limit beyond which we cannot go: It would be uneconomical (given the cost and complexity of a modern technological system) to design systems for zero maintenance, whereby all components have the same lifetime that is equal to the planned life of the entire system [42]. This limitation may not apply to certain subsea systems, probably due to the challenges of carrying out regular maintenance underwater and the vast income from oil and gas which profitably pays for systems that tend to be maintenance-free.

The goal is to apply the amount of maintenance that is necessary and sufficient while considering a given item's failure rate among other important factors. This brings about the need to establish a method for the minimization of maintenance-related risk. It is therefore of interest to make a more holistic study of the positive and negative impacts of maintenance and develop the most optimal strategy for doing maintenance. In a nutshell, this leads us to the issue of maintenance optimization.

2.8 Maintenance optimization

Maintenance optimization is about balancing the benefits of maintenance with the cost or risk involved. The element of maintenance being optimized may be the interval, the strategy, the manpower, the spare parts, the time of renewal, grouped activities, etc [107]. The choice of whether to do a cost or risk based

optimization is critical. For relatively low-risk operations, it may be acceptable to do cost-based optimization while keeping safety as a constraint. However, for high-risk operations (usually linked to the potential for a major accident), a risk-based optimization is crucial due to the extreme, potential consequences of insufficient control. Besides, by assigning cost to risk we can optimize with respect to both at the same time.

Several efforts have been made with the aim of optimizing maintenance frequencies in order to minimize equipment maintenance costs while safety is not compromised. The early methods focused on test interval optimization based on minimizing the time-average unavailability without considering cost [28, 37, 96, 110]. This approach was later extended to optimization based on cost with safety primarily being a constraint [13, 109, 106, 111, 112] and optimization based on equipment risk without consideration for risk to humans [38, 39, 40, 43, 44, 111]. Cost-based optimization is being widely applied in industrial engineering. The latter features as a step in the RCM (Reliability Centered Maintenance) process where it is used to optimize the maintenance interval after a suitable maintenance task would have been selected with the RCM decision tree [85]. In addition, cost-based optimization has also found application in the concept of maintenance grouping [27, 57, 66, 108, 122, 123].

Reason [87] in his book chapter titled "Maintenance can Seriously Damage your System" highlights the effect of the amount of direct contact between people and the system. According to him, such contacts constitute the greatest human performance problem in most high-risk industries where frequency of contact can be seen as a greater error opportunity. The likelihood of error is further analyzed together with neglected maintenance to explain the risks they posed to the system [87]. Reason [87] phrased this as "the maintainer's touch can harm as well as heal." Besides, Reason [87] views the safety-criticality of items as a key contributor to the motivation for high level of maintenance contact (which implies high level of exposure of personnel). As regards optimization to justify the rationale for preventive maintenance, Reason [87] suggests a graphical approach (Cost Vs. Level of maintenance plot) whereby the optimal level of preventive maintenance is determined by combining the cost of both preventive and corrective maintenance and then selecting the level that coincides with the lowest overall maintenance cost.

Some previous events can be seen to support the concept of risk-based optimization with consideration for risk to humans. According to Evans and Thakorlal [20], the issue of maintenance frequency has resulted in a paradigm shift in the design of unmanned platforms following the Piper Alpha disaster in 1988. Firefighting systems, e.g. fire pumps, are usually not installed anymore based on the reason that the risk reduction benefit they offer to maintenance personnel for unmanned platforms is not commensurate with their frequency of visits unlike in a manned facility [20]. In other words, safety systems such as fire pumps are considered to offer negative risk balance with respect to an unmanned platform

in relation to the frequency of visit of maintenance personnel. The aforementioned paradigm shift is also supported by the concept of inherently safer design (ISD).

A human-risk-related preventive maintenance problem has also been studied earlier in The Netherlands, where the focus is on scheduling maintenance to prevent fatalities due to unmanageable railway track maintenance workload at night [105]. However, as regards risk-based optimization with consideration for risk to humans, a literature that treats it explicitly and comprehensively has yet to be identified.

Chapter 3
Research questions and objectives

3.1 Research questions

Research questions indicate what the researcher wants to know first and above all. He/she then performs a research necessary and sufficient to find answers to the questions. The research questions also give cues on the research methods to be applied in order to answer the questions. In addition, they help to identify specific objectives that the research will be tied to. Besides, being able to find answer to a research question will help address a "research problem" which is a problem "readers think is worth solving" [121].

Further to the aforementioned discussions and the lessons that recent maintenance related major accidents (e.g. Imperial Sugar dust explosion and fire in the U.S.) have taught us, it is reasonable to ask the following questions:

3.1.1 How does maintenance influence major accident risk?

Maintenance is a key means to improve and maintain the integrity of plant operations and systems. Lack of maintenance or erroneous maintenance may, however, cause a sudden or gradual development into a system failure. Even perfectly performed maintenance may have a negative impact on risk. Personnel are exposed to more risk while executing maintenance than during normal operation and too frequent maintenance may cause rapid wear-out of equipment. In the execution of maintenance, new hazards and failures may be introduced without being noticed [97]. Management decisions, sometimes distant from the maintenance planning and execution, may introduce small changes in prioritization, organization, and resources available for maintenance, whose (unwanted) consequences are not so easy to foresee. Complex organizations and systems, like those that we find in the petroleum and petrochemical industry, challenge sim-

ple causal relationships between underlying events and major accidents. Maintenance may be a triggering event in an accident sequence, but also a direct or indirect cause of barrier failures. Øein et al [62] have linked improper equipment classification to major accident risk; this study does not seem to be complemented by other research initiatives. A conceptual and holistic model may have to be established that relates different kinds of maintenance and decisions (at the "micro level") to major accident events (at the "macro level").

3.1.2 To what extent has maintenance been a cause of major accidents?

There are always lessons to learn from prior accidents, from studying them individually and by analyzing them jointly to identify the more underlying phenomena of causes. Many investigation reports, articles and books, published after major accidents and precursor events, address maintenance-related issues. What seems to be lacking is in-depth analysis of maintenance as a contributing factor to major accidents when comparing the lessons learnt from several accidents. To what extent has maintenance influenced the accidents, and what were the most frequent causes? Do prior accidents point at particular types of maintenance deviations as more dominating in their contribution to major accidents?

3.1.3 How should maintenance be optimized in relation to the major accident risk?

Prior knowledge reveals that increased preventive maintenance frequency implies increased opportunity to prevent functional failure and this increases the exposure of personnel to risk. Similarly, increased maintenance frequency also increases the opportunity for making errors [87] and this may increase risk. Hence, there is the need to establish a means of determining the optimal maintenance that minimizes risk. Several cost-based maintenance optimization models exist, wherein safety is being kept as a constraint. Besides, very few risk-based maintenance optimization models have also been seen, where the focus is on risks generally, not delineating a minor risk from a major risk. These are also focused on risk to equipment, with little or no attention to human risk. We cannot be certain that a risk-based optimization method that is suitable for minor risk is equally suitable for major risk. Given our challenge of "confronting" the major accident risk, cost-based optimization is not considered suitable. Yet, the existing risk-based optimization may not be sufficient, which calls for further investigation and validation.

3.1.4 How can maintenance contribute to the robustness and resilience of organizations?

The purpose of maintenance is to prevent failures and restore systems to a functioning state. Maintenance also contributes to improved system knowledge and interdisciplinary coordination that may benefit the entire organization. This may indicate that maintenance may be a contributor to robust and resilient organizations whose ability to act upon unexpected events is improved. It is therefore of interest to investigate how maintenance can be performed to gain this "added value" of increased organizational robustness and resilience.

3.2 Research objectives

Research objective is about what one's goal is with respect to the research. In other words, it is the contribution to the body of knowledge or the service of society being pursued. The need for new knowledge led to the setting of academic or scientific objectives and the determination of the scope of the thesis [54].

The overarching objective of this PhD project is the development of new strategies for the prevention of maintenance-related major accidents in the process industries. This objective encompasses the following set of objectives:

Objective 1: The realization of a well-structured framework and expanded/modified knowledge about the causal relationship between maintenance and major accident.

- 1st sub-objective: A completed investigation of how maintenance influences major accident risk in relation to the energy-barrier perspective of major accidents.
- 2nd sub-objective: A developed classification scheme for maintenance-related effects on major accident risk.
- 3rd sub-objective: A completed investigation of how maintenance influences major accident risk in relation to other perspectives of major accidents.

Objective 2: Enhanced demonstration of the applicability of the knowledge derived from the causal relationship between maintenance and major accidents.

- 1st sub-objective: Current figure on what percentage of major accidents is caused by maintenance in addition to other relevant statistics.
- 2nd sub-objective: Empirical evidence showing the practicability of the newly developed classification scheme by using it to classify the maintenance influence in a large number of major accidents.
- 3rd sub-objective: Applicability of the results (statistics) generated to maintenance management.

Objective 3: The proposal of novel risk reduction strategies for maintenance-related major accidents.

- 1st sub-objective: An improved basis for maintenance optimization which allows for optimization with respect to major accident risk, not just cost
- 2nd sub-objective: A developed framework of maintenance strategies for improving the robustness and resilience of organizations

3.3 Scope

The scope of this PhD project covers the following:

- Major accidents: This will involve exploring theories and investigation reports in relation to major accidents. It will focus on maintenance-related major accidents and will consider both major accidents and precursor events.
- Sociotechnical system: The study will touch on human, organizational, technical and operational elements, but will not be a social science study. It will also analyze the organizational accident perspectives and their relationship with maintenance.
- Maintenance optimization: This will be based on optimizing maintenance interval in terms of risk, while delimiting the optimization with no cost analysis. It will be limited to safety systems.
- Application areas: The research will be focused on the hydrocarbon and chemical process industries, however, it may draw inspiration from other industries.

Chapter 4
Research methodology and approach

4.1 Overview of research

The purpose of this section is to present the background for the specific research approach being applied in this PhD project.

Research, as defined in Merriam-Webster dictionary [53], is "studious inquiry or examination; especially: investigation or experimentation aimed at the discovery and interpretation of facts, revision of accepted theories or laws in the light of new facts, or practical application of such new or revised theories or laws." Methods of research encompass scientific research and research in the humanities. In this PhD project, the focus has been on the scientific.

Scientific method, as defined in Merriam-Webster dictionary [53], is "principles and procedures for the systematic pursuit of knowledge involving the recognition and formulation of a problem, the collection of data through observation and experiment, and the formulation and testing of hypotheses." Research method is about how one wants to reach the goal of the research. In other words, it is a means to realizing the research objective.

Generally, research may be classified in many different ways. However, on a broader level, all research can be classified in relation to the quantifiability of data into:

- *Qualitative*: Qualitative research, as defined by Saunders [93], is "research dealing with phenomena that are difficult or impossible to quantify mathematically, such as beliefs, meanings, attributes, and symbols."
- *Quantitative*: Given [24] sees quantitative research as "the systematic empirical investigation of any phenomena via statistical, mathematical or computational techniques."

It is arguable that quantitative research and qualitative research can go hand in hand, with the latter supporting the former. This is maintained by Kuhn [47] in the following words: "large amounts of qualitative work have usually been prerequisite to fruitful quantification in the physical sciences." In addition to being

either qualitative or quantitative, research, depending on the discipline (whether arts, humanities, social sciences, pure sciences or applied sciences etc.) may be classified further into several types such as [93]: Basic, applied, correlational, descriptive, ethnographic, experimental, exploratory, grounded theory, historical and phenomenological.

This PhD research project falls into the technological/engineering science category of four research cultures including natural science, social science and humanities. In the technological/engineering science category, research may be classified also in relation to the degree of practicability according to the following.

- *Basic research*: This is also called fundamental research and is pursued to increase the knowledge base of a particular field of study [8]. It may be classified into two: Pure basic research and oriented basic research.
  - *Pure basic research*: This is "research carried out for the advancement of knowledge, without working for long-term economic or social benefits and with no positive efforts being made to apply the results to practical problems or to transfer the results to sectors responsible for its application" [64].
  - *Oriented basic research*: This is "research carried out with the expectation that it will produce a broad base of knowledge likely to form the background to the solution of recognized or expected current or future problems or possibilities" [64].
- *Applied research*: This is "original investigation undertaken in order to acquire new knowledge which is directed primarily towards a specific practical aim or objective" [64]. Applied research uses the knowledge base created by basic research to devise solutions, often technological, to specific problems [8].

Scientific research may also be seen from the following main perspectives [21, 22, 54, 76]:

- *Theoretical research*: A theoretical research may involve a novel application of an existing theory, the extension of the theory, the modification of the theory, the validation of the theory (with rational arguments) or the development of a new theory.
- *Empirical research*: An empirical research may involve observation, experimentation or experience. Empirical evidence may be collected through experiments, from investigation reports, in-service data etc. They have the potential to validate a theory or refute it. This is subject to the fulfillment of some criteria, including statistical significance of the empirical data, repeating experiments etc.

One thing both perspectives have in common is that they are methods of acquiring knowledge and involve a careful perusal of mostly published works like

international peer-reviewed journals and conference proceedings. The perspectives may also involve the use of reports from reputable research institutes and the R&D (research and development) department of companies.

The data collection method in research may also be qualified as scientific or otherwise. In addition to literature review (which cuts across nearly every academic field), scientific methods that can be used for collecting data include the following [6, 55]:

- *Case study*: This is useful in getting a comprehensive contextual view of a particular phenomenon. Generalization should be handled carefully, since case studies are focused on special cases as implied in the name. It is advisable that theoretical concepts are used in relation to generalization.
- *Textual analysis*: This can be an interpretative textual analysis or a quantitative content analysis (e.g. how many times an event features in a given medium). The textual extracts have to be clear, consistent and logical. Logic enhances plausibility of reasoning, enables distinction between correct reasoning and incorrect reasoning and enable the evaluation of reasoning that links premises to conclusion [79].
- *Experiment*: This involves the manipulation of an independent variable under well-controlled conditions to know whether and how it causes a change in the dependent variable and by how much.
- *Action research*: This is peculiar to social sciences and involves real-life settings of which the researcher forms a part of the operation.
- *Natural observation*: This is an observation in the field or in real-life settings without interferences such as artificial interventions and laboratory limitations.
- *Survey*: This is carried out with data collected through standardized interviews or questionnaires.
- *Statistical sampling*: This involves identifying relevant statistical populations, selecting a subset of individuals (i.e. sample) and collecting information related to the latter to evaluate characteristics of the former.

How data are interpreted depends on the theoretical background (previous knowledge) [55]. Theory encompasses concepts (i.e. measurable objects, phenomena, events etc.), causal relationships, structural pattern, lawfulness, or explanations, models (mathematical, analogy, etc) [55]. Theories/models enable theoretical integration of knowledge (systematics), predictability of behavior and generalizability of experiences (data), although the imperfection of theories is not improbable [55]. Aristotle, the great philosopher, says: There is nothing like improbability; sometimes the most improbable thing happens. It is also required of researchers to justify or validate theories with empirical evidence. However, the theories may be false even though there may be a match between them and a limited amount of data, so Popper [79] suggests that it is equally reasonable to also try to falsify the theory and see what happens.

Furthermore, scientific research may also be classified according to some methodological traditions which encompasses the following [5, 6, 41, 55]:

- *Positivism*: According to Kasim [41], modern quantitative research evolved from Auguste Comte's philosophy of positivism, which emphasized "the use of the scientific method through observation to empirically test hypotheses explaining and predicting what, where, why, how, and when phenomena occurred."
- *Interpretivism*: This considers social sciences to be about the qualitative understanding of an artificial object within its cultural, historical, and in situ context.
- *System theory*: This is partly critical of positivism but premised on the same scientific ideal, and encompasses system thinking (i.e. inquiring to understand how things, regarded as systems, influence one another within a whole), system decomposition (i.e. breaking down a system into its components subsystem and analyzing each separately, e.g. hierarchical decomposition), system aggregation (i.e. putting the analyzed components subsystem back into the system), systems integration (i.e. integrating information sources and prior knowledge), verification (i.e. confirming that that research was carried out in accordance with the requirements) and validation (i.e. an acceptance that the research truly solves the problem that it was intended for).

4.2 Overview of scientific method

Generally, research can be seen as structured in nature, although there may be variations in the sequence of steps depending on the subject matter and the researcher's disciplinary leaning. The formalities of scientific research usually align with the following systematic procedures and steps [99, 101, 118, 120]:

- *Observation and formulation of question*: This begins with observations about the unknown, the vague or novelty, and is followed by thorough investigation of theories related to what was observed. The theories should be screened for relevance and not chosen randomly. This helps to narrow down as much as possible to the main focus area of the research and saves time and effort since extensive review of literature is necessary to identify research gaps. The justification for the research should be established by linking its significance to existing knowledge about the topic. A research gap in existing literature, as identified by the scientist, provokes a research question. The research question may be parallel to the hypothesis - the supposition that requires testing.
- *Hypothesis*: Hypothesis is a conjecture, a suggested explanation for our observation, whose trial confirms or falsifies the perceived relationship between

two or more variables. It is based on knowledge obtained while formulating the question.

- *Predictions*: Predictions by reasoning (including deductive reasoning) are made possible by a good hypothesis. Deductive reasoning, also called deductive logic or logical deduction or, informally, "top-down" logic, is the process of reasoning from the more general (theories) to the more testable specific (hypotheses) to reach a logically certain conclusion. Furthermore, predictions may be developed in relation to *theoretical (or conceptual) definition* or *operational definition*. Theoretical definition contains built-in theories and inductive or deductive consequences related to the theories being presented as products of the research. It involves the description of a concept by relating it to other concepts. Operational definition defines the variables and how they will be evaluated and assessed in the study. Besides, the relationship between both types of definition is such that an operational definition is usually dedicated to modeling a theoretical definition in relation to empirical experience.
- *Gathering of data*: This involves collecting and measuring information on variables of interest, according to established methods that enable the answering of research questions, the testing of hypotheses, and the evaluation of results.
- *Analysis and interpretation of data*: This involves decomposing the individual pieces of data for the purpose of drawing conclusions about them. This may be reported/represented through tables, figures, pictures or words.
- *Testing of hypothesis*: The hypothesis is tested with the collected data. The hypothesis is considered true or false based on the analysis of the test result. If the hypothesis is false, it could be revised and tried again or lead to redefining the subject. This indicates the iterative nature of the scientific method.
- *Communicating research findings*: This involves the documentation, reporting, peer review and publishing of the research findings at the end of the research.

4.3 The research content of this PhD project

4.3.1 Application of the scientific methodology to this PhD project

The scientific method as applied to individual research articles is described in the following:

- *Observation and formulation of question*: I established a description of state-of-the-art research on the topic of major accident risk and maintenance. The amount of literature directly related to this topic was limited and a wide search was performed, to ensure that related literature that also may be of

interest were identified. The literature reviewed were related to system reliability, maintenance management, risk analysis, human and organizational factors, systems theories, major accident perspectives and major accident investigation reports. Meanwhile, some research gaps were identified, leading to the formulation of research questions.

- *Hypothesis, predictions and gathering/analysis of data*: There was no formal formulation of hypotheses, but the research questions had the same tendency or direction as would formal hypotheses. In other words, the objectives of the research questions were closer to hypotheses. Similar to hypotheses, research questions are bound to lead to answers by reasoning and this can be tested for being realistic or not. This PhD research work built on the literature reviews, applying the principles of theoretical/operational definitions in relation to logical reasoning and this brought about significant innovation and/or creativity as presented in the following.

  – Classification schemes for maintenance influence on major accidents were developed based on literature review, systematic analysis of accident reports and of the problem area using different perspectives (e.g. maintenance management perspective, accident process perspective and work performance perspective). Both direct influence (e.g. through maintenance correcting errors and ensuring reliability or through maintenance errors inducing errors in the system) and indirect influence (e.g. through inadequate maintenance planning, inadequate procedures for performing maintenance, inadequate training of maintenance personnel) were considered and included in the classification scheme.
  – The analysis of accident reports integrated with the already developed classification scheme also provided information about the extent of the problem (i.e. to what degree maintenance has been a cause of major accidents) and the key mechanisms (i.e. the most important factors). Data was collected from the accident investigation reports, broken down finely and interpreted. According to the aforementioned description of scientific data collection methods, the method here conforms to statistical sampling.
  – The relationship between key maintenance factors (i.e. the independent variables) and the major accident risk they influence (i.e. the dependent variable) was analyzed. This led to the development of individual risk models (from the individual maintenance factors) which served as basis for the overall maintenance optimization model for major accident risk reduction. As far as possible, the final model was also applied to a case to test its suitability. It was also compared with existing models to show its novel contribution.
  – A combined robustness and resilience framework for maintenance in association with other key departments was established. This was intended to improve the ability of an organization to prevent or survive major accidents. It was realized through a thorough analysis of existing organi-

zational accidents perspectives and theories of maintenance management and departmental interfaces within the process industries.

- *Testing of hypothesis*: Since there was no formal formulation of hypothesis in this PhD project (as mentioned earlier), there was no basis for testing any hypothesis. Yet, there was the burden of testing that the research questions were answered correctly and that the research objectives were fulfilled. To this end, a selection of accidents from various sources were used to test the suitability of the classification schemes. This led to extensions of the original classification schemes. Based on the revised classification schemes, a better insight into the influence of maintenance on major accident causation was presented. Peer-review comments from editors and reviewers of internationally reputed journals also served as part of the test mechanism.
- *Communicating research findings*: The research was reported in the form of original articles and published in international publication channels such as journals and conferences.

An overview of the research attributes of this thesis is presented in the following, in relation to quantifiability of data, degree of practicability, main perspective, data collection method and methodological tradition.

There is a mixture of qualitative and quantitative characteristics obviously due to the nature of what is required in the PhD project: (i) a research associated with a collection of scientific opinions (i.e. qualitative, as shown in articles 1, 2, 4, 5 and 6) and (ii) a research associated with a collection of facts and figures (i.e. quantitative, as shown in articles 3 and 4). Article 4 may be seen as being semiquantitative, since it is made up of both original qualitative and quantitative parts, whereby the former served as a basis for the latter.

The research is entirely applied since all the articles have the potential for addressing immediate practical needs. The articles (1, 2 and 5) on description and/or classification of maintenance-related causes of major accidents are applied, since the prevention of an effect is based on the identification of the causes of the effect. The article on statistical analysis (article 3) is applied, since the results can have immediate impact on decision-making as regards the prevention of maintenance-related major accidents. The articles on maintenance optimization (article 4) and maintenance robustness/resilience (article 6) are also applied, since they can also be used readily to reduce the major accident risk.

Some aspects of the research are both theoretical and empirical (i.e articles 1, 2, 3 and 4) since they combined major accident theories with data from accident investigation reports and other sources. Articles 5 and 6 were theoretical. The theoretical research perspective involved organizing and documenting phenomena in the form of models, e.g., gathering and structuring information about how maintenance has influenced major accidents and precursor events and subsequently developing new models to describe these phenomena. It also involved the extension of previous theoretical or applied type of research in a given disci-

pline or sub-discipline, e.g. developing new models for optimizing maintenance intervals with respect to major accident risk. Methods for optimization with respect to cost are well known, where safety is kept as a constraint. However, optimization with respect to risk only is not a topic that has been studied much earlier. In addition, the theory of robustness and resilience were extended to maintenance in relation to improving these qualities in a process industry organization as a whole. The empirical research perspective involved the statistical analysis of data collected from the U.S. Chemical Safety Board and the Bureau for Analysis of Industrial Risks and Pollution in France, culminating in the interpretation of the statistical results. This includes the trend of maintenance related major accidents in the process industries in addition to statistics on the degree and distribution of the causes of the major accidents. The Work and Accident Process (WAP) classification scheme developed in this PhD project was applied to the data which covered the U.S. and Europe geographically.

The entire research employed literature review for information collection. This involved the collection of information from theories related to system reliability, maintenance management, risk analysis, human and organizational factors, systems theories, major accident perspectives and from major accident investigation reports. Besides, statistical sampling was also applied as a data gathering method when accident data were needed in relation to articles 1, 2 and 3.

Furthermore, the methodological tradition in this PhD project is related to systems theory due to the systematic and systemic characteristics of the research. Some examples are presented as follows: System thinking (e.g. this encompasses viewing maintenance-related factors as part of the overall system, maintenance-related major accident risk, and the process of understanding how the factors, which may be regarded as systems themselves, influence one another within the whole. This is akin to smaller problems working together to produce a bigger problem. System thinking example also include the process of understanding how relevant theories, major accident information sources and prior knowledge can work together to solve the maintenance-related major accident problem), system decomposition (e.g. breaking down data from accident theories and reports and analyzing each separately for improved understanding), system aggregation (e.g. putting the analyzed data pieces back into a whole), systems integration (e.g. using logical reasoning to integrate knowledge from accident theories/reports with prior knowledge in order to realize new solution-oriented frameworks and methods), verification (e.g. confirming that the research was carried out in accordance with the requirements of the scientific method, by testing finished work with statistical samples from accident databases and subjecting same to universal criticism) and validation (e.g. applying the new knowledge to more realistic situations to prove that it truly contributes significantly to the advancement of the body of knowledge). The systemic nature is indicated by the fact that the failure to correctly analyze the factors that influence the maintenance-related major accident risk (seen as parts

of the system) will make prevention of major accidents (seen as a system) difficult to realize. This relationship is depicted in the bigger picture of the PhD project as shown in Fig. 4.1.

4.3.2 The bigger picture of the entire PhD research process

As regards the bigger picture (See Fig. 4.1), it can be seen that basic risk management principles were covered in the compilation of the various articles that comprise this PhD project. Fig. 4.1 shows a systematic transition from one "project subsystem" to another. Besides, more insight was given into the principles in relation to the maintenance-related major accident risk. This is summarized in the following.

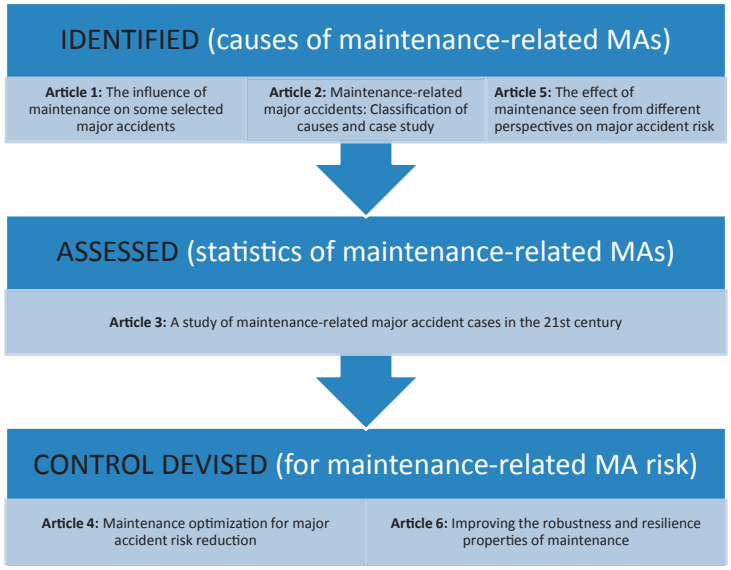


Fig. 4.1 Classification of research findings

- IDENTIFY: "*Why* maintenance-related major accidents happen" were uncovered in articles 1, 2 and 5.

- ASSESS: "*What* proportion of major accidents is linkable to maintenance and *where* the various distributions are most concentrated" were revealed in article 3.
- CONTROL: "*How* to control the risk of maintenance-related major accidents" was offered suggestions in articles 4 and 6.

4.3.3 The detailed picture of the entire PhD research process

The basis for the detailed picture (See Fig. 4.2), which shows transitions between individual research articles (i.e. parts of the project subsystems), was set by the bigger picture. The former shows how the individual articles influence each other for the purpose of realizing the overarching objective which is to prevent maintenance-related major accidents (i.e. the end of the bigger picture). This is described with respect to the relationship between the appended papers in the following.

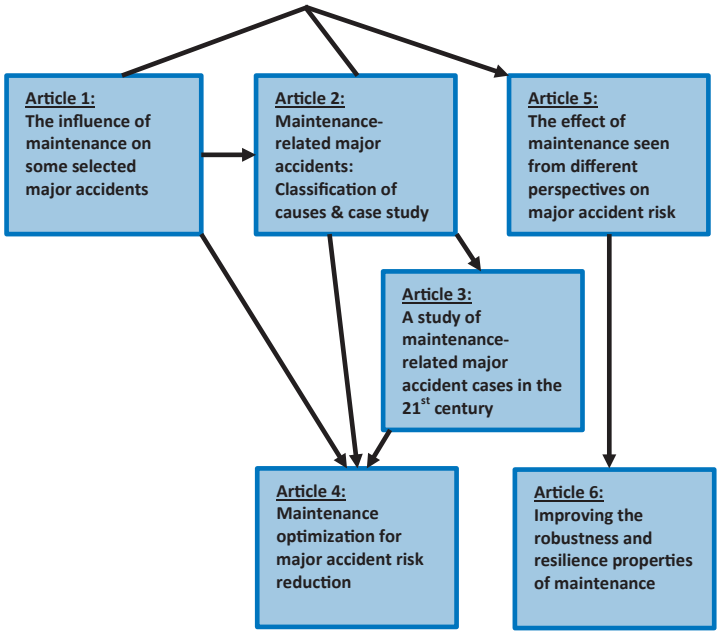


Fig. 4.2 Relationship between the appended papers

The research process for Article 1 built on a review of literature related to the management of major accident risk in the process industry, theories of the causal relationship between maintenance and major accidents and accident investigation reports from the European Agency for Safety and Health at Work (EU-OSHA), the U.S. Chemical Safety Board and Failure Knowledge Database in Japan. The research resulted in the development of causal classification schemes in terms of the accident process and the maintenance management cycle. The main purpose of Article 1 was to develop a classification scheme, apply it on a few accidents to see whether it works and then adjust/finalize it.

The need to contribute exhaustively to the same theme as in Article 1 justified the extension of Article 1 to Article 2. The accident process perspective features in both articles. However, Article 2 combined this with the maintenance work process perspective, unlike Article 1 which combined it with the maintenance management cycle perspective. The maintenance management cycle perspective is related to the Plan-Do-Check-Act cycle of the traditional management system (i.e. a bigger picture), whereas the maintenance work process perspective shows a more elaborate technical and operational scope (i.e. a detailed picture). The research process for Article 2 built on theories related to Article 1 and more theories of the causal relationship between maintenance and major accidents. The first task was to establish a suitable classification scheme that could form a basis for analyzing the influence of maintenance on historical accidents. This would enable identification of where improvement is most needed. The Work and Accident Process (WAP) scheme was developed for this purpose. It was tested with sample cases from the U.S. Chemical Safety Board database and found suitable for all the accident cases selected from a variety of process industries.

To assess the current status (based on empirical evidence) of the extent of maintenance influence on major accidents, Article 3 applied the WAP scheme (developed in Article 2) on a much larger number of major accidents and revealed novel facts in relation to the maintenance influence over a decade. This includes the identification of the most important causes of major accidents related to maintenance.

The findings from Article 3 justified further research aimed at developing Article 4, which is about devising a means of reducing the maintenance-related major accident risk perceived in Article 3. Article 4 focused on how to optimize the frequency of maintenance in order to minimize the major accident risk associated with it. It built on theories related to maintenance optimization and the accident process perspective of the classification schemes developed in Articles 1 and 2.

Article 5, which is about the influence of maintenance based on various existing organizational accident perspectives, was triggered by the observation of organizational factors among technical factors in all the major accident investigation reports used in Articles 1 and 2. Therefore, it was important to look more

into the theories of the different organizational accident perspectives in order to gain as much knowledge as possible.

Article 6, which is dedicated to the 4th research question - How can maintenance contribute to the robustness and resilience of organizations?, was naturally influenced by Article 5. Robustness is about the ability of organizations to resist or counteract accidental events, whereas resilience is about organizations being able to adapt to or recover from accidental events. Hence, the results of Article 5, being about how maintenance can influence the prevention/causation of organizational accidents, was of significant relevance to Article 6. The research process for Article 6 built on inputs from Article 5 and on theories of robustness and resilience, industrial organization and maintenance work process.

The development of all the articles was integrated with critical thinking and creativity. The elements of critical thinking as defined by The National Council for Excellence in Critical Thinking (NCECT) was applied in the development of all the articles: i.e., "the intellectually disciplined process of actively and skillfully conceptualizing, applying, analyzing, synthesizing, and/or evaluating information gathered from, or generated by, observation, experience, reflection, reasoning, or communication, as a guide to belief and action. In its exemplary form, it is based on universal intellectual values that transcend subject matter divisions: clarity, accuracy, precision, consistency, relevance, sound evidence, good reasons, depth, breadth, and fairness. . . incorporated in a family of interwoven modes of thinking, among them: scientific thinking, mathematical thinking, historical thinking, anthropological thinking, economic thinking, moral thinking, and philosophical thinking" [94].

Overall, the first author conceptualized and planned all the articles with the supervisor/co-author. As the first author of all the articles, I conceived the ideas for the research, carried out information analysis, developed and submitted the abstracts, then did the structuring and writing of the first version of the articles. I was also responsible for further iterations following criticisms from myself, my supervisor/co-author and the reviewers. The reasoning was formal, logical and traceable. Furthermore, uncertainties surrounding the findings, together with appropriate generalizations, were defined, e.g. the validity of the statistical findings being constrained by the uncertainty associated with the assumption that future failures will occur at the current rate which was established based on historical experience. All the articles were eventually subjected to international peer-review.

Chapter 5
Main results

5.1 Main results

The main results of this PhD project are originally presented in six articles. Five of the articles are published with one under review. The articles were aimed at providing answers to the research questions posed in Section 3.1 and realizing the research objectives mentioned in Section 3.2.

In this chapter, a summary of the main results is provided by matching the research questions and objectives with the corresponding contributions that represents results from an article. An overview of the distribution of the results from the articles in relation to the research questions and objectives is shown in Table 5.1.

Table 5.1 Overview of distribution of results

	Question 1	**Question 2**	**Question 3**	**Question 4**
Objective 1	Articles 1, 2, 5			
Objective 2		Article 3		
Objective 3			Article 4	Article 6

5.1.1 "How does maintenance influence major accident risk?" (question 1) - "The realization of a well-structured framework and expanded/modified knowledge about the causal relationship between maintenance and major accident." (objective 1)

This has been addressed in Articles 1 [69], 2 [68] and 5 [67].

5.1.1.1 Contributions from Article 1 [69]

The aforementioned question was answered and the research objective fulfilled from the perspectives of both maintenance management and the accident process. By combining the perspectives, a simple classification scheme was realized. This was used to reanalyze some selected maintenance-related major accidents, giving new insights into their causation. The accidents were also used to test the scheme. The main intention in article 1 was to develop a classification scheme, demonstrate it with few accidents to see whether it is applicable and then modify/conclude it. This turned out successful on all the accidents considered from different sources in different countries (CSB in USA, EU-OSHA in Europe and FKD in Japan). The accident process perspective is described as shown in Table 5.2, whereas the maintenance management perspective is described as shown in Table 5.3.

Table 5.2 Factors based on the accident process perspective

Factors	Definition
Lack of barrier maintenance	Lack of barrier maintenance which allows barriers to be breached by failure mechanisms (e.g. lack of maintenance leading to corrosion).
Barrier maintenance error	Wrong maintenance directly breaching safety barriers (e.g. wrong calibration of level transmitter).
New hazard	Maintenance introduces new hazards, which may be triggered by events (e.g. hot tapping).
Initiating event	Maintenance being an initiating event for an accident scenario (e.g. loss of containment due to a wrong valve being operated).

5.1.1.2 Contributions from Article 2 [68]

The aforementioned question was answered and the objective fulfilled from the perspectives of both the maintenance work process and the accident process, the combination of which is called the Work and Accident Process (WAP) classification scheme. The accident process part was divided, like in article 1 [69], into both active failures and latent failures, but in this case there was further refinement to the latent failures categorization. The classification related to the active failures is identical to the one developed in article 1 [69], whereas the classification related to the latent failures is described as shown in Table 5.4. The latent failure classification is based on Reason's [87] view of its being characterized

Table 5.3 Factors based on the maintenance management perspective

Factors	Definition
Lack of maintainability	Lack of the ability to retain an item or restore it to a state in which it can perform its required functions, e.g. lack of testability/accessibility.
Deficient fault diagnosis	Deficiency in fault detection, fault localization and identification of causes, e.g. insufficient test coverage [19].
Deficient planning	Deficiency in the organization and documentation of a set of maintenance tasks that include the activities, procedures, resources and time scale required to execute maintenance, e.g. communication gap between maintenance and production units [19].
Deficient scheduling	Deficiency in predetermined detailing of when a specific maintenance task should be executed, e.g. too late timing [19].
Deficient execution	Deficiency in the hands-on actions taken to retain an item or restore it to a state in which it can perform its required functions, e.g. wrong performance of a correct task.
Deficient checking	Deficiency in supervision, confirmation or performance evaluation, e.g. inadequacy of checklists.

by management failure and on similar information obtained from accident investigation reports [12].

The work process classification is described as shown in Table 5.5. This focuses more on operational elements in addition to management elements unlike the corresponding perspective of the scheme in article 1 [69].

In addition, some other classification schemes, e.g. Threat and Error Management (TEM) and Man-Technology-Organization (MTO) framework were adapted to maintenance-related major accidents from other industrial (e.g. aviation) or application areas. This increased the range/variety of classification schemes that may be useful in certain maintenance-related situations. However, they were considered less suitable for this PhD project because they did not treat major accident hazards explicitly or did not describe the accident process. The Work and Accident Process (WAP) scheme, which is a combination of the work process and accident process schemes was recommended. This is because the accident process scheme would provide a better insight into the underlying and contributing causes in relation to the barriers dedicated to preventing major accidents, while the work process scheme identifies the starting, intermediate and terminal phases of the accidents in relation to the maintenance operational

Table 5.4 Latent failures of the accident process

Latent Failures	Definitions
Deficient regulatory oversight	Inadequacies of regulatory bodies in directing, guiding, inspecting, auditing and sanctioning companies under their watch.
Deficient risk assessment	Inadequacies in identifying hazards, analyzing and evaluating associated risks.
Deficient implementation of requirements	This refers to inadequacies in adopting external requirements.
Deficient Management of Change (MOC)	Inadequacies in handling changes, especially non-routine permanent and temporary changes in physical systems, organizations, operations and the operational environment.
Deficient documentation	Inadequacies in safety-related documentation
Deficient design, organization or resource management	Inadequacies in design, layout, coordination, communication, safety culture and management of human, material and financial resources etc.
Unbalanced safety and production goals	This is the disproportionate allocation of resources to production at the expense of safety.
Deficient monitoring of performance	This covers inadequacies in measuring performance and detecting trends.
Deficient audit	Inadequacies in checking the conformity of the status of personnel, organization, systems and processes to established requirements.
Deficient learning	Inadequacies in learning from safety reviews, safety audit reports, industry news, etc.

process. This would also contribute to a better understanding of the underlying and contributing causes, thus promoting prevention efforts.

The main intention in Article 2 was to develop a causal classification scheme, test it with few maintenance-related major accidents to see if it is implementable and then revise/finish it. The focus covered the identification of the underlying and contributing maintenance-related causes of major accidents, and by implication, gave more insight into how maintenance influences the major accident risk. The rigorous iterative verification process and the harmonization of the independent analysis of both authors resulted in the fine and comprehensive categorization of maintenance-related major accidents. Meanwhile, the test also provided an opportunity to help improve the scheme. The resulting Work and Accident Process (WAP) scheme is based on the combination of the accident process and the maintenance work process classification schemes developed in-

Table 5.5 Factors based on the work process

Factors	Definition
Deficient planning, scheduling and failure diagnosis	Planning is the organization and documentation of a set of tasks that include the activities, procedures, resources and time scale required to carry out maintenance, whereas scheduling is the predetermined detailing of when a specific maintenance task should be carried out and by whom [19]. Failure diagnosis refers to actions taken for fault detection, fault localization and identification of causes [19].
Deficient mobilization/shutdown	Mobilization is the supply, movement and deployment of resources. Shutdown is outage implemented in advance for maintenance, or other purposes [19].
Deficient preparation for maintenance work	Preparation refers to provision of required information and applying the requirements (e.g. Permit to work-PTW, Lockout/Tagout-LOTO procedure, hazardous material evacuation, securing of isolation points, etc.) that will enable maintenance to be performed effectively and safely.
Deficient performance of the maintenance work	Performance implies hands-on actions taken to retain an item in or restore it to a state in which it can perform its required functions.
Deficient startup	Startup is a state in which a maintained item is being made "live," i.e. the item is being activated or actuated.
Deficient normal operation	Normal operation is a state in which an item is in service.

dividually earlier. WAP was used to reanalyze a larger number of accidents, giving more insights into their occurrence.

5.1.1.3 Contributions from Article 5 [67]

The aforementioned question was answered and the objective fulfilled on the basis of six existing organizational accident perspectives. The perspectives have not all been thoroughly investigated before with the relationship between maintenance and major accidents in mind. Hence, it was interesting to look at the perspectives from a maintenance point of view to see what new knowledge they might offer or whether they could support some prior knowledge related to the subject of this PhD project. The results from the investigation are presented in Table 5.6.

Table 5.6 The effects of maintenance seen from from different major accident perspectives

Perspective	Implication	Maintenance effects (Results)
Energy-barrier	Major accidents result from the failure of the barrier between a hazard and an asset.	Maintenance is seen as a key means of retaining major-accident barriers in or restoring them to a functional state.
Normal accident	Major accidents are inevitable in high-risk technologies due to their interactive complexities and tight couplings.	Maintenance is seen only as a safeguard for the individual parts of high-risk systems, but not ensuring the safety of the whole system. Maintenance is also seen as adding complexity and tight couplings.
High reliability organization (HRO)	Major accidents are preventable through diligence in failure analysis, learning, balancing production and safety goals, decentralization and centralization of authorities and redundancy.	HRO organizations are proactive in failure management and this should also extend to ensuring good maintenance, to avoid technical failures.
Man-made disaster	Major accidents result from lack of information flow.	The technical and maintenance status of systems is key information that should flow to the right persons.
Conflicting objectives	Major accidents result from organizational objectives clashing with each other, leading to drift towards accidents.	Maintenance costs are under pressure to be reduced.
Resilience engineering	Major accidents are due to a breakdown in the adaptive capacity necessary to cope with the real world of complexity.	Being a synthesis of ideas on barriers, complexity, conflicting goals and HRO, how maintenance is viewed will tend to be coincidental to these.

The various perspectives gave us different views, and by implication, different insight into how maintenance influences major accidents. The energy-barrier perspective clearly emphasizes the role of maintenance as a key means of ensuring the availability and reliability of barriers to prevent accidents, whereas other perspectives highlight the importance of maintenance to maintain organizational balance in relation to other elements within the industrial organization as shown in Table 5.6. Given that there is merit in all the perspectives, it ap-

pears reasonable to give attention to all, thus consolidating strategies for major accident prevention as demonstrated in Article 6.

5.1.2 "To what extent has maintenance been a cause of major accidents?" (question 2) - "Enhanced demonstration of the applicability of the knowledge derived from the causal relationship between maintenance and major accidents" (objective 2)

This has been addressed in Article 3 [70]. A much larger number of major accident cases from the US and Europe between 2000 and 2011 were studied. The Work and Accident Process (WAP) scheme developed in Article 2 was applied/tested further on 183 major accident cases. This resulted in the statistics presented in Table 5.7.

Table 5.7 Statistics of maintenance-related major accidents

Year	USA & Europe	Moving Average
2000	7	
2001	6	
2002	9	7.3
2003	12	9.0
2004	9	10.0
2005	8	9.7
2006	4	7.0
2007	4	5.3
2008	8	5.3
2009	4	5.3
2010	5	5.7
2011	4	4.3
Total	**80**	
Sample size	**183**	
Percentage	**44%**	

Table 5.7 indicates that, overall, maintenance is a causal factor in 44% of major accidents in the process industries, and the proportion per year has decreased over the period.

Further results relevant to research objective 2 are presented as shown in Fig. 5.1, Fig. 5.2, Fig. 5.3, Fig. 5.4, Fig. 5.5 and Fig. 5.6. These consist of the most common causes associated with maintenance-related major accidents in the process industries. The most frequent cause in terms of the active accident process is "lack of barrier maintenance" (42% of 96 active causal occurrences - See Fig. 5.1) and (50% of 80 maintenance-related accidents - See Fig. 5.2). The most frequent cause in terms of the latent accident process is "deficient design, organization and resource management" (25% of 276 latent causal occurrences - See Fig. 5.3) and (85% of 80 maintenance-related accidents - See Fig. 5.4). This may be due to the fact some related factors which are individually significant were merged for simplicity sake. In addition, the most frequent cause in terms of the work process is "deficient planning/scheduling/fault diagnosis" (36% of 150 work-process causal occurrences - See Fig. 5.5) and (69% of 80 maintenance-related accidents - See Fig. 5.6). This may be due to the fact that planning can influence all the other phases of the work process without exception.

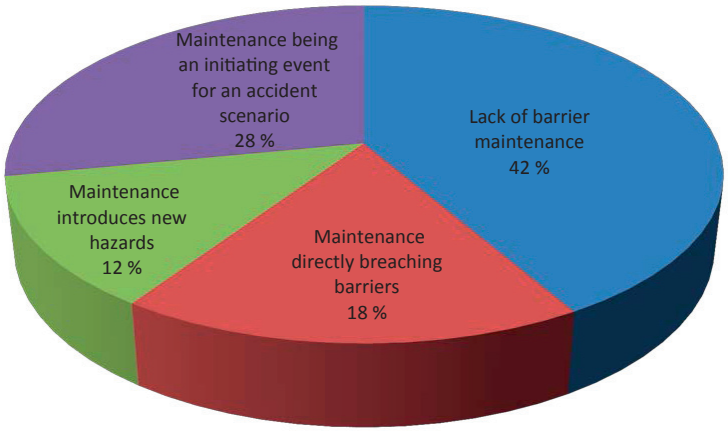


Fig. 5.1 Percentages of different categories of active failures in 96 active causal occurrences

More results are shown in Table 5.8, Table 5.9 and Table 5.10. It can also be seen from Table 5.8 that the most frequent combination of active failures is "maintenance introduces new hazards - maintenance being an initiating event" (42% of all the combinations). This combination is likely in safety-critical maintenance work in plants with significant amounts of hazardous substances. The new hazards are those generated by maintenance e.g. through the application of new, unvalidated procedures, processes, conditions and equipment or existing undervalidated ones. These may become triggered by events (e.g. certain main-

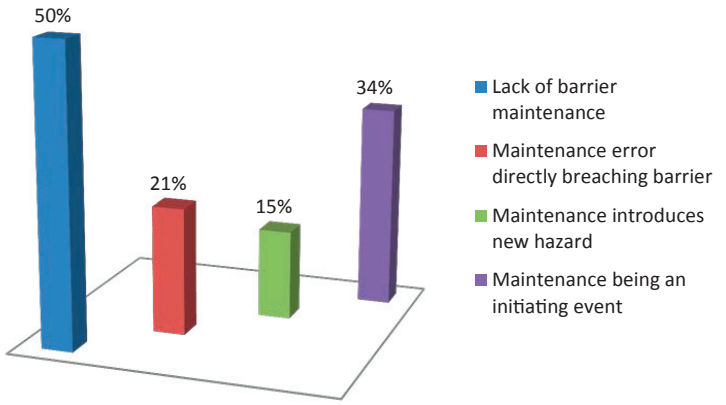


Fig. 5.2 Percentages of different categories of active failures in 80 maintenance-related accidents

Table 5.8 Combinations of active failures (number of occurrences)

	Maintenance error directly breaching barriers	**Maintenance induces new hazards**	**Maintenance being an initiating event**
Lack of barrier maintenance	6	2	3
Maintenance introduces new hazards			8

tenance interventions) that favor their development into an accident. Table 5.9 also shows that the most frequent combination of latent failures is "deficient risk assessment - deficient design, organization and resource management" (36% of all the combinations). These two sets of elements are such that they can influence each other: deficient risk assessment may influence deficient design and on the other hand deficient organization and resource management may influence risk assessment. In addition, Table 5.10 reveals that the most frequent combination of work-process related failures is "deficient planning/scheduling/fault diagnosis - deficient normal operation" (33% of all the combinations).

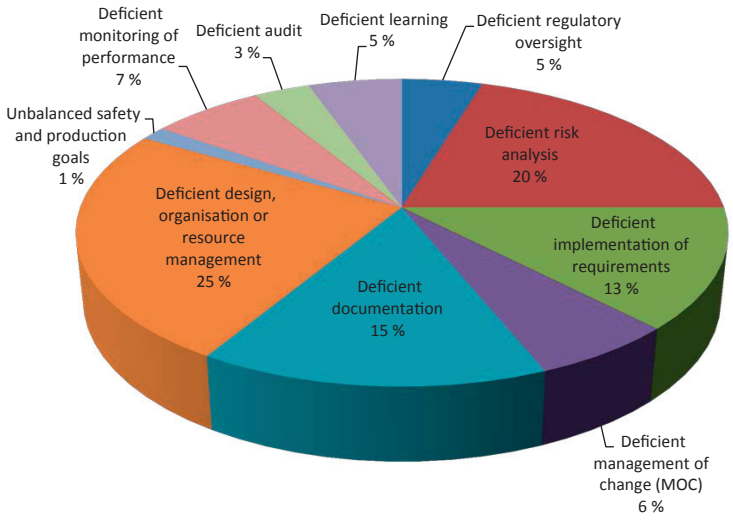


Fig. 5.3 Percentages of different categories of latent failures in 276 latent causal occurrences

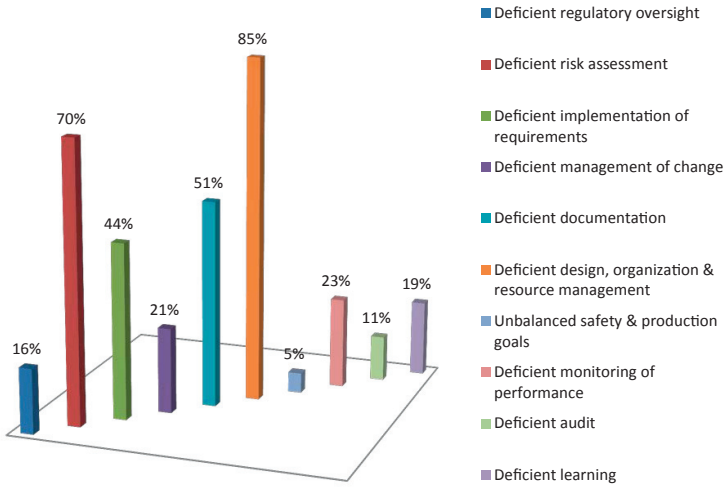


Fig. 5.4 Percentages of different categories of latent failures in 80 maintenance-related accidents

Table 5.9 Combinations of latent failures (number of occurrences)

	Deficient documentation	**Deficient design, organisation or resource management**	**Deficient monitoring of performance**
Deficient risk assessment	28	48	
Deficient implementation of requirements		30	5
Deficient management of change (MOC)	9		
Deficient monitoring of performance		14	

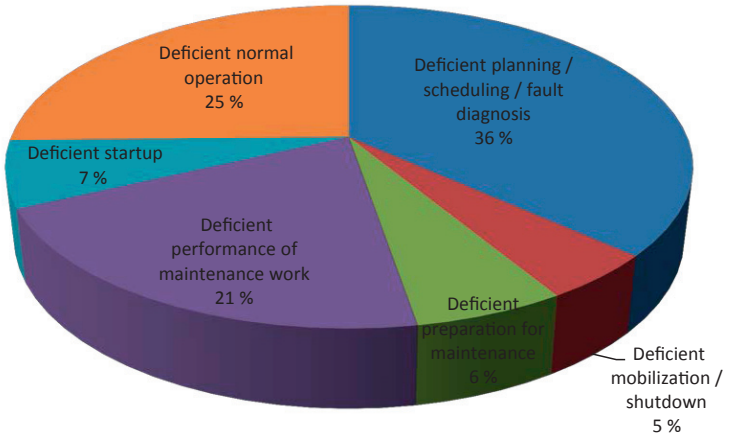


Fig. 5.5 Percentages of different categories of work-process failures in 150 work-process causal occurrences

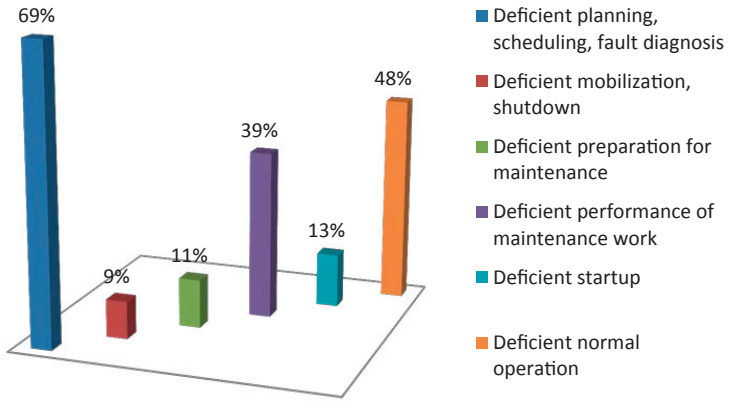


Fig. 5.6 Percentages of different categories of work-process failures in 80 maintenance-related accidents

Table 5.10 Combinations of work-process failures (number of occurrences)

	Deficient mobilization/ shutdown	**Deficient preparation for maintenance**	**Deficient performance of maintenance**	**Deficient startup**	**Deficient normal operation**
Deficient planning/ scheduling/fault diagnosis	4	4	20	7	27
Deficient mobilization/ shutdown		1	1		
Deficient preparation for maintenance			4		1
Deficient performance of maintenance work				2	10

5.1.3 *"How should maintenance be optimized in relation to the major accident risk?" (question 3) - "The proposal of novel risk reduction strategies for maintenance-related major accidents" (objective 3)*

This has been addressed in Article 4 [71] by establishing a basis for optimizing preventive maintenance interval with respect to risk. Optimizing the maintenance interval implies optimizing the exposure of personnel to major hazards, thus reducing the major accident risk. Prior to the development of the quantitative part of the optimization, the personnel risk associated with maintenance was systematically analyzed based on the effects of increasing and decreasing maintenance interval. The risk contributions were defined in terms of the potential loss of life (PLL) and this has been illustrated in the event tree shown in Fig. 5.7.

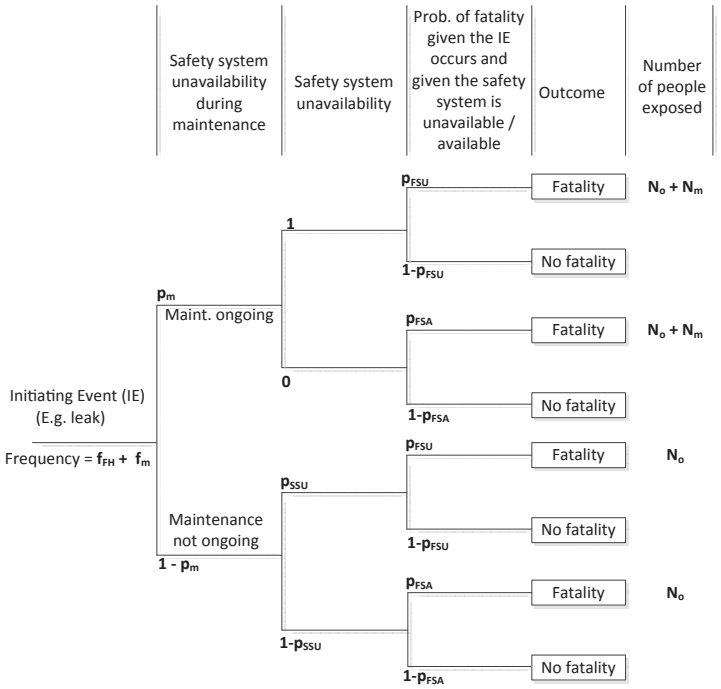


Fig. 5.7 An event tree analysis in relation to personnel risk in the process industry

This event tree is much simplified compared to typical event trees applied in QRAs (Quantitative Risk Assessments) for process plants. However, it has been simplified to enable illustration of the effects of maintenance, while all other effects are assumed to be compiled into the initiating event frequency and the probabilities applied in the event tree. This can easily be done if a valid QRA is available.

The optimization equation derived from the event tree, is given by:

$$\begin{aligned} PLL = {} & (f_{FH} + f_m) * p_m * p_{FSU} * (N_m + N_o) \\ & + (f_{FH} + f_m) * (1 - p_m) * p_{SSU} * p_{FSU} * N_o \\ & + (f_{FH} + f_m) * (1 - p_m) * (1 - p_{SSU}) * p_{FSA} * N_o \end{aligned} \quad (5.1)$$

Where the following notations and meanings are used,

- f_{FH} - frequency of initiating event (can be determined from QRA for plant).
- f_m - additional contribution to frequency due to maintenance. This will be dependent on the maintenance interval. Assuming that there is a constant contribution (f_c) per maintenance interval, this can be expressed as f_c/τ.
- p_m - probability that maintenance is ongoing. This is assumed to be equal to the proportion of time when maintenance is ongoing. This will be dependent on how often maintenance is performed (maintenance interval) and the duration of the maintenance period and can be calculated as d/τ. This is the only time when both maintenance and operations personnel are present.
- p_{FSU} - probability of fatality when the safety system is unavailable (can be determined from QRA for the plant).
- p_{FSA} - probability of fatality when the safety system is available (can be determined from QRA for the plant).
- N_m - number of maintenance personnel required for the work.
- N_o - number of operations personnel normally present.
- p_{SSU} - probability of safety system being unavailable.

The PLL equation assumes that optimization takes place with regard to single components only (or that the entire system is considered as a whole). This equation is valid for one initiating event. To optimize with respect to total risk would imply adding together the effects over all initiating events. Only risk contributions that are affected by the maintenance of the safety system being considered need to be included in the optimization. This approach was adapted from the nuclear industry, where maintenance optimization based on risk to equipment (e.g. the core damage frequency of a nuclear power plant) was performed by Vaurio [111] for a single component or a train of components in series, on standby or in normal operation. This involved the definition of a risk function, R(τ), as equal to the product of the frequency of initiating event (f) and the product of unavailability states (basic events) of safety systems, such that,

$$R(\tau) = f * (\rho + \frac{d}{\tau} + \frac{\lambda\tau}{2}) \tag{5.2}$$

Where the terms in the equation are defined as [111, 38]:

- f - the frequency of initiating event
- ρ - the safety system unavailability consisting of various contributions, including the probability of introducing new failures during maintenance.
- τ - the maintenance interval.
- d - the maintenance duration.
- λ - the failure rate of the safety system.
- d/τ - the safety system unavailability owing to maintenance being carried out at intervals.
- $\lambda\tau/2$ - the average unavailability of the safety system due to failure between maintenance.
- $\rho + d/\tau + \lambda\tau/2$ - the total average unavailability of the safety system.

Equation 5.2 implies that if we set dR/dτ to zero, the optimal maintenance interval, τ^*, can then be expressed as:

$$\tau^* = \sqrt{\frac{2d}{\lambda}} \tag{5.3}$$

Furthermore, p_{SSU} can be seen also as the combination of all factors that influence the safety system unavailability. In relation to this, we can apply the formula from the nuclear industry given by Vaurio (i.e. Equation 5.2), and assume that the average unavailability due to failure of the system is $\lambda\tau/2$ and the constant contribution from maintenance errors is ρ. If maintenance is ongoing, p_{SSU} is set to 1, in accordance with the assumption in Article 4 [71].

Hence, Equation 5.1 may be rewritten as:

$$\begin{aligned} R(\tau) = {} & (f_{FH} + \frac{f_c}{\tau}) * \frac{d}{\tau} * p_{FSU} * (N_m + N_o) \\ & + (f_{FH} + \frac{f_c}{\tau}) * (1 - \frac{d}{\tau}) * (\rho + \frac{\lambda\tau}{2}) * p_{fsu} * N_o \\ & + (f_{FH} + \frac{f_c}{\tau}) * (1 - \frac{d}{\tau}) * (1 - (\rho + \frac{\lambda\tau}{2})) * p_{FSA} * N_o \end{aligned} \tag{5.4}$$

By setting dR/dτ to zero, the optimal maintenance interval, τ^*, can be obtained. The general solution is however quite complex and is not described here. Use of mathematical tools such as MAPLE and MATLAB is recommended.

Using a graphical solution, we then arrive at an optimal maintenance interval of about 3050 hours given the following parameters: $f_{FH} = 1 \bullet 10^{-3}$ per year, $f_m = 1 \bullet 10^{-6}$ per maintenance operation, d = 6 hours, $p_{FSU} = 0.001$, $p_{FSA} = 0.0008$, $N_m = 2$ persons, $N_o = 10$ persons, $\rho = 1 \bullet 10^{-4}$ and $\lambda = 1 \bullet 10^{-5}$ per hour.

Comparatively, if we apply Equation 5.3, using λ and d from above, we get 1100 hours, i.e. a considerably shorter interval. This difference in maintenance interval is to be expected, since the negative effects on personnel risk are taken into account, tending to increase the intervals. How changes in the various parameters affect the maintenance interval is described in Table 5.11.

In conclusion, we can say that a new approach for risk-based maintenance optimization has been developed for the process industry. This has been adapted from the nuclear industry. In the nuclear industry method proposed by Vaurio [111], an optimization procedure involving a complete risk function was developed and it was suggested that the risk function could be e.g. the core-damage frequency. This is a highly relevant risk measure in the nuclear industry, but not directly applicable in the process industry.

Table 5.11 Effect of changes in parameters on the optimal maintenance interval

Parameter	Effect of changes
f_{FH}	The existing risk level in the plant will affect both operational personnel and maintenance personnel and the effect of this will depend on the balance between the risks for these two groups. However, since the operations personnel normally is most exposed to risk (because they are there the whole time), a high risk level will normally imply that we want a high availability of the safety systems and the maintenance interval is therefore shorter. Reduced frequency will have the opposite effect.
f_m	This is the additional risk introduced by maintenance. Obviously, the higher this value is, the larger the maintenance interval will tend to be. On the other hand, if this is equal to or very close to zero (which may be the case for many maintenance operations), the maintenance interval will approach the interval calculated with Equation 5.3 (i.e. assuming $f_m = 0$ implies a maintenance interval of 1550 hours).
d	The duration of the maintenance operation has two effects: It increases the exposure of maintenance personnel and it increases the unavailability of the safety system. Increased duration will therefore always lead to increased maintenance interval.
p_{FSU} p_{FSA}	These values are the probabilities of fatalities, given that the safety system is unavailable/available respectively. First, it is noted that if these values are the same, no optimal maintenance interval can be found. The reason is that this implies that the safety system has no effect, and optimization with respect to risk is then not possible. In effect, it is therefore the difference between these two values that is important for the maintenance interval. If the difference increases (implying that the difference in risk when the system is unavailable compared to available increases), the maintenance interval will decrease, because it is more attractive to have a working system.
N_m N_o	The number of people exposed, maintenance and operations personnel, will influence the maintenance interval in different ways. First of all, for a given ratio between N_m and N_o (regardless of the actual values), the maintenance interval will remain constant. However, increasing N_o will generally decrease the maintenance interval, whereas increasing N_m will increase the interval. Increasing N_o increases the "everyday" risk (which normally will be the biggest portion of risk), making it beneficial to do maintenance more often. On the other hand, more maintenance people implies more additional people exposed to risk.
ρ	Changing this will have no effect since this is a constant contribution that will not change with the maintenance interval. The risk level will increase/decrease, but the optimal point remains the same.
λ	The failure rate for the safety system obviously influences the maintenance interval. High failure rate implies short maintenance interval and vice versa.

5.1.4 *"How can maintenance contribute to the robustness and resilience of organizations?" (question 4) - "The proposal of novel risk reduction strategies for maintenance-related major accidents" (objective 3)*

The has been addressed in Article 6 [72] by investigating and identifying robustness and resilience properties in the maintenance process and how these could be improved in relation to maintenance interaction with other activities such as production and support. This implies improvement of the robustness and resilience of the industrial organization as a whole. The properties were derived from the organizational accident perspectives described earlier in article 5 and they are presented as shown in Table 5.12.

Table 5.12 Robustness and resilience properties

Properties	**Meanings**	**Perspectives**
Proactivity	Foreseeing what can go wrong and deploying barriers in advance.	Energy-barrier, HRO and resilience engineering
Redundancy	Deploying more than one means to a required function.	Energy-barrier and HRO
Simplicity	Making the design of organizational interactions simple.	Normal accident
Loose couplings	Allowing slacks, variant sequences, alternative means and independent events in organizations.	Normal accident
Learning	Reviewing incidents and near-misses, sharing/updating situation or industry knowledge.	HRO and resilience engineering
Decisiveness	Successfully balancing goals, e.g. production-safety goals.	Conflicting objectives, adaptation and drift
Communication and coordination	Exchanging information and acting on it harmoniously.	Man-made disaster
Emergency response	The quality to readily intervene in accidental events.	Resilience engineering
Management of change	Management of organizational-related, operational and environmental changes.	Resilience engineering

The energy-barrier, normal accident, HRO, man-made disaster and conflicting objectives perspectives indicate various causes of organizational accidents. The negative qualities that best describe these causes are identified and the op-

posite, positive qualities are derived as properties with which such unwanted events can be resisted or counteracted. This provides a basis for establishing robustness, retaining the original stability of the system being protected [2]. The resilience engineering perspective also presents another view about the causes of organizational accidents and the presence of resilience defines the ability to adapt to or recover from accidental events, while stability is realized in a new state. Since this also includes core topics from the other perspectives [15, 89], it is expected that some recommended properties would overlap between robustness and resilience as shown in Table 5.12.

Based on the results from Table 5.12, concrete suggestions were provided in article 6 [72] in relation to the link between the various phases of the maintenance work process, the production and support units of the process industry organization and the operating environment. These suggestions were offered as shown in Table 5.13, Table 5.14 and Table 5.15 for the Maintenance-Production link, the Maintenance-Support link and the Maintenance-Environment link respectively.

Table 5.13 Robustness/resilience improvement suggestions for the Maintenance-Production link

Properties	**Suggestions**
Proactivity	Proactivity to risk management in maintainable production systems. E.g. Joint job safety analysis (JSA) or toolbox meetings prior to inter-departmental work.
Redundancy	Organizational and technical redundancy for safety-critical production systems. E.g. Joint agreement on training and keeping standby personnel who are multi-skilled in both production and maintenance regardless of any existing outsourcing policy.
Simplicity	Simplicity in maintenance planning, procedures and organization in relation to safety-critical production systems. E.g. Simplification of production-maintenance interfaces and elimination of bureaucracies in the network between production-maintenance.
Loose couplings	Looseness of couplings in maintenance organization to tolerate shortcomings in production organization. E.g. Putting joint alternative operational plans in place and being tolerant of delays, errors and failures in mutual interaction.
Learning	A learning culture that promotes safety in maintenance of hazardous production systems. E.g. Joint planning of HSE review meetings, participation in HSE workshops and other related forums.
Decisiveness	Decisiveness in discouraging risky imbalances between maintenance and production. E.g. Joint agreement on guidelines for potential trade-offs that will not create imbalance between business and safety objectives.
Communication and coordination	Communication and coordination between maintenance and production staff in the maintenance work process of safety-critical production systems. E.g. Cooperation on PTW, CMMS, HAZID, safety planning and maintenance/production interface lead.
Emergency response	Emergency preparedness and response to accidental events arising from maintenance-production interactions. E.g. Joint emergency exercises and drills planning/participation and emergency maintenance of deficient process safety equipment.
Management of change	Management of change (MOC) related to alterations in the maintenance-production network. E.g. Joint development of MOC procedure relevant to maintenance-production relations

Table 5.14 Robustness/resilience improvement suggestions for the Maintenance-Support link

Properties	**Suggestions**
Proactivity	Proactivity to management of obsolescence of critical parts. E.g. Anticipating the obsolescence of critical items and hence doing timely upgrade.
Redundancy	Organizational redundancy in relation to suppliers of critical parts. E.g. Keeping redundant suppliers of critical maintenance-related resources on vendors list.
Simplicity	Simplicity of maintenance support systems. E.g. Making maintenance-related cyber-physical systems user-friendly.
Loose couplings	Looseness of couplings in relation to fault tolerance of maintenance support systems. E.g. Procuring a bug-tolerant computerized maintenance management system.
Learning	Learning on critical part verification. E.g. Training maintenance staff to acquire the know-how of verifying critical parts before and after supply.
Decisiveness	Decisiveness in confirming the responsible party for critical part replacement between maintenance and external technical support. E.g. Consulting in-house documentations on after-sales advice/agreement.
Communication and coordination	Communication and coordination for technical support via electronic channels. E.g. Interacting with sales/service engineers to ensure the availability of critical maintenance related resources such as e-PTW and CMMS supplied earlier.
Emergency response	Emergency preparedness in conjunction with the dedicated emergency response department. E.g. Emergency maintenance planning for deficient emergency response equipment.
Management of change	Management of change with respect to alterations in the maintenance-support network. E.g. Development of MOC procedure relevant to maintenance-support relations.

Table 5.15 Robustness/resilience improvement suggestions for the Maintenance-Environment link

Properties	**Suggestions**
Proactivity	Proactivity to management of unsafe environmental conditions arising during maintenance, e.g. through maintenance optimization in relation to dynamic grouping of maintenance activities.
Simplicity	Simplicity in maintenance operations in relation to concurrent activities in neighboring areas. E.g. Postpone maintenance activities such as abrasive blasting in relation to concurrent fueling activity nearby.
Loose couplings	looseness of couplings with respect to decentralizing maintenance for speedy response to hazardous effects from environmental forces.
Learning	Learning on keeping a conducive working environment.
Decisiveness	Decisiveness in adapting maintenance operations to the livelihood of the host community, e.g. through diligent waste management and site reinstatement efforts.
Communication and coordination	Communication and coordination on weather forecast and cultural issues related to the host community.
Emergency response	Emergency maintenance to prevent or mitigate the effects of sudden environmental hazards.
Management of change	Management of change (MOC) procedure relevant to maintenance-related environmental changes.

Besides, the maintenance organization itself can also experience drift, which will affect the process industry organization at large. Drift is “a metaphor for the slow, incremental movement of systems operation toward (and eventually across) the boundaries of their safety envelope” [14, 84]. Some suggestions on how this could be prevented in maintenance were also offered as presented in Table 5.16.

Table 5.16 Suggestions on drift prevention in maintenance

Drift source	Preventive measure
Maintenance postponement to satisfy a time-based customer demand rather than lose the order to competitors	Avoid maintenance postponement of safety-critical elements.
Accumulated errors in maintenance-related decision making, e.g. accumulated errors in critical spare parts management.	Use effective maintenance management tools.
Increase in annual maintenance risk	Optimize maintenance intervals in terms of risk to minimize the major accident risk.

Chapter 6
Discussion and conclusion

Overview

The chapter will feature criticisms, quality assurance, conclusion, expected industrial applications and possibilities for future research in relation to the thesis.

6.1 Criticisms

Various aspects of research within this PhD project are subject to criticisms, e.g. there have been some deviations from the traditional scientific method. There are reasons why certain things appeared as seen. However, it is of utmost importance to ensure that this does not affect the results negatively. This was addressed with some compensating measures.

- *Formulation of hypothesis*: This PhD project deviated from the traditional scientific method by not formulating hypotheses. However, the research questions were oriented towards the same goal as would formal hypotheses. A research question could be e.g. "Why do we experience day and night?" and a corresponding hypothesis could be e.g. "We experience day and night, because the earth rotates on its axis." The former poses a question which needs to be investigated and answered correctly, whereas the latter proposes a solution/answer which needs to be tested.
- *Testing of hypothesis*: Another deviation, in some cases, was not using experiment, case study or statistical sampling for testing of hypotheses. This was not necessary since we did not formulate hypotheses at the beginning. However, since the objectives of the research questions were close to potential hypotheses, we decided to show the fulfillment of the objectives (which were set in relation to the research gaps) by e.g. testing the developed classification schemes for suitability with accident cases from a variety of process

industries. Furthermore, the subjection of the finished research work to peer review both internally and internationally also served for testing.

- *Uncertainty associated with accident report authors*: We had no control over the errors that may have originated from the investigators of the accidents whose reports we used for testing the classification schemes developed in articles 1 and 2. The errors may be associated with the type of method used in the investigation or the type of scheme they applied.
- *Uncertainty associated with accident report users*: We may have misunderstood the accident reports. To limit this as much as possible, we did independent reviews of the accident reports and compared our results.
- *The Work and Accident Process (WAP) classification scheme*: It was shown that the most frequent cause in terms of the latent accident process is "deficient design, organization and resource management" (25% of 276 latent causal occurrences). This may be due to the fact some related factors which are individually significant were merged for simplicity sake. This points to a weakness in the scheme, however it applies only to a subcategory element and does not weaken the basis for the main categorization. Besides, the aforementioned three-in-one element could also be split into three separate elements without affecting the basis for the classification scheme.

6.2 Generic tools for measuring quality of research

The quality of research may be checked by using applicable criteria in the following list [54, 83, 95].

- Originality
  - Theme (off-road, niche, novel combination or unexplored area)
  - Problem (novel challenge)
  - Difficulty (attacking hard challenges)
  - Methods (novel developments, improvements or novel applications)
  - Theory (original and well-supported by hypotheses and theories)
  - Results (new knowledge)
- Solidity
  - Data quality (clear, obvious, large effects, many experiments, sufficient statistics)
  - Methodological quality (sufficient methods; advanced methods)
  - Control (adequate positive and negative control experiments, checking and excluding ambiguities)
  - Information power (well-defined and solid conclusions)
- Informativity

- Clarity (of problem formulation, results and conclusions)
- Objectivity (critical evaluation of own data; balanced evaluation of similar research from other authors, fair credit attribution)
- Knowledgeability (expertise, broad knowledge and insight, relevant and representative reference choice)
- Technical quality (clear, well-organized and informative figures and tables)

6.3 Quality assurance of this PhD project

All the articles have been subjected to international peer review. Besides, the aforementioned criteria for research quality can be recognized in this PhD project as described in the following.

- *Solidity*: The scientific method was applied to the research which is about a problem within the applied sciences.
- *Solidity*: The descriptions of accident data in the investigation reports were detailed enough to permit classification in Articles 1 and 2. They gave sufficient details to enable analysis of causal factors. The variety of sources of data used in Articles 1 and 2, and the reputation of the collectors and custodians of the data boosted our confidence in the different causal factors identified. The accident sources used in Articles 1 and 2 focused broadly in the same direction.
- *Originality, solidity and informativity*: The classification schemes developed in Articles 1 and 2 are comprehensive, complete and finely categorized to address specific industrial challenges, encompassing technical, human and organizational factors. The processes of developing the schemes were rigorous and iterative. They were characterized by independent analysis by both authors, which were compared afterward. This helped in refining and perfecting the schemes, eliminating overlaps and ambiguities.
- *Informativity*: The classification schemes developed in Articles 1 and 2 were also used as a basis for developing other researches - Articles 3 and 4.
- *Informativity*: The relationship established between maintenance and individual major accident perspectives in Article 5, provided a basis for further research which was realized in Article 6.
- *Informativity*: Being objective in self-criticism of one's research in addition to demonstrating a balanced evaluation of the optimization formula of Vaurio [111] which is the most related to the new formula we developed in Article 4.
- *Solidity*: The sufficiency of statistical sampling (183 accidents) collected from identified populations of accidents with respect to the intention in Arti-

cle 3 - to determine the extent of maintenance influence on major accidents quantitatively.
- *Originality*: Improving an existing risk-based, maintenance optimization method with the results of Article 4.
- *Solidity*: The research methods are repeatable and the results are reproducible.
- *Originality*: The confirmation of the results of the articles as new knowledge by international peer review teams.

6.4 Conclusion

This PhD project has provided insights into the maintenance-related causes of major accidents in the process industries, the frequency of occurrence of such accidents and the causes, how to prevent the accidents by strengthening the maintenance organization itself and in relation to collaborating departmental organizations and how to prevent the accidents by minimizing the risk of exposure of maintenance personnel to major hazard facilities.

The most important achievements in this PhD project are the following three main contributions to the process industries for the prevention of maintenance-related major accidents:

1. *Novel frameworks for maintenance-related major accident classification and the identification of the main causes*: The research has reaffirmed that maintenance related major accidents pose a big problem to the process industry and it clearly identified and prioritized factors for appropriate improvement efforts. In addition, the research informs the process industries to look beyond searching for safety through only best practice of maintenance management/work process, but to consider also the accident process in relation to maintenance.
2. *A novel maintenance optimization formula for the reduction of major accident risk in the process industries*: The research has established a new relationship that balances the equipment and human risk, which is important considering the unavoidable contact between maintainers and equipment: The maintainers may be harmed by the equipment, by other workplace hazards or a combination of these, and the equipment may be neglected to failure or compromised by the maintainer.
3. *A novel framework for improving the robustness and resilience properties in the organizational network encompassing maintenance and other key units within the process industry organization*: The research informs the process industries that in order to counter the challenge of major accidents related to maintenance, there has to be a transition from just concentrating on the

maintenance of physical systems to a holistic focus on this and the robustness and resilience of the links between the maintenance organization and others.

The aforementioned contributions satisfy the overarching objective of this PhD project which is the *development of new strategies for the prevention of maintenance-related major accidents in the process industries*. Similarly, they justify the topic of the PhD project: *Maintenance strategies for major accident prevention*.

6.5 Expected benefits of this PhD project to the industry

This project will give the industry better tools for managing maintenance-related major accident risk on the basis of the following:

- The accident process perspective (barrier-related) of the scheme supports the suggestion for the broadening of the process safety management (PSM) focus to cover barrier maintenance as a key feature [78]. According to Pitblado [78], process safety management alone, based on its current composition, had not shown reasonable reduction in major accident risk. Furthermore, the maintenance management perspective will sensitize establishments on evaluating appropriate attention for the management-related factors at the "blunt end" of operation rather than concentrating only on improvement in execution. This is supported by the fact that most accidents occur during work execution (i.e. at the "sharp end" of operation) and tend to make the personnel in this phase of operation the most investigated, limiting focus on the management's influence [84, 87, 102].
- In addition to the accident process perspective which features barrier-related and organizational causes, the maintenance work process perspective identifies the origin, intermediate (if applicable) and manifestation phases of the accident. It is important to know how maintenance can cause major accident barriers to fail and how this is influenced by the state of maintenance activities. The coverage of technical, human, organizational and operational factors makes the scheme suitable for supporting a far-reaching prevention strategy against maintenance-related major accidents. The scheme is readily practicable for describing/analyzing accidents, since it consists of key unambiguous and non-overlapping terms peculiar to the industry.
- The classification schemes developed can be used as a basis/templates to assess data from other reported accidents and precursor events in the future. The categories were clearly defined, such that they can be applied by different persons and still arriving at the same result (repeatability). Coherence and consistency of information was guaranteed by using key terms that are familiar to the process industry. The aforementioned template can serve dual purpose, being applicable to both investigation and analysis of accidents.

- The classification schemes, by being barrier-related, will promote the existing barrier management concept in the process industry. Barriers are indispensable and critical to the prevention of major accidents. It is important to know both how maintenance can cause barriers to fail and which phase of the work process is most frequently involved in order to improve major accident prevention strategies. The identification of the underlying and contributing maintenance-related causes is the first step in the prevention of the associated major accidents.
- Hale et al. [26] highlighted also the need for encouraging the development of auditing techniques. The WAP scheme is finely categorized and consists of both technical and organizational elements which are adaptable to an auditing template. This can be consolidated with the robustness and resilience related recommendations for maintenance in article 6.
- Concerning the use of the statistical findings in relation to maintenance management, the knowledge of the percentage of major accidents that are maintenance-related would give us an updated picture/awareness of the phenomenon. Working with older statistics may lead to excessive, insufficient or unnecessary use of time and resources to tackle a prevailing problem whose status may have changed over time. In addition, the knowledge of the most important causes will help to prioritize decisions related to developing an efficient and effective prevention program.
- The new robustness/resilience framework creates new awareness about some hidden robustness and resilience potentials of maintenance and how to apply these to a large extent in managing the organizational factors of major accidents.
- Improved methods for analysis of potential positive and negative effects of maintenance on safety, specifically in relation to major accidents. This includes methods for optimization of maintenance with respect to minimizing major accident risk, not just cost.
- Further application is possible with the maintenance optimization formula developed such that specific data are applied in relation to safety systems such as pressure safety valves (PSV) and emergency shutdown valves (ESDV) within, say, the Norwegian continental shelf. This will go a long way in improving activities such as re-certification of valves.

6.6 Future research

This PhD project is valuable as a basis for future research in the following ways:

- The application of the knowledge of the Work and Accident Process (WAP) classification scheme and the observed causal frequencies in the modeling of maintenance related major accident risk in the process industries.

- The robustness and resilience properties of maintenance identified can also be used in future as a basis for the quantification of risk reduction in relation to maintenance-related, human and organizational factors.
- Further optimization may be done, focusing on systems other than safety systems. There may be different or several important bases (including risk) to optimize with respect to, which would lead to different models.

Chapter 7
Acronyms and abbreviations

BP	British Petroleum
BSEE	Bureau of Safety and Environmental Enforcement
CBM	Condition Based Maintenance
CM	Corrective Maintenance
CMMS	Computerized Maintenance Management System
COAD	Conflicting Objectives, Adaptation and Drift
CSB	U.S. Chemical Safety Board
DOE	U.S. Department of Energy
FMEA	Failure Modes and Effects Analysis
HAZID	Hazard Identification
HRO	High Reliability Organizations
HSE	Health and Safety Executive
IChemE	Institution of Chemical Engineers
IDEF0	Integration Definition for Function Modeling
IEC	International Electrotechnical Committee
IEEE	Institute of Electrical and Electronic Engineers
ISD	Inherently Safety Design
JSA	Job Safety Analysis
MAs	Major Accidents
MMD	Man-Made Disaster
MOC	Management of Change
NAT	Normal Accident Theory
NCS	Norwegian Continental Shelf
NOPSEMA	National Offshore Petroleum Safety and Environmental Management Authority
NTNU	Norwegian University of Science and Technology
OECD	Organization for Economic Co-operation and Development
OGP	International Association of Oil and Gas Producers
OSHA	Occupational Safety and Health Administration
PM	Preventive Maintenance

PSA	Petroleum Safety Authority
PSM	Process Safety Management
PTW	Permit To Work
RAMS	Reliability, Availability, Maintainability, and Safety
RCM	Reliability Centered Maintenance
SINTEF	Stiftelsen for Industriell og Teknisk Forskning
TEM	Threat and Error Management
TU-Delft	Delft University of Technology
UK	United Kingdom
US	United States
USEPA	U.S. Environmental Protection Agency
VTT	VTT Technical Research Centre of Finland Ltd
WAP	Work and Accident Process

References

[1] Anderies, J. M., Janssen, M. A., and Ostrom, E. (2004). A Framework to Analyze the Robustness of Social-ecological Systems from an Institutional Perspective. *Ecology and Society*, 9(1).

[2] Asbjø rnslett, B. and Rausand, M. (1999). Assess the vulnerability of your production system. *Production Planning and Control*, 10(3):219–229.

[3] BBC (2011). Germany: Nuclear power plants to close by 2022. (http://www.bbc.co.uk/news/world-europe-13592208).

[4] Bird, F., Germain, G., and Clark, D. (2004). *Practical Loss Control Leadership*. DNV, Atlanta, 3rd edition.

[5] Blanchard, B. and Fabrycky, W. (1998). *Systems engineering and analysis*. Prentice Hall, New Jersey.

[6] Blaxter, L., Hughes, C., and Tight, M. (2006). *How to research*. Open University Press, Berkshire, UK, 3rd edition.

[7] Boissieres, I. and Marsden, E. (2005). Organisational Factors of Robustness. In *Proceedings of the 2nd International ISCRAM Conference*, pages 117–122, Brussels.

[8] Boundless (2014). The Study of Life. In *Boundless biology*. boundless.com. (https://www.boundless.com/biology/textbooks/boundless-biology-textbook/the-study-of-life-1/the-science-of-biology-48/two-types-of-science-basic-science-and-applied-science-266-11399/).

[9] Chandra, C. and Grabis, J. (2007). *Supply Chain Configuration: Concepts, Solutions, and Applications*. Springer, New York, 1st edition.

[10] Comlaw (2007). Occupational Health and Safety (Safety Standards) Regulations 1994. Commonwealth of Australia, Canberra. (http://www.comlaw.gov.au/Details/F2007C00737).

[11] Commonwealth of Australia (2009). Offshore Petroleum (Safety) Regulations 2009, Select Legislative Instrument 2009 No. 382. Commonwealth of Australia, Canberra.

[12] CSB (2007). Investigation Report, Refinery Explosion and Fire, (15 Killed, 180 Injured), BP, Texas City, Texas, March 23, 2005. Report No. 2005-04-I-TX. Technical report, U.S. Chemical Safety Board, Texas.

[13] Dekker, R. (1996). Applications of maintenance optimization models: a review and analysis. *Reliability Engineering & System Safety*, 51(3):229–240.

[14] Dekker, S. (2006). Resilience Engineering: Chronicling the Emergence of Confused Consensus. In Hollnagel, E., Woods, D. D., and Leveson, N., editors, *Resilience Engineering: Concepts and Precepts*, chapter 7, pages 77–92. Ashgate, Surrey.

[15] Dekker, S., Hollnagel, E., Woods, D. D., and Cook, R. (2008). Resilience Engineering : New directions for measuring and maintaining safety in complex systems. Technical report, Lund University School of Aviation.

[16] DHSG (2011). Final Report on the Investigation of the Macondo Well Blowout. Technical Report May 2010, Deepwater Horizon Study Group.

[17] DOE (2004). DOE Handbook, DOE-HDBK-1100-2004: Chemical Process Hazard Analysis. Technical report, US Department of Energy, Washington, DC.

[18] EC (2005). Guidance on the Preparation of a Safety Report to meet the Requirements of Directive 96/82/EC as amended by Directive 2003/105/EC (Seveso II), Report EUR 22113 EN. Technical report, European Commission.

[19] EN 13306 (2010). Maintenance: Maintenance Terminology. Standard. European Committee for Standardization, Brussels.

[20] Evans, J. and Thakorlal, G. (2004). Total Loss Prevention - Developing Identification and Assessment Methods for Business Risks. In *11th International Symposium on Loss Prevention and Safety Promotion in the Process Industries*, Praha. WP Loss Prevention.

[21] Fabiano, B. (2014). Editorial: Loss Prevention and Safety Promotion in the Process Industries. *Process Safety and Environmental Protection*, 92:277–279.

[22] Feldman, R. (2001). Evidence. In Audi, R., editor, *The Cambridge Dictionary of Philosophy*, pages 293–294. Cambridge University Press, Cambridge, UK, 2nd edition.

[23] Gibson, J. J. (1961). The contribution of experimental psychology to the formulation of the problem of safety - a brief for basic research. *Behavioral approaches to accident research*, pages 77–89.

[24] Given, L. M. (2008). *The Sage encyclopedia of qualitative research methods*. Sage Publications, Los Angeles, California.

[25] Gran, B., Bye, R., Nyheim, O., Okstad, E., Seljelid, J., Sklet, S., Vatn, J., and Vinnem, J. (2012). Evaluation of the Risk OMT model for maintenance work on major offshore process equipment. *Journal of Loss Prevention in the Process Industries*, 25(3):582–593.

[26] Hale, A., Heming, B., Smit, K., Rodenburg, F., and van Leeuwen, N. (1998). Evaluating safety in the management of maintenance activities in the chemical process industry. *Safety Science*, 28(1):21–44.

[27] Hameed, Z. and Vatn, J. (2012). Role of grouping in the development of an overall maintenance optimization framework for offshore wind turbines. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 226(6):584–601.

[28] Hirsch, H. (1971). Setting test intervals and allowable bypass times as a function of protection system goals. *IEEE Trans. Nuclear Science*, N-18:488–494.

[29] Hitchcock, C. (2011). Probabilistic Causation. In Zalta, E. N., editor, *The Stanford Encyclopedia of Philosophy*. Stanford University, Stanford, winter edition.

[30] Hollnagel, E. (2009). Safety Culture, Safety Management and Resilience Engineering. Mines ParisTech, Paris. (http://www.atec.or.jp/Forum__09__Hollnagel.pdf).

[31] Hollnagel, E. (2011). Prologue: The Scope of Resilience Engineering. In Hollnagel, E., Paries, J., Woods, D. D., and Wreathall, J., editors, *Resilience Engineering in Practice: A Guidebook*. Ashgate, Surrey.

[32] HSE (1987). Dangerous maintenance. A study of maintenance accidents and how to prevent them. HSE Books, ISBN 0118863479, London.

[33] HSE (1992). A guide to the Offshore Installations (Safety Case) Regulations 1992. Health and Safety Executive, London.

[34] HSE (2001). Maintenance-Reducing the risk, Offshore Technology Report 2001/007. Technical report, Health and Safety Executive, London.

[35] HSE (2009). Guidance on management of ageing and thorough reviews of ageing installations - offshore information sheet No. 4/2009. Technical report, Health and Safety Executive, Aberdeen.

[36] IEC 61511 (2004). Functional safety - Safety instrumented systems for the process industry. Standard. International Electrotechnical Commission, Geneva.

[37] Jacobs, I. (1968). Reliability of engineered safety features as a function of testing frequency. *Nuclear Safety*, 9:303–312.

[38] Jo, Y.-d. and Park, K.-s. (2003). Dynamic management of human error to reduce total risk. *Journal of Loss Prevention in the Process Industries*, 16:313–321.

[39] Kančev, D. and Čepin, M. (2011a). Evaluation of risk and cost using an age-dependent unavailability modelling of test and maintenance for standby components. *Journal of Loss Prevention in the Process Industries*, 24(2):146–155.

[40] Kančev, D. and Čepin, M. (2011b). The price of risk reduction: Optimization of test and maintenance integrating risk and cost. *Nuclear Engineering and Design*, 241(4):1119–1125.

[41] Kasim, R., Alexander, K., and Hudson, J. (2010). A choice of research strategy for identifying community-based action skill requirements in the process of delivering housing market renewal. Technical report, Research Institute for the Built and Human Environment, University of Salford, Salford, UK.

[42] Kelly, A. (1984). *Maintenance Planning and Control*. Butterworths, London.

[43] Khalaquzzaman, M., Gook, H., Cheol, M., and Hyun, P. (2011). Optimization of periodic testing frequency of a reactor protection system based on a risk-cost model and public risk perception. *Nuclear Engineering and Design*, 241(5):1538–1547.

[44] Khalaquzzaman, M., Kang, H. G., Kim, M. C., and Seong, P. H. (2010). Quantification of unavailability caused by random failures and maintenance human errors in nuclear power plants. *Nuclear Engineering and Design*, 240(6):1606–1613.

[45] Khan, F. (1999). Major accidents in process industries and an analysis of causes and consequences. *Journal of Loss Prevention in the Process Industries*, 12(5):361–378.

[46] Kjellen, U. (1984). The Deviation Concept in Occupational Accident Control - I. *Accident Analysis and Prevention*, 16:289–306.

[47] Kuhn, T. S. (1961). The Function of Measurement in Modern Physical Science. *Isis*, 52(2):161–193.

[48] LaPorte, T. and Consolini, P. (1991). Working in Practice but Not in Theory: Theoretical Challenges of High-Reliability Organizations. *Public Administration Research and Theory*, 1(1):19–47.

[49] Lind, S. (2009). *Accident sources in industrial maintenance operations: Proposals for identification, modelling and management of accident risks*. PhD thesis, Tampere University of Technology, Tampere, Finland.

[50] Lind, Salla; Nenonen, S.; Kvistö-Rahnasto, J. (2008). Safety risk assessment in industrial maintenance. *Journal of Quality in Maintenance Engineering*, 14(2).

[51] Lortie, M. and Rizzo, P. (1999). The classification of accident data. *Safety Science*, 31:31–57.

[52] Maguire, R. (2007). Comparing and Contrasting some of the Approaches in UK and USA Safety Assessment Processes. In Redmill, Felix; Anderson, T., editor, *The Safety of Systems*, chapter 8, page 117. Springer, London.

[53] Merriam-Webster (2014). Research. (http://www.merriam-webster.com/dictionary/research).

[54] Moan, T. (2011a). IFEL 8000: The thesis and other publications, dissemination of research results. Technical report, Norwegian University of Science and Technology, Trondheim, Norway.

[55] Moan, T. (2011b). Overview of IFEL 8000 - Introduction to Research Methodology, Theory of Science and Ethics. Technical report, Norwegian University of Science and Technology, Trondheim, Norway.

[56] National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (2011). Final Report, Deepwater, The Gulf Oil Disaster and The Future of Offshore Drilling, Report to The President. Technical report, USA.

[57] Nicolai, R. P. and Dekker, R. (2008). Optimal Maintenance of Multi-component Systems : A Review. In Kobbacy, K. and Murthy, D., editors, *Complex System Maintenance Handbook*, number 1991, chapter 11, pages 263–268. Springer, London.

[58] Nielsen, L. and Holmefjord, A. (2004). How to Design a Robust Emergency Preparedness Organisation for Offshore Drilling. In *The Seventh SPE International Conference on Health, Safety, and Environment in Oil and Gas Exploration and Production*, pages 1–4, Calgary. Society of Petroleum Engineers.

[59] NOPSA (2008). NOPSA Annual report 2007-08. Technical report, National Offshore Petroleum Safety Authority, Perth, Australia.

[60] NORSOK Z-008 (2011). Risk based maintenance and consequence classification. Standard, Standards Norway, Lysaker, Norway.

[61] Ø ien, K. and Schjø lberg, P. (2007). Maintenance as a means to prevent major accidents; Maintenance status and challenges, SINTEF report A2535. Technical report, SINTEF, Trondheim, Norway.

[62] Ø ien, K., Schjø lberg, P., Meland, O., Leto, S., and Spilde, H. (2010a). Correct Maintenance Prevents Major Accidents. *MaintWorld*, pages 26–28.

[63] Ø ien, K., Schjø lberg, P., Meland, O., Leto, S., and Spilde, H. (2010b). The Importance of Maintenance To Prevent Major Accidents. In *Euromaintenance*, pages 34–37, Verona, Italy.

[64] OECD (2013). Glossary of statistical terms. Organisation for Economic Co-operation and Development. (http://stats.oecd.org/glossary/detail.asp?ID=2206).

[65] OGP (2008). Asset integrity - the key to managing major incident risks. Technical Report 415, International Association of Oil and Gas Producers, London.

[66] Okoh, P. (2014). Optimizing maintenance to manage the major accident risk. In *Institution of Chemical Engineers Symposium Series 159, Hazards 24*, Edinburgh. Institution of Chemical Engineers.

[67] Okoh, P. and Haugen, S. (2012). The Effect of Maintenance Seen From Different Perspectives on Major Accident Risk. In *IEEE International Conference on Industrial Engineering and Engineering Management*, pages 917–921, Hong Kong. IEEEXplore.

[68] Okoh, P. and Haugen, S. (2013a). Maintenance-related major accidents: Classification of causes and case study. *Journal of Loss Prevention in the Process Industries*, 26:1060–1070.

[69] Okoh, P. and Haugen, S. (2013b). The Influence of Maintenance on Some Selected Major Accidents. *Chemical Engineering Transactions*, 31:493–498.

[70] Okoh, P. and Haugen, S. (2014a). A study of maintenance-related major accident cases in the 21st century. *Process Safety and Environmental Protection*, 92:346 – 356.

[71] Okoh, P. and Haugen, S. (2014b). Maintenance optimization for major accident risk rduction. *Submitted to Journal of Loss Prevention in the Process Industries*.

[72] Okoh, P. and Haugen, S. (2015). Improving the robustness and resilience properties of maintenance. *Process Safety and Environmental Protection*, 94:212–226.

[73] Pavard, B., Dugdale, J., Saoud, N. B.-b., Darcy, S., and Salembier, P. (2007). Design of robust socio-technical systems. *Resilience Engineering, Juan les Pins, France. (http://www.resilience-engineering-association.org/download/resources/symposium/symposium-2006%282%29/Pavard_et_al_R.pdf)*.

[74] Pekka, P. (2001). An analysis of maintenance failures at nuclear power plant. *Reliability Engineering & System Safety*, 72(3).

[75] Perrow, C. (1984). *Normal Accidents: Living with High-Risk Technologies*. Princeton University Press, New Jersey.

[76] Pickett, J. (2011). *The American Heritage Dictionary of the English Language*. Houghton Mifflin Harcourt, Boston, USA, 5th ed. edition.

[77] Pitblado, R. (2004). Real Time Safety Metrics and Risk Based Operations. In *11th Intl Symposium Loss Prevention, Prague*, number Figure 1.

[78] Pitblado, R. (2011). Global process industry initiatives to reduce major accident hazards. *Journal of Loss Prevention in the Process Industries*, 24(1):57–62.

[79] Popper, K. (1959). *The Logic of Scientific Discovery*. Mohr Siebeck.

[80] PSA (2010a). Management Regulations. Petroleum Safety Authority, Stavanger, Norway.

[81] PSA (2010b). Trends in risk level in the petroleum activity. Technical report, Petroleum Safety Authority, Stavanger, Norway.

[82] PSA (2013). Trends in risk level in the petroleum activity. Technical report, Petroleum Safety Authority, Stavanger, Norway.

[83] Pugh, DS; phillips, E. (2000). *How to get a PhD*. Open University Press, Buckingham, 3rd edition.

[84] Rasmussen, J. (1997). Risk Management in A Dynamic Society: A Modelling Problem. *Safety Science*, 27(2/3):183–213.

[85] Rausand, M. and Vatn, J. (2008). Reliability Centred Maintenance. In Kobbacy, K. and Murthy, D., editors, *Complex system maintenance handbook*, chapter 4, pages 79–108. Springer, London.

[86] Reason, J. (1990). *Human Error*. Cambridge University Press, Cambridge.

[87] Reason, J. (1997). *Managing the risks of organisational accidents*. Ashgate, Aldershot, UK.

[88] Reisinger, D. (2008). The Art of Accident Classification. In *61st annual International Air Safety Seminar*, number October 2008, pages 1–29, Honolulu. Flight Safety Foundation.

[89] Rosness, R., Grø tan, T., Guttormsen, G., Herrera, I., Steiro, T., Stø rseth, F., Tinmannsvik, R., and Wæ rø, I. (2010). Organisational accidents and resilient organisations: Six perspectives, SINTEF A17034. Technical report, SINTEF, Trondheim.

[90] Sagan, S. D. (1993). *The Limits of Safety: Organizations, Accidents, And Nuclear Weapons*. Princeton University Press, New Jersey.

[91] Saleh, J., Marais, K., and Cowlagi, R. (2010). Highlights from the literature on accident causation and system safety: Review of major ideas, recent contributions, and challenges. *Reliability Engineering & System Safety*, 95:1105–1116.

[92] Sanders, R. (2005). Maintenance-Induced Accidents and Process Piping Problems. In *Chemical process safety: learning from case histories*, chapter 5, pages 91–123. Elsevier Inc., third edition.

[93] Saunders (2003). Research. In *Miller-Keane Encyclopedia and Dictionary of Medicine, Nursing, and Allied Health*. Elsevier, 7th edition.

[94] Scriven, M. and Paul, R. (1987). Critical Thinking as Defined by the National Council for Excellence in Critical Thinking. In *8th Annual International Conference on Critical Thinking and Education Reform*, California. National Council for Excellence in Critical Thinking.

[95] Seglen, P. (2001). Evaluating Biology: A Scientometric Study of a University Biology Department. NIFU Skriftserie;2001-6. Technical report, Nordisk institutt for studier av innovasjon, forskning og utdanning, Oslo.

[96] Signoret, J. (1976). Availability of a periodically tested standby system, NUREG/TR-0027. Technical report, Nuclear Regulatory Commission, Washington, DC.

[97] SINTEF (2010). Reliability Prediction Method for Safety Instrumented Systems: PDS Method Handbook. Technical report, SINTEF Technology and Society, Trondheim.

[98] Smith, E. J. and Harris, M. J. (1992). The role of maintenance management deficiencies in major accident causation. *Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering 1989-1996 (vols 203-210)*, 206(15):55–66.

[99] Sternberg, R. J. (2009). *Cognitive Psychology*. Wadsworth, Belmont, USA.

[100] Swain, A.D.; Guttmann, H. E. (1983). Handbook of human reliability analysis with emphasis on nuclear power plant applications. Technical report, Nuclear Regulatory Commission, Washington, DC.

[101] Trochim, W. (2006). Deduction & Induction. (http://www.socialresearchmethods.net/kb/dedind.php).

[102] Turner, B. A. (1978). *Man-Made Disasters*. Wykeham Science Series, London.

[103] UK (1999). The Control of Major Accident Hazards Regulations 1999. The British Government, London. (http://www.legislation.gov.uk/uksi/1999/743/regulation/2/made).

[104] USEPA-OSHA (1996). MOU Between The United States Environmental Protection Agency, Office of Solid Waste and Emergency Response, Office of Enforcement and Compliance Assurance and The United States Department of Labor, Occupational Safety and Health Administration. USA.

[105] van Zante-de Fokkert, J., den Hertog, D., van den Berg, F., and Verhoeven, J. (2007). The Netherlands Schedules Track Maintenance to Improve Track Workers' Safety. *Interfaces*, 37:133–142.

[106] Vatn, J. (1997). Maintenance optimisation from a decision theoretical point of view. *Reliability Engineering & System Safety*, 58(2):119–126.

[107] Vatn, J. (2007). Veien frem til "World Class Maintenance": Maintenance Optimisation. Technical report, Norwegian University of Science and Technology, Trondheim, Norway.

[108] Vatn, J. (2008). Maintenance in Railway Industry. In Kobbacy, K. and Murthy, D., editors, *Complex System Maintenance Handbook*, chapter 21, pages 509–534. Springer, London.

[109] Vatn, J., Hokstad, P., and Bodsberg, L. (1996). An overall model for maintenance optimization. *Reliability Engineering & System Safety*, 51(3):241–257.

[110] Vaurio, J. (1991). Comments on system availability analysis and optimal test intervals. *Nuclear Engineering and Design*, 128:401–402.

[111] Vaurio, J. (1995). Optimization of test and maintenance intervals based on risk and cost. *Reliability Engineering & System Safety*, 49(1):23–36.

[112] Vaurio, J. (1997). On time-dependent availability and maintenance optimization of standby units under various maintenance policies. *Reliability Engineering & System Safety*, 56(1):79–89.

[113] Vinnem, J., Bye, R., Gran, B., Kongsvik, T., Nyheim, O., Okstad, E., Seljelid, J., and Vatn, J. (2012). Risk modelling of maintenance work on major process equipment on offshore petroleum installations. *Journal of Loss Prevention in the Process Industries*, 25(2):274–292.

[114] Vinnem, J., Seljelid, J., Haugen, S., and Husebø, T. (2007). Analysis of hydrocarbon leaks on offshore installations. In Aven and Vinnem, editors, *Risk, Reliability and Societal Safety*, pages 1559–1566. Taylor & Francis Group, London.

[115] Vinnem, J. E. (2012). On the analysis of hydrocarbon leaks in the Norwegian offshore industry. *Journal of Loss Prevention in the Process Industries*, 25(4):709–717.

[116] Vinnem, J. E. (2013). On the development of failure models for hydrocarbon leaks during maintenance work in process plants on offshore petroleum installations. *Reliability Engineering & System Safety*, 113:112–121.

[117] VTT (2002). Systematic Analysis of Dependent Human Errors. From the Maintenance. History at Finnish NPPs. Technical report, Nordic Nuclear Safety Research (NKS).

[118] Wacker, J. G. (1998). A definition of theory: research guidelines for different theory-building research methods in operations management. *Journal of Operations Management*, 16(4):361–385.

[119] Wallace, S. and Merritt, C. (2003). Know when to say 'when': A review of safety incidents involving maintenance issues. *Process Safety Progress*, 22(4):212–219.

[120] Watt, J. H. and van den Berg, S. A. (1995). *Research Methods for Communication Science*. Allyn & Bacon, Inc., Connecticut, 1st edition.

[121] Wayne, B. (1995). *The Craft of Research*. The University of Chicago Press, Chicago.

[122] Wildeman, R., Dekker, R., and Smit, A. (1997). A dynamic policy for grouping maintenance activities. *European Journal of Operational Research*, 99(3):530–551.

[123] Wildeman, R. E. (1996). *The Art of Grouping Maintenance*. Doctoral, Erasmus University Rotterdam.

[124] Woods, D. D. (2006). Resilience engineering: Redefining the culture of safety and risk management. *Human Factors and Ergonomics Society Bulletin*, 49(12):1–3.

Part II
Articles

Article 1

Article 1

The Influence of Maintenance on Some Selected Major Accidents
–In *Chemical engineering transactions*

CHEMICAL ENGINEERING TRANSACTIONS
VOL. 31, 2013
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Guest Editors: Eddy De Rademaeker, Bruno Fabiano, Simberto Senni Buratti

ISBN 978-88-95608-22-8; **ISSN** 1974-9791
DOI: 10.3303/CET1331083

The Influence of Maintenance on Some Selected Major Accidents

Peter Okoh*, Stein Haugen

Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim
peter.okoh@ntnu.no

In spite of large and increasing efforts to control major accident risk, a number of serious accidents over the last few years have shown that control still is not sufficient in some cases. Examples of such accidents within the chemical process and oil and gas industries are Flixborough Disaster, Bhopal Disaster, Piper Alpha Disaster, Phillips 66 Disaster, Sodegaura Refinery Disaster, DSM Chemical Plant Explosion, Stockline Plastics Factory Explosion and Texas City Refinery Explosion.
Investigations of the accidents have uncovered a variety of causes and in recent years focus have tended to switch more and more towards organizational and management issues. However, in this paper, we want to focus on how maintenance has influenced some of these major accidents.
Safety barriers are installed to control the risk but this may fail due to barrier vulnerability and/or deficiencies imposed by maintenance itself or due to postponement of maintenance. Maintenance activities in themselves may also trigger events which may develop into major accidents. Maintenance may therefore influence accidents in many ways.
The main objective of the paper is to discuss how maintenance has influenced some major accidents in the oil and gas and chemical process industry.
The paper builds primarily on a thorough literature review, including review of earlier literature on this topic and review of investigation reports from a selection of accidents.

1. Introduction

Major accidents are typically defined as adverse events such as major leaks/releases, fire, explosion or loss of structural integrity, leading to serious danger/damage, to multiple deaths and/or major damages to the environment or properties, as supported by the views of ComLaw (2007), EC (2005), Maguire (2007), OGP (2008) and PSA (2010).
Most industries that handle hazardous substances such as the petroleum and chemical industries have a major accident potential. Several major accidents have occurred during the last 35 years. Flixborough Disaster, Bhopal Disaster, Piper Alpha Disaster, Phillips 66 Disaster, Sodegaura Refinery Disaster, DSM Chemical Plant Explosion, Stockline Plastics Factory Explosion and Texas City Refinery Explosion are a few examples of accidents with devastating consequences to personnel, the environment, the companies and host communities.
Efforts have been made to enhance defences against major accidents based on lessons learnt from accidents. Despite this effort, it can be argued that the risk of major accidents does not always show a positive trend. The number of major hydrocarbon leaks, a key indicator for major accident risk in the Norwegian oil and gas industry, has for example increased between 2008 and 2010 (PSA, 2010).
Major accidents are seldom the result of one failure, but often a combination of failures (Turner, 1978). High degree of technological and organizational complexity is usually mentioned as an attribute of

Please cite this article as: Okoh P. and Haugen S., 2013, The influence of maintenance on some selected major accidents, Chemical Engineering Transactions, 31, 493-498 DOI: 10.3303/CET1331083

industries with a major accident potential (Perrow, 1984). For this reason, it is common to deploy multiple and independent safety barriers that are capable of preventing or mitigating the consequences of unexpected events. This design philosophy is sometimes referred to as defense-in-depth (e.g. in the nuclear industry) (Reason, 1997) and layers of protection (in the process industry) (IEC 61511, 2003). Independence among barriers may be influenced by the use of different design principles, ranging from physical, mechanical to electrical/electronic/programmable systems.

The integrity of the barriers cannot be maintained without adequate level of maintenance. Maintenance is therefore a key activity to reduce the risk of major accidents. On the other hand, maintenance may have a negative effect on barrier performance if the execution is incorrect, insufficient, delayed, or excessive. Maintenance can also be the triggering event, e.g. by operating equipment wrongly. Besides, maintenance also exposes people to risk and should be minimized from this point of view.

Major accidents have been investigated and/or analyzed by some authors such as Khan (1999), Kletz (2001), Lees (2005), Øien et al. (2010) and CSB (2007), but they have tended to view the maintenance complicity in them more from a maintenance management perspective. In this paper, we will look at the accidents from the perspectives of both the accident process and the maintenance management process.

The objective of this paper is to review these accidents and to identify if and how maintenance has influenced each of the events. A simple causal classification is applied to each of the cases. At the end, some conclusions are drawn.

2. Review of Selected Major Accidents

Some authors have offered maintenance management related insights into the classification of maintenance factors influencing major accidents in the hydrocarbon and process industries: Examples are lack of or erroneous maintenance (Hale et al., 1998), poor communication between maintenance and operations staff (Sanders, 2005), maintainability (Hale et al., 1998) and the maintenance management cycle as a whole (Smith and Harris, 1992).

However, in the context of the aforementioned insights, enough focus has not been directed at safety barriers which are critical and crucial to the prevention of major accidents. Hence, it is pertinent to build on the ideas from above and still consider an additional basis that is focused on safety barriers.

In this section, the major accidents will be analyzed on the bases of both the accident process (including safety barriers) and maintenance management cycle. The factors based on safety barriers are as follows: (1) Lack of maintenance: Lack of barrier maintenance which allows barriers to be breached by failure mechanisms (for e.g. lack of maintenance leading to corrosion of barriers), (2) Maintenance error: Wrong maintenance directly breaching safety barriers (for e.g. wrong calibration of level transmitter), (3) New hazard: Maintenance introduces new hazards, which may be triggered by events (for e.g. hot tapping – an ignition source), and (4) Initiating event: Maintenance being an initiating event for an accident scenario (for e.g. loss of containment due to a wrong valve being operated as part of preparations). The factors based on maintenance management cycle are as follows: (1) Lack of maintainability (EN 13306, 2010): Lack of the ability to retain an item or restore it to a state in which it can perform its required functions (for e.g. lack of testability/accessibility), (2) Deficient fault diagnosis (EN 13306, 2010): Deficiency in fault detection, fault localization and identification of causes (for e.g. too little test), (3) Deficient planning (EN 13306, 2010): Deficiency in the organization and documentation of a set of maintenance tasks that include the activities, procedures, resources and time scale required to execute maintenance (for e.g. poor communication between maintenance and operations staff), (4) Deficient scheduling (EN 13306, 2010): Deficiency in predetermined detailing of when a specific maintenance task should be executed (for e.g. too late timing), (5) Deficient execution: Deficiency in the hands-on actions taken to retain an item or restore it to a state in which it can perform its required functions (for e.g. wrong performance of a correct task) and (6) Deficient checking: Deficiency in supervision, confirmation or performance evaluation (for e.g. inadequacy of checklists).

In this paper, the term “active influencing maintenance factors” refers to the maintenance factors which directly influence the realization of an accident, while the term “latent failure” refers to the dormant

factors which contribute indirectly to the realization of the accident (Reason, 1997). The latent failures contribute to the weakening of defences and thus increase the probability of occurrence of accidents through the active failure pathway as shown in Figure 1.

2.1 Case 1: The Texas City Refinery Explosion (March 23, 2005)

On March 23, 2005, at the BP Texas City Refinery, the startup of an isomerization unit whose raffinate tower was overfilled, led to overheating of the raffinate and the opening of pressure relief devices. This resulted in a flammable liquid geyser from a blowdown stack unequipped with flare, leading to an explosion and fire, killing 15 workers and injuring over 170 (CSB, 2007).

The major hazard is flammable and explosive liquid - raffinate. The active influencing maintenance factors include the following (CSB, 2007): (1) Failure to calibrate level transmitter correctly (maintenance error), (2) Failure to clean sight glass (lack of maintenance), and (3) Failure of high level alarm (lack of maintenance), which were in turn influenced by deficient maintenance program. The latent failures include (CSB, 2007): (1) Business objectives and cost unbalanced with maintenance, and (2) Lack of effective process mechanical integrity program. These causes can be illustrated as shown in Figure 1. The influence of maintenance is also associated with deficient fault diagnosis, deficient planning, deficient execution and deficient checking as shown in Table 1.

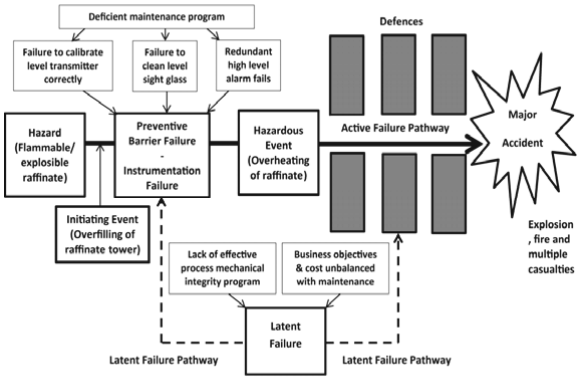


Figure 1: Maintenance-related accident scenario for the Texas City Refinery

2.2 Case 2: Stockline Plastics Explosion (May 11, 2004)

On May 11, 2004, at Stockline Plastics industry in Glasgow, an ageing liquefied petroleum gas (LPG) pipe with inadequate protection when buried, failed due to corrosion and released gas which ignited, exploded and razed the factory building to the ground, killing 9 workers and injuring 40 (OSHA, 2012).

The major hazard is flammable LPG. The active influencing maintenance factor is failure to inspect and maintain an LPG pipe (lack of maintenance) (OSHA, 2012). The latent failures include (OSHA, 2012): (1) Failure to perform suitable and sufficient risk assessments, and (2) Very weak health and safety procedures. The influence of maintenance is also associated with lack of maintainability and deficient fault diagnosis as shown in Table 1.

2.3 Case 3: DSM Chemical Plant Explosion (April 1, 2003)

On April 1, 2003, the DSM melamine plant at Geleen in the Netherlands experienced an explosion as a maintenance crew was restarting the oven; this caused the top cover to collapse and topple over while three workers who were standing on the cover fell into the oven and died (OSHA, 2012).

The major hazard is flammable natural gas and residual gases from other plants; this was ignited by a stray spark. The usually contaminated residual gases had to be filtered, the plant had to be shut down regularly to clean the filters and restarting takes a lot of time; hence a fast-track starting procedure was developed, albeit without adequate testing. The active influencing maintenance factors are: (1) Difficult maintenance (lack of maintainability) and (2) Combustive mixture of gas and air resulting from untested fast-track procedure (new hazard) (OSHA, 2012). The latent failures include (OSHA, 2012): (1) Business objectives and cost unbalanced with maintenance, and (2) Poor safety culture. The influence of maintenance is also associated with deficient planning as shown in Table 1.

2.4 Case 4: Sodegaura Refinery Disaster (October 16, 1992)

On October 16, 1992, the Sodegaura refinery in Japan experienced an explosion and fire, following the breaking-off of the lock ring of the channel cover of a heat exchanger and the blowing-off of the lock ring, channel cover and other parts; ten people died while seven were injured (FKD, 2012).

The major hazard is an explosive gas – hydrogen. The active influencing maintenance factors include the following (FKD, 2012): (1) Repeated ratcheting, leading to reduction in the diameter of the gasket retainer which keeps the heat exchanger airtight (maintenance error), (2) Incorrect replacement of the gasket retainer which contributed to hydrogen gas leak (maintenance error), (3) Removal of insulation, which induced temperature difference (new hazard) that led to thermal deformation of the inner parts of the tube area and contributed to the increase of the diameter of the channel barrel, (4) Inadequate replacement of the internal flange set bolts, leading to their destruction, increased load on the channel cover set bolts, bending and diameter decrease in the lock ring (maintenance error). The latent failures include (FKD, 2012): (1) Misjudgement of whom between the user and manufacturer of the heat exchanger is responsible for the decision and confirmation of the parts replacement, (2) Poor management, and (3) Incomplete standard of replacement. The influence of maintenance also includes lack of maintainability, deficient planning, deficient execution and deficient checking (see Table 1).

2.5 Case 5: The Phillips 66 Disaster (October 23, 1989)

On October 23, 1989, the polyethylene unit of Phillips 66 at Pasadena in USA experienced a chemical release, which subsequently formed flammable vapors and ignited, resulting in a vapor cloud explosion and series of further explosions and fires, killing 23 and injuring between 130 and 300 people; this happened during scheduled maintenance to clear three of the settling legs on a reactor (Lees, 2005).

The major hazard is the buildup of hazardous chemical. The release of the hazard was initiated by wrong maintenance. The active influencing maintenance factors include the following (Lees, 2005): (1) Consolidated isolation via double-block valve or blind flange was not stipulated in existing maintenance procedure (maintenance error), and (2) The only isolating ball valve was kept open by wrongly connected air supply hoses (maintenance error). The latent failures are (Lees, 2005): (1) Non-compliance to company/industry isolation procedure, (2) Non-compliance to site procedure, and (3) Inadequate Permit-To-Work (PTW) system. The influence of maintenance is also associated with deficient planning, deficient execution and deficient checking as shown in Table 1.

2.6 Case 6: The Piper Alpha Disaster (July 6, 1988)

On July 6, 1988, the Piper Alpha offshore platform being operated by Occidental Petroleum experienced a series of explosions in the North Sea, resulting in gas risers ruptures, subsequently causing the structural collapse of the platform and the death of 167 people (Kletz, 2001).

The major hazard is flammable condensate; its leakage was preceded by delayed maintenance schedule and poor maintenance planning; a condensate pump under repair and not tagged-out was mistakenly used to replace another one that failed during operation. The active influencing maintenance factors include the following (Kletz, 2001): (1) Disassembled and non-isolated defective

pump (new hazard), and (2) Replacement with defective pump due to communication gap between maintenance and operations staff at shift handover (initiating event). The latent failures are (Kletz, 2001): (1) Poor quality of safety audits and training, (2) Inadequate maintenance and safety procedures, and (3) Lack of emergency planning. The influence of maintenance is also associated with deficient planning, deficient scheduling and deficient checking as shown in Table 1.

2.7 Case 7: The Bhopal Gas Tragedy (December, 1984)

In December, 1984, about 4000 people were killed and 500,000 injured by toxic release from a chemical plant in Bhopal, following a runaway reaction between Methylisocyanate (MIC) in a storage tank and uncontrolled water for cleaning product lines, which led to vigorous boiling, overpressure of the MIC tank and MIC vapor expulsion to the atmosphere via a rupture disc (Kletz, 2001).

The major hazard is a toxic, unstable chemical - MIC; its runaway reaction with water was initiated by maintenance. The active influencing maintenance factors include the following (Kletz, 2001): (1) Failure of product-line valves due to corrosion (lack of maintenance), (2) Omission of an isolating blank/spade between the MIC tank and the connected product line being cleaned with water (maintenance error), (3) Failure of Nitrogen-line valves due to neglect (lack of maintenance) and (4) Maintenance execution initiating a hazardous reaction between water and MIC (initiating event). The latent failures are (Kletz, 2001): (1) Excessive storage of (MIC) Methlyisocyanate, (2) Business objectives and cost unbalanced with maintenance, and (3) Unavailable safety features: The refrigeration system which could have provided cooling for the storage tank was turned off, the scrubber which should have absorbed the vapour was inoperative, and the flare stack which should have burnt off any residual vapour was out of service. The influence of maintenance also includes deficient fault diagnosis, deficient planning, deficient execution and deficient checking as shown in Table 1.

2.8 Case 8: Flixborough Disaster (June 1, 1974)

On June 1, 1974, twenty-eight workers were killed and 36 injured at the Nypro (UK) site at Flixborough, when a bypass system ruptured and released cyclohexane which formed a combustible mixture with air and exploded on coming into contact with an ignition source (OSHA, 2012).

The major hazard is flammable cyclohexane. The active influencing maintenance factors include (OSHA, 2012): (1) Limited calculations were done on the bypass line (lack of maintenance), (2) Bypass line was not pressure-tested after plant modification (lack of maintenance). The latent failure includes the absence of full risk assessment to support plant modification (OSHA, 2012). The influence of maintenance also includes deficient planning, deficient execution and deficient checking (see Table 1).

Table 1: Maintenance influence on major accident cases

		Barrier-based maintenance factors			
		Lack of maintenance	Maintenance error	New hazard	Initiating event
Maintenance management cycle factors	Lack of maintainability	Case 2	Case 4	Case: 3,4	
	Deficient fault diagnosis	Cases: 1,2,7			
	Deficient planning	Cases: 1,7,8	Cases: 1,4,5,7	Cases: 3,4,6	Cases: 6,7
	Deficient scheduling			Case 6	
	Deficient execution		Cases: 1,4,5,7		Cases: 6,7
	Deficient checking	Cases: 1,7,8	Cases: 1,4,5,7	Cases: 3,4,6	Cases: 6,7

3. Conclusion

This paper is one in a planned series of publications dedicated to a research project titled “Maintenance Strategies for Major Accidents Prevention.” The paper has reanalysed some selected maintenance-related major accidents and given further insights into their causation mechanisms. It has

linked causes to both barrier-based and maintenance management cycle factors. Although the number of cases considered is few, the most occurring barrier-based factor is maintenance error and the most occurring maintenance management factors are deficient planning, deficient execution and deficient checking. This is not indicative enough of what is expected of the result of a larger sample size; however, it will stimulate the sharing of focus to planning, checking and barrier maintenance. Barrier maintenance will augment Process Safety Management which has failed to yield significant reduction in major accident risk (Pitblado, 2011). Besides, industries will be guided against concentrating only on improvement in execution despite the fact that most accidents occur during work execution.

References

Comlaw, 2007, Occupational Health and Safety (Safety Standards) Regulations 1994. <www.comlaw.gov.au/Details/F2007C00737> accessed 29.06.2012

CSB (U.S. Chemical Safety Board), 2007, Investigation Report, Refinery Explosion and Fire, (15 Killed, 180 Injured), BP, Texas City, Texas, March 23, 2005. Report No. 2005-04-I-TX. Tech. rep., Texas, USA.

EC (European Commission), 2005, Guidance on the Preparation of a Safety Report to meet the Requirements of Directive 96/82/EC as amended by Directive 2003/105/EC (Seveso II), Report EUR 22113 EN. Tech.rep., European Communities, Luxemburg.

FKD (Failure Knowledge Database), 2012, Case details, <www.sozogaku.com/fkd/en/cfen/CB1011018.html> accessed 06.07.2012.

Hale, A. R., Heming, B. H. J., Smit, K., Rodenburg, F. G., van Leeuwen, N. D., 1998, Evaluating safety in the management of maintenance activities in the chemical process industry, Safety Science 28 (1), 21–44.

IEC 61511 (International Electrotechnical Commission Standard), 2003, Functional safety - Safety instrumented systems for the process industry sector, Geneva, Switzerland.

Khan, F., 1999, Major accidents in process industries and an analysis of causes and consequences, Journal of Loss Prevention in the Process Industries 12 (5), 361–378.

Kletz, T., 2001, Learning from accidents, 3rd Edition, Gulf Professional Publishing, Oxford, UK.

Lees, F. P., 2005, Loss Prevention in the Process Industries, 3rd Edition, Butterworth Heinemann, Burlington, USA.

Maguire, R., 2007, Comparing and Contrasting some of the Approaches in UK and USA Safety Assessment, In: The Safety of Systems, Springer, London, UK., Ch. 8, p. 117.

EN 13306 (European Standard), 2010, Maintenance - Maintenance terminology, European Committee for Standardization, Brussels.

OGP (International Association of Oil and Gas Producers), 2008, Asset integrity – the key to managing major incident risks, Tech. Rep. 415, London, UK.

OSHA (European Agency for Safety and Health at Work), 2012, Accidents <www.osha.europa.eu/en/campaigns/hw2010/maintenance/accidents> accessed 29.06.2012.

Øien, K; Schjølberg, P; Meland, O; Leto, S; Spilde, H., 2010, Correct Maintenance Prevents Major Accidents, MaintWorld, 26–28.

Perrow, C., 1984, Normal Accidents: Living with High-Risk Technologies, Princeton University Press, New Jersey, USA.

Pitblado, R., 2011, Global process industry initiatives to reduce major accidents hazards, Journal of Loss Prevention in the Process Industries, 24, 57-62.

PSA (Petroleum Safety Authority), 2010, Trends in risk level in the petroleum activity, Tech. rep., Stavanger, Norway.

Reason, J., 1997, Managing the risks of organisational accidents, Hampshire, UK.

Turner, B. A., 1978, Man-Made Disasters, Wykeham Science Series, London, UK.

Sanders, R., 2005, Maintenance-Induced Accidents and Process Piping Problems, In: Chemical process safety: learning from case histories, 3rd Edition, Elsevier Inc., Ch. 5, 91–123.

Smith, E. J., Harris, M. J., 1992, The role of maintenance management deficiencies in major accident causation, Archive: Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering 1989-1996 (Vol 203-210) 206 (15), 55–66.

Article 2

Article 2

Maintenance-related major accidents: Classification of causes and case study

–In *Journal of Loss Prevention in the Process Industries*

Journal of Loss Prevention in the Process Industries 26 (2013) 1060–1070

Contents lists available at SciVerse ScienceDirect

Journal of Loss Prevention in the Process Industries

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

Maintenance-related major accidents: Classification of causes and case study

Peter Okoh*, Stein Haugen

Department of Production and Quality Engineering, Norwegian University of Science and Technology, NO 7491 Trondheim, Norway

ARTICLE INFO

Article history:
Received 14 February 2013
Received in revised form
5 April 2013
Accepted 5 April 2013

Keywords:
Classification
Maintenance
Major accident
Risk
Hydrocarbon
Chemical process

ABSTRACT

The potential for major accidents is inherent in most industries that handle or store hazardous substances, for *e.g.* the hydrocarbon and chemical process industries. Several major accidents have been experienced over the past three decades. Flixborough Disaster (1974), Seveso Disaster (1976), Alexander Kielland Disaster (1980), Bhopal Gas Tragedy (1984), Sandoz Chemical Spill (1986), Piper Alpha Disaster (1988), Philips 66 Disaster (1989), Esso Longford Gas Explosion (1998), Texas City Refinery Explosion (2005), and most recently the Macondo Blowout (2010) are a few examples of accidents with devastating consequences.

Causes are being exposed over time, but in recent years maintenance influence tends to be given less attention. However, given that some major accidents are maintenance-related, we intend to concentrate on classifying them to give a better insight into the underlying and contributing causes.

High degree of technological and organizational complexity are attributes of these industries, and in order to control the risk, it is common to deploy multiple and independent safety barriers whose integrity cannot be maintained without adequate level of maintenance. However, maintenance may have a negative effect on barrier performance if the execution is incorrect, insufficient, delayed, or excessive. Maintenance can also be the triggering event.

The objectives of this article are: (1) To investigate how maintenance impacts the occurrence of major accidents, and (2) To develop classification schemes for causes of maintenance-related major accidents.

The paper builds primarily on model-based and empirical approaches, the latter being applied to reports on accident investigation and analysis. Based on this, the Work and Accident Process (WAP) classification scheme was proposed in the paper.

1. Introduction

The list of major accidents in the hydrocarbon and chemical process industries over the last three decades is long. Maintenance has been a contributing factor in a number of the cases, such as the Texas City Refinery Explosion (2005), the Phillips 66 Disaster (1989), the Piper Alpha Disaster (1988) and the Bhopal Gas Tragedy (1984). The hydrocarbon and chemical process industry handle hazardous substances and thereby have an inherent potential for major accidents. Safety barriers are usually installed to control the risk associated with such industrial facilities (Sklet, 2006b) and the barriers depend on maintenance to sustain their integrity (Okoh & Haugen, 2012). Control of hazards might sometimes be lost due to barrier degradation or failure introduced by maintenance. Maintenance may also cause major accidents directly by triggering unwanted events. Hence, there is a need to prevent maintenance-related causes of major accidents.

In recent years, attention in accident investigations has tended to be more on organizational issues than technical and human causes of accidents. When BP set up the Baker Panel following the Texas City Refinery Explosion in 2005, the mandate was to investigate process safety management and safety culture in all its US refineries (Pitblado, 2011), although deficient safety barrier maintenance was a contributing factor to the event (U.S. Chemical Safety and Hazard Investigation Board, 2007). Maintenance management features prominently in this report as an element in Process Safety Management. The obvious, potential, maintenance-related improvements among all ten of the panel's recommendations are: (i) making provision for a cross-functional team of auditors with substantial expertise covering maintenance and other departments (Recommendation No.8) and (ii) making provision for process safety awareness training for maintenance personnel and others

* Corresponding author.
E-mail addresses: peter.okoh@ntnu.no, okohpee@yahoo.com (P. Okoh).

0950-4230/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jlp.2013.04.002

(Recommendation No.3) (The BP U.S. Refineries Independent Safety Review Panel, 2007). The panel's recommendations did not address technical safety barriers (Pitblado, 2011; The BP U.S. Refineries Independent Safety Review Panel, 2007) and the maintenance of these (The BP U.S. Refineries Independent Safety Review Panel, 2007). According to Pitblado (2011), many US-based companies have accepted the Baker Panel recommendations, and a suggestion to those that intend to use the recommendations as their primary driver, is to fill the gap.

Significant effort has been expended in the modeling of major accident risk in relation to maintenance and modification works in the hydrocarbon industry and this include the works of Gran et al. (2012), Røed, Mosleh, Vinnem, and Aven (2009), Sklet (2006a), Sklet, J. E. Vinnem, and Aven (2006), Sklet, J. Vinnem, and Aven (2006), Skogdalen and Vinnem (2012), Vinnem (2012, 2013) and Vinnem et al. (2012). In some of these works, maintenance work on process equipment has been classified according to type of work, as a basis for modeling risk.

Some studies (Gran et al., 2012; Hale, Heming, Smit, Rodenburg, & van Leeuwen, 1998; Øien, Schjølberg, Meland, Leto, & Spilde, 2010; Sanders, 2005, chap. 5; Smith & Harris, 1992; Vinnem, 2012, 2013; Vinnem et al., 2012; Wallace, Stephen, & Merritt, 2003) have discussed or applied maintenance related causes of major accidents. According to Hale et al. (1998), such major accidents may occur in the course of production or maintenance itself as a result of deficiencies in maintenance management or flawed transition between both phases. In Sanders (2005, chap. 5), the causes of such major accidents in chemical piping are considered to be improper or insufficient maintenance and lack of a comprehensive maintenance program. The research of Smith and Harris (1992) also linked the causes of such major accidents to deficiencies in maintenance management. Furthermore, the work of Øien et al. (2010) implies that such major accidents are linkable to incorrect classification of equipment. Gran et al. (2012), Vinnem et al. (2012) and Vinnem (2012, 2013) applied Reason's classification (Reason, 1997, 1980) and work process based classification respectively to maintenance work in hydrocarbon process plants. However, an article on classification of causes of maintenance related major accident which has seen it from the perspective of an accident process has yet to be identified. Most of the work that has been done, has been from a maintenance management perspective.

Several investigation reports have pointed at maintenance as a contributing factor to accidents in the hydrocarbon and chemical process industries (Hale et al., 1998; National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 2011; Øien et al., 2010; Sanders, 2005, chap. 5; Smith & Harris, 1992). Overall, the investigations indicate that about 30–40% of all accidents and precursor events in the chemical process industry are due to maintenance-related factors. 30% of all accidents in the chemical process industry between 1982 and 1985 were linked to maintenance by UK's Health and Safety Executive (HSE) (HSE, 1987; Smith & Harris, 1992). The data for the analysis were a mixture of major accidents, occupational accidents and serious incidents. Koehorst reported in 1989, based on the analysis of accidents in FACTS database, that about 40% of accidents involving chemical releases were linked to maintenance (Hale et al., 1998). Hurst et al. reported in 1991 that about 40% of 900 accidents associated with piping failures in the chemical industry were linked to maintenance (Hale et al., 1998), and maintenance accounts for about 30% of major factors leading to accidents in the chemical industries as reported by Lees in 1996 (Khan, 1999). Reports from the hydrocarbon industry vary in their estimation of how maintenance has contributed, and some studies attribute up to 70% of all accidents and precursor events in the hydrocarbon industry to maintenance: Considering both immediate (4.1%) and latent errors (15.3%) from intervention together with an uncertain percentage of 11.8% of technical faults, over 65% of major hydrocarbon leaks on the Norwegian sector of the North Sea were linked to maintenance (Vinnem, Seljelid, Haugen, & Husebø, 2007), and about 33% of hydrocarbon topside gas releases between 1985 and 1988 in Australia were linked to maintenance (NOPSA, 2008).

One of the objectives of this paper is to propose a scheme for classification of maintenance related causes of major accidents in the hydrocarbon and chemical process industries. This is in addition to the objective of understanding how maintenance influences major accidents in the aforementioned industries.

The rest of the paper is structured as follows. First, some discussion on what constitutes a major accident, based on definitions from different sources, is presented. This is followed by a review of classifications applied in other industries, before moving on to some suggestions for how the classification can be performed. The classification scheme that is proposed is then described, and some results from a test of the scheme are provided. Finally, some concluding remarks are provided.

In view of the objectives of this paper, the Work and Accident Process (WAP) classification scheme has been proposed. The classification will view maintenance related major accidents from different perspectives, taking into account the increased focus on organizational influence on accidents, not just the direct causes. The intention is that an improved classification scheme will give a better basis for identification of the most common causes, to help drive improvement.

2. The concept of major accident in hydrocarbon/process industries

Since the purpose of this paper is to establish a classification scheme for maintenance related causes of major accidents, we also need to discuss the concept of major accidents. There is no universally accepted definition of a major accident. Within the process industry, the term process accident is also frequently used with more or less the same meaning. Key elements of major accident definitions by different organizations (Comlaw, 2007; EC, 2005; HSE, 1992; Maguire, 2007, chap. 8; OGP, 2008; PSA, 2010; USEPA-OSHA, 1996) are presented in Table 1.

Terms used to describe major accidents are "adverse"/"unplanned" and "acute"/"sudden". The event types included in the definitions vary somewhat, mainly because the different organizations focus on different industries where different types of events are relevant. For the hydrocarbon/process industries it is releases of flammable and toxic material which is the main concern, although other types of events may also be relevant.

The main aspect of the accidents which make them "major" is of course the consequences. The exact definitions vary significantly, but for this purpose consequences to life and health, to the environment and to assets are all considered. Further, it is noted that some definitions require an actual consequence to have occurred ("Death or serious injury", "One or more human fatalities"). However, in other cases, it is sufficient that there is a potential for a serious consequence ("Serious danger to human health", "Escalation potential for multiple fatalities"). This is an important distinction, also for our purpose. We cannot be certain that the causes of events with actual consequences are the same as events with potential consequences, and since it is actual consequences we want to reduce, we should perhaps limit ourselves to events with actual consequences only.

We have chosen to include also events with potential consequences in our definition. The advantage is that the database is

Table 1
Elements of major accident definitions.

Authority	Mode or magnitude of event	Event types	Impact	Timing of impact	Impact location (as per facility)
Seveso/COMAH, EU/UK, (EC, 2005; UK, 1999)	Adverse occurrence	Major emission, fire or explosion	Serious danger to human health or the environment	Immediate or delayed	Inside or outside
PSA, Norway (PSA, 2010)	Acute incident	Major discharge/ emission or a fire/ explosion	Several serious injuries and/or loss of human life, serious harm to the environment and/or loss of substantial material assets	Immediate or delayed	
HSE, UK (HSE, 1992)		Fire, explosion, dangerous release, loss of structural integrity and helicopter, diving and other work-related events	(a) Death or serious personal injury to persons in the vicinity of the installation, (b) Major damage to the structure of the installation, (c) Collision of a helicopter with the installation, (d) Critical failure of diving operations in connection to the installation and (e) Death or serious personal injuries to five or more persons in the vicinity of the installation arising from other events, excluding hazards such as slips, trips and falls.		Vicinity of installation
NOPSA, Australia (Comlaw, 2007)	Sudden occurrence		Serious danger or harm to a relevant person, an at-risk community, a property or the environment	Immediate or delayed	At facility
OSHA/USEPA, USA (USEPA-OSHA, 1996)		Major chemical accident or release	At least one of the following: (1) Results in one or more human fatalities, (2) Results in the hospitalization of three or more workers or members of the public, (3) Causes property damage (on- and/or off-site) initially estimated at $500,000 or more in total, (4) Presents a serious threat to worker health or safety, public health, property, or the environment, (5) Has significant off-site consequences, such as large-scale evacuations or protection-in-place actions, closing of major transportation routes, substantial environmental contamination or substantial effects (*e.g.*, injury, death) on wildlife or domesticated animals, or (6) Is an event of significant public concern	Immediate or delayed	On-site or off-site
OGP, International (OGP, 2008)	Unplanned event	Hazardous releases and major structural failure or loss of stability that could put the whole asset at risk	Escalation potential for multiple fatalities and/or serious damage		Possibly beyond the asset itself

extended significantly. This introduces some uncertainty since there may be differences in causes, but this is considered to be a limited problem. The consequences are often determined by more or less arbitrary factors not related to the causes at all, such as whether an ignition source is present at the time of a release of flammable material.

There is a broad agreement that both immediate and delayed effects should be considered and this is therefore adopted also in our definition. There is some difference in whether the effects should be limited to the facility where the event occurs or not, but this is considered to be mainly a difference between definitions primarily relevant for offshore facilities (which usually are remote and will not affect anyone outside the facility) and onshore facilities. For our purpose, we will consider effects both inside and outside the facility.

To summarize the above, we have, for the purpose of this paper, defined a major accident as "an unexpected event that causes or has the potential to cause serious consequences such as several serious casualties, extensive environmental or asset damage, with immediate or delayed effects experienced, within or outside the incident facility."

3. Lessons from other industries

This section seeks to present an overview of accident classification in other industries and find classifications that may be relevant to consider also for the hydrocarbon and chemical process industries.

In the nuclear industry, the International Atomic Energy Agency (IAEA) has classified accidents in order of increasing severity from

anomaly to major accidents, has defined a major accident and also classified the initiating events (IAEA, 2003, 2005, 2008). The principle of classification based on initiating events is an idea that is relevant to consider also for maintenance related accidents. The initiating event classification developed for the nuclear industry is however not directly relevant.

In the marine industry, the International Maritime Organization (IMO) has also provided a standard definition for a marine accident, and classified such accidents based on causes and severity of events (Mullai, 2006). Some flag states, *e.g.* US and Sweden, also use their own definitions and/or classification schemes (Mullai, 2006).

Railway accidents have been classified in various ways in Evans (2000) and Edkins and Pollock (1997). Evans (2000) classified fatal train accidents both in terms of causes and consequences, whereas Edkins and Pollock (1997) classified the accidents only with respect to causes and with emphasis on the following: (i) outcome, (ii) principal unsafe acts, (iii) psychological precursors, and (iv) latent organizational factors. Some of this structure may be relevant to consider also for maintenance related causes.

In the aviation industry, there has been an evolution of accident classification by the International Air Transport Association (IATA) over the years (Reisinger, 2008). The IATA Accident Classification Task Force (IATA-ACTF) has classified accidents based on the TEM (Threat and Error Management) framework in relation to the following major characteristics (Reisinger, 2008): (1) Latent conditions, (2) Threats, (3) Errors, (4) Undesired aircraft state, (5) End state, and (6) Post-crash event. The IATA-ACTF reviews accidents every year and this is published in annual safety reports (Reisinger, 2008). In the UK's Civil Aviation Authority (CAA) safety review (2008), a summary of an industry-wide classification scheme of air accidents based on flight phases was presented (CAA, 2008). An equivalent approach would be to classify the maintenance-related causes in terms of the phases of the maintenance management process. An additional lesson for the hydrocarbon and chemical process industries (with respect to maintenance influence classification) is to consider further decomposition of the classification to cover threats and error management; this will address the associated human and organizational factors that contribute to organizational accidents (Reason, 1997; Turner, 1978). Furthermore, according to Goldman, Scott, Fiedler, Edna, and King (2002) of the U.S. Department of Transportation (DOT), the National Transportation Safety Board (NTSB) classified general aviation maintenance-related accidents in terms of type of maintenance activity, which include: (1) installation, (2) maintenance, (3) maintenance inspection, (4) annual inspection, (5) service of aircraft, (6) adjustment, (7) modification, (8) overhaul, and (10) other. The primary focus of the analysis performed in Goldman et al. (2002) with the NSTB classification include the comparison of the categories of maintenance activities on the bases of frequency of types of maintenance, maintenance personnel status, frequency of occurrence of accidents and number of casualties (Goldman et al., 2002). Also in Goldman et al. (2002), installation errors are classified into: (1) wrong part, (2) reversed installation, (3) incorrect attachment, (4) omission, and (5) incorrect connection.

The aforementioned findings support the view of Saleh, Marais, and Cowlagi (2010) that accidents are often classified based on consequence across industries wherein threshold values such as number of fatalities etc are set. An example is the American mining industry where an event involving five fatalities constitutes a mining disaster – a potential administrative tool (Saleh et al., 2010). Saleh et al. (2010), however, pointed out (by virtue of a biological analogy) that a threshold-based classification is only "phenotypical", i.e. not recognizing the underlying factors in an accident unlike a "genotypical" classification. In other words, the phenotypical looks at the consequences (i.e. the end states) of an accident (an event), whereas the genotypical looks at the antecedents (i.e. the preceding states) usually from the origin.

According to Lortie and Rizzo (1999), the knowledge of the underlying causes of accidents is necessary for their prevention. Besides, Larsson (1990) advised earlier that accident prevention objectives are unrealizable with only accident information collection. This is a basis for the genotypical analysis being applied in the following sections.

4. Classification of maintenance-related major accidents

Based on the review of literature and based on the problem being considered, some alternative approaches to classification of causes of maintenance-related accidents are explored. At the end of this section, this is concluded with a proposed classification scheme. Initially, we will however give some reflections on what is a useful classification scheme in this context.

It is important to understand the basis for an intended classification before undertaking it. A relevant guide for the purpose of this paper is presented in the following subsection.

4.1. Criteria for a useful classification scheme

There may be many purposes for developing a classification scheme, and the objectives will also influence what is a useful classification scheme. Some comments are therefore provided to this:

- First of all, the purpose of the classification is to develop a better understanding of causes of accidents. In other words, the focus must be on causal classification and not severity classification. By focusing on only major accidents, we have established a "lower limit" on the actual or potential severity of the consequences.
- The causal classification may take on different shapes, and several alternatives are discussed in the following sections.
- We are focusing on maintenance and maintenance related causes. This means that it may be useful to focus on maintenance-specific factors, such as the maintenance process or the types of systems influenced by maintenance. This will enable identification of which parts of the process most often are causes of accidents. For improvement purposes, this is useful.
- In addition to this, we are also looking to find out more about both direct causes and root causes. A suitable classification scheme therefore needs to consider both groups of causes.

In addition to this, we may also put forward some more general criteria (Kjellen, 1984; Lortie & Rizzo, 1999):

- The defined categories must be such that they do not overlap and should as far as possible also be exhaustive (although this can be solved by adding an "other" category).
- The categories must be clearly defined, such that they can be applied by different persons and still arriving at the same result.
- On a more pragmatic level, it is also necessary to consider the availability of information in the accident reports being used as a basis for classification. There is no point in defining a classification scheme if the information is not available in the sources we have.
- Suitable sorting strategies, *e.g.* typology, must be used to make data coherent in a situation of variability of key terms.

- String of words categorizing a set of data must not be abridged without considering whether it would lead to information loss or not.
- Literal or automatic classification of terms may lead to significant bias. Terms must be investigated for implicit or contextual interpretation.
- There is an optimum degree of structuring, i.e. the number of classes of the classification scheme. A coarse categorization may lead to information too generic for peculiar preventive purposes, whereas a too detailed categorization may be too complicated for statistical surveys and inferences.
- Delimitation of the accident process analysis is essential. The starting point of an accident sequence must be well-defined, if the accident or near-accident process is being defined with respect to time and space.

4.2. Classification in relation to accident process

The maintenance related causes linked to accident process may be described as shown in Fig. 1. Fig. 1 is a bow-tie diagram which illustrates the relationship between a given hazardous (or accidental) event, it's maintenance related causes, the consequences, the deployed safety barriers, and the failure pathways. The active failure pathway in this paper refers to the direct/immediate route to the realization of a major accident, whereas the latent failure pathway refers to the indirect/dormant route to the realization of the major accident (Reason, 1997). The probability of occurrence of major accidents via the active failure pathway can be increased or decreased by changes in the degree of latent failures/conditions.

Based on Fig. 1, there are four main scenarios associated with the barrier-based, maintenance related causes; namely, (1) *Lack of barrier maintenance*: Lack of barrier maintenance which allows barriers to be breached by failure mechanisms (*e.g.* corrosion of safety valves due to neglected maintenance), (2) *Barrier maintenance error*: Maintenance error directly breaching safety barriers (*e.g.* wrong calibration of a safety device), (3) *New hazard*: Maintenance introduces new hazards, which may be triggered by events (*e.g.* a metallic tool forgotten inside a tank containing hazardous chemical after cleaning could become a source of localized corrosion – a weakening of the "containment barrier"), and (4) *Initiating event*: Maintenance being an initiating event for an accident scenario (*e.g.* loss of containment due to a wrong valve being operated as part of preparations). For a major accident to occur, "lack of barrier maintenance" or "barrier maintenance error" must be in combination with "new hazard", "initiating event" or other non-maintenance related causes. The safety barriers may be physical (*e.g.* smoke detector, firewall, containment, corrosion inhibitor etc.) or non-physical (for *e.g.* maintenance procedure, permit to work, warning signs etc.) (Sklet, 2006b).

"Lack of barrier maintenance" is associated with either the latent failure pathway (*e.g.* a lack of maintenance program with effective condition monitoring) or the active failure pathway (*e.g.* failure to pressure-test a new gas bypass system after plant modification, leading to rupture and explosion). "Barrier maintenance error", "new hazard" and "initiating event" are all related to the active failure pathway.

"Lack of barrier maintenance", "barrier maintenance error", "new hazard" and "initiating event" may be gradual or sudden, partial or complete. They may also be classified in terms of errors of omission and commission (Swain & Guttmann, 1983).

A summary of the classifications is presented in Table 2.

This classification scheme presents technical, human and organizational factors comprehensively in the pattern of an accident process. It unfolds the various failure mechanisms (both human and technical) of barriers, which are critical to major accident prevention. It also includes various organizational influences in the form of latent failures.

4.3. Classification in relation to work process

Taking cues from Hale et al. (1998), HSE (1987) and NEA (2001), we can also classify maintenance related causes in terms of work process as shown in Fig. 2. Maintenance errors can occur in one of the following two situations: (1) During turnaround or outage, and (2) During normal operation. The situations are characterized by similar work processes with certain exceptions in relation to shutdown and startup. Shutdown is not necessary in situations of unplanned outages and during such activities as hot tapping and hot bolting. Startup is not necessary either for the latter. Potential deficiencies for each phase are also listed in Fig. 2. According to Hale et al. (1998), out of the 30–40% of serious accidents in the chemical process industry attributable to maintenance, 17% of these occurred during preparation of site for maintenance, 76% during maintenance itself, 7% during or soon after handover to production, and not less than 8% in other phases (start-up, shutdown or normal operations) due to technical failures linked to insufficient maintenance. As regards preparation for maintenance, Wallace and Merritt (2003) suggest that inspection under safe conditions to ensure that equipment is free from residual hazardous materials, testing for pollution, and securing isolation points are imperative. However, the effectiveness of inspection and testing depends on correct calibration of the tools being used.

This classification scheme identifies the various phases of a work process in which something can wrong and it demonstrates what can go wrong in each phase. This will enable us to go into specific details phase-wise when managing safety rather than sorting information from a more general source associated with normal operations or just overlooking a phase as not important for specific risk analysis. Some of the phases such as shutdown, preparation and startup need to be given adequate concern, because accidents involving them could also have serious consequences in like manner accidents associated with the actual performance of

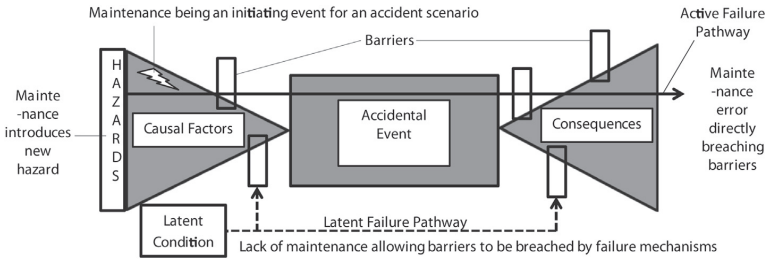


Fig. 1. Classification of barrier-based maintenance-related causes.

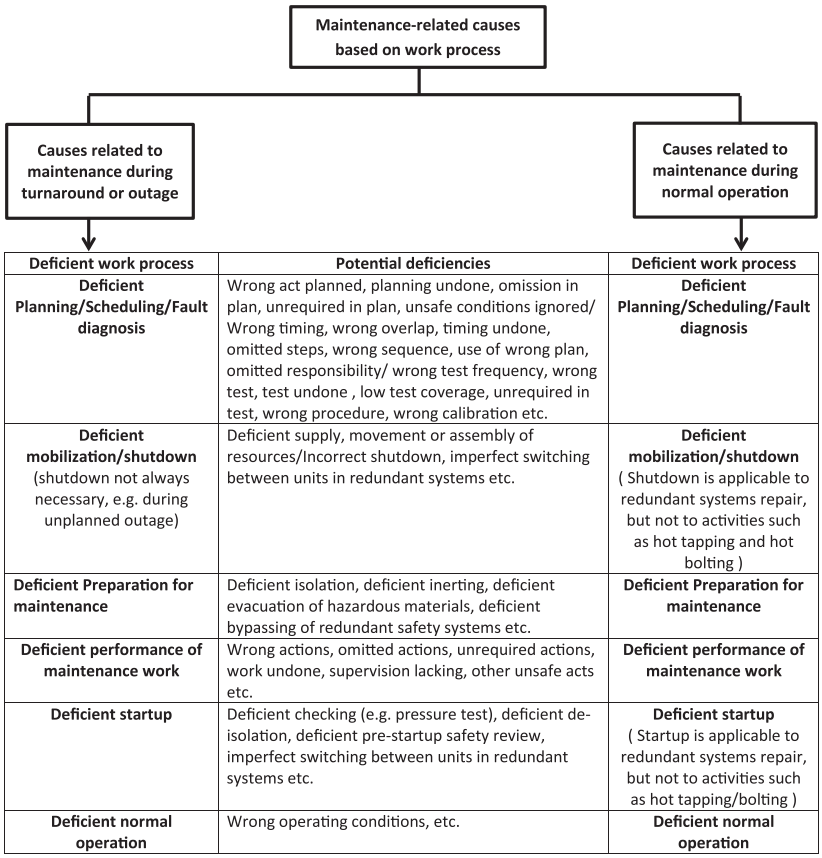
Table 2
Summary of barrier-based classifications.

Maintenance-related causes	Active path	Latent path	Gradual	Sudden	Partial	Complete	Error of omission	Error of commission
Lack of barrier maintenance	•	•	•		•	•	•	
Barrier maintenance error	•		•	•	•	•	•	•
New hazard	•		•	•	•	•	•	•
Initiating event	•			•	•	•	•	•

maintenance work and normal operations. According to Malmén, Nissilä, Virolainen, and Repola (2010), a lot of companies in the hydrocarbon and chemical process industries tend to focus their systematic safety management system on normal operations even though many major accidents have happened during shutdown and startup. Even if an accident manifests during the actual performance of maintenance work or normal operations, it may have started from an earlier phase in the work process! The starting and terminal phases of the accident in the work process are all important in order to better understand the underlying and contributing causes – this enhances their prevention (Lortie & Rizzo, 1999).

4.4. Classification in relation to Threat and Error Management (TEM) Framework

In Section 3, the Threat and Error Management Framework from the aviation industry was mentioned and we can also apply this for our purpose. This is shown in Fig. 3. Maintenance-related major accidents are preceded by latent conditions, threats, errors and undesired maintenance states. The end state is the maintenance-related accidental event. The post-incident events, which are associated with consequences and emergency response, influence the potential for escalation; they can prevent an accidental event from becoming a full-blown accident, an accident from becoming a major accident or a major accident from getting worse. The bold lines indicate the pathways of unmanaged situations, while the broken lines indicate the pathways of managed situations. Latent conditions in combination with either errors or threats or both can create an undesired maintenance state which, if unmanaged, would lead to an accidental state. Safety barriers are required to prevent the undesired maintenance state from reaching the end state. The latent conditions, which include deficiencies in regulatory oversight, safety management system (SMS), training, backlog management etc., are (same as latent



Deficient work process	Potential deficiencies	Deficient work process
Deficient Planning/Scheduling/Fault diagnosis	Wrong act planned, planning undone, omission in plan, unrequired in plan, unsafe conditions ignored/ Wrong timing, wrong overlap, timing undone, omitted steps, wrong sequence, use of wrong plan, omitted responsibility/ wrong test frequency, wrong test, test undone , low test coverage, unrequired in test, wrong procedure, wrong calibration etc.	**Deficient Planning/Scheduling/Fault diagnosis**
Deficient mobilization/shutdown (shutdown not always necessary, e.g. during unplanned outage)	Deficient supply, movement or assembly of resources/Incorrect shutdown, imperfect switching between units in redundant systems etc.	**Deficient mobilization/shutdown** (Shutdown is applicable to redundant systems repair, but not to activities such as hot tapping and hot bolting)
Deficient Preparation for maintenance	Deficient isolation, deficient inerting, deficient evacuation of hazardous materials, deficient bypassing of redundant safety systems etc.	**Deficient Preparation for maintenance**
Deficient performance of maintenance work	Wrong actions, omitted actions, unrequired actions, work undone, supervision lacking, other unsafe acts etc.	**Deficient performance of maintenance work**
Deficient startup	Deficient checking (e.g. pressure test), deficient de-isolation, deficient pre-startup safety review, imperfect switching between units in redundant systems etc.	**Deficient startup** (Startup is applicable to redundant systems repair, but not to activities such as hot tapping/bolting)
Deficient normal operation	Wrong operating conditions, etc.	**Deficient normal operation**

Fig. 2. Classification in relation to maintenance-related work process.

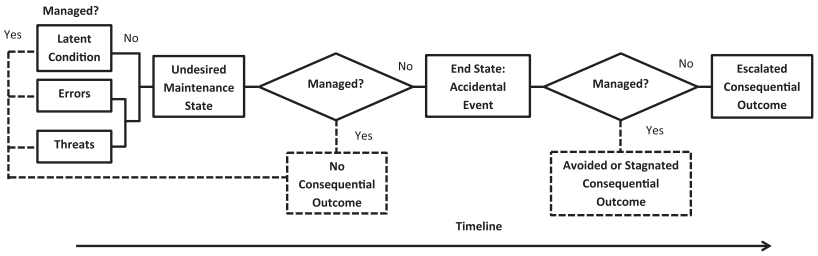


Fig. 3. TEM-based framework as applied to maintenance-related accident process.

failures) as defined earlier. The threats may include equipment malfunction, unfavorable weather condition, unavailability of maintenance support, etc. The errors may be errors of commission or omission. The undesired maintenance state refers to a neglected, ineffective or dangerous state.

This classification scheme, like the barrier-based scheme (mentioned earlier), describes an accident process which is important in understanding the root and contributing causes of accidents. Good knowledge of the underlying causes of accidents is necessary for their prevention (Lortie & Rizzo, 1999). However, the scheme focuses more on human and organizational than on technical factors. The issue of major accident hazards is not explicitly treated. Although the analysis of threats is involved, it does not mean the same thing as the analysis of hazards. According to Rausand (2011), hazard is "a source of danger that may cause harm to an asset.", whereas threat is "anything that might exploit a vulnerability" or in other words "any potential cause of an incident." A spark, for example, is a threat that could exploit the vulnerability due to hydrocarbon leak (Rausand, 2011). This is similar to the TEM-based definition of threats – "events or errors that occur beyond the influence of cabin crew, increase operational complexity, and which must be managed to maintain the margins of safety" (IATA, 2012). In the aviation industry, insufficient separation between two aircrafts, for example, is a threat that could exploit the vulnerability due to wake vortices.

4.5. Classification in relation to Man, Technology and Organisation (MTO)

The Norwegian Petroleum Safety Authority (PSA) have suggested a MTO (Man, Technology and Organisation) based classification of causal factors relating to hydrocarbon leaks (PSA, 2010). Adopting this basis, we can also classify causal factors of maintenance-related major accidents as shown in Fig. 4. According to Wallace and Merritt (2003), the process equipment design phase, should be given timely consideration in order to avoid maintainability challenges later on during usage. Moreover, the unavailability and vulnerability of safety-critical systems are also related to accident causation and they, together with lack of maintainability, belong to the "technology" category (PSA, 2010). The "organization" category constitutes causal factors of major accident according to the theories of Rasmussen (1997), Turner (1978) and Reason (1997). The "man" category represents the contributions of an individual (usually a hands-on personnel) to major accidents (Edkins & Pollock, 1997; PSA, 2010; Reason, 1997).

This classification scheme covers human, organizational and technical factors. However, it does not describe an accident process. The accident process gives a better insight into the underlying causes of accidents and hence promotes their prevention (Lortie & Rizzo, 1999).

4.6. Recommended classification scheme for maintenance related causes

Our recommendation is associated with the two types of causality, the deterministic and probabilistic. Although the theories belong to opposing schools of thought, there is still the possibility of combining both as may be necessary. The deterministic causality of David Hume implies that if A causes B, then B must follow A, but this was countered by the probabilistic causality of Salmon et al. with analogies such as day follows night but night does not cause day (Hitchcock, 2011). The heterogeneity of circumstances in which the cause develops challenges the Humean causality (Hitchcock, 2011). Scientists are usually interested to know precisely the mechanisms by which A causes B, but this is difficult sometimes in the presence of heterogeneity of causal circumstances (Hitchcock, 2011); so it is more convenient for scientists to say that A probably causes B based on statistical correlation between A and B considerably greater than chance (Hitchcock, 2011); this makes the scientists both deterministic and probabilistic in this case (Hitchcock, 2011).

Furthermore, the recommendation is linked to two research approaches, a model-based approach and an empirical approach.

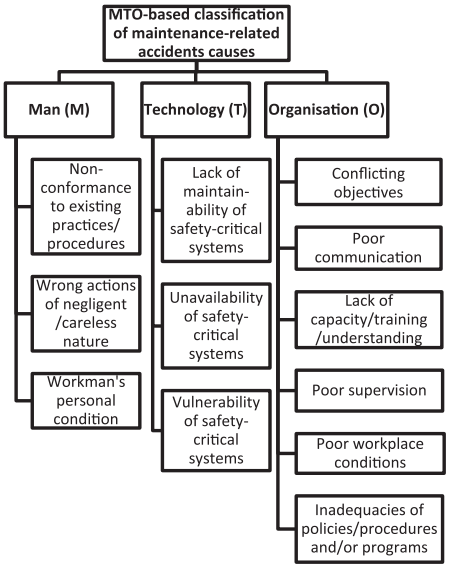


Fig. 4. MTO-based classification of maintenance related causes.

The former is the basis for deriving maintenance-related causes from the work and accident processes, whereas the latter is the basis for deriving the categories of latent failures from the accident reports of the U.S. Chemical Safety Board and French's ARIA database. From a more practical point of view, the quality of information in the accident reports being analyzed can influence its use as a basis for classification. It is pointless to develop a classification scheme that cannot be supported by the sources of information being used.

We recommend a combination of the following types of classification presented earlier: (1) Classification in relation to accident process and (2) Classification in relation to work process. The resulting classification scheme is called the Work and Accident Process (WAP) scheme. The active failures are as presented earlier in the accident-process-related scheme; the same is the case with the latent failures, although these have been dimensioned in this recommendation, based on insights from the accident reports of the U.S. Chemical Safety Board and French's ARIA database, into the following: (1) Deficient regulatory oversight, (2) Deficient risk assessment, (3) Deficient implementation of requirements, (4) Deficient Management of Change (MOC), (5) Deficient documentation, (6) Deficient design, organization or resource management, (7) Unbalanced safety and production goals, (8) Deficient monitoring of performance, (9) Deficient audit, and (10) Deficient learning. All the features of the work-process-related scheme mentioned earlier have also been retained. The latent failures are defined in details as shown in Table 3.

5. Case study

In order to test the suitability of the proposed classification scheme and also to improve and refine it, the scheme was applied to a selection of major accident cases.

Twenty major accident cases from the U.S. Chemical Safety Board (CSB) reports were analyzed and classified with the Work and Accident Process (WAP) scheme and thirteen of them were found to be maintenance-related, see Table 4. Binary numbers 0 and 1 indicate "no" and "yes" (or false and true) respectively.

In the case of the Texas City Refinery Explosion (March 23, 2005), the failures of high level alarm and level sight glass (lack of barrier maintenance – active failure) were associated with deficient planning/scheduling/failure diagnosis, the wrong calibration of level transmitter (barrier maintenance error – active failure) happened via deficient performance of maintenance work and the occurrence of the hazardous events (explosion and fire) is linked to deficient startup. The latent failures include: (i) Deficient implementation of requirements, (ii) Deficient management of change (MOC), (iii) Deficient design, organization or resource management, (iv) Unbalanced safety and production goals, (v) Deficient monitoring of performance and (vi) Deficient learning.

The process of verification of WAP was rigorous and iterative. Both authors worked independently on all of the selected cases and classified the accidents in accordance with the proposed scheme. This served several purposes. It gave an indication of the usability and suitability of the classification scheme and whether the available reports could form a sufficient basis for classification. In this way, both the completeness of the categories suggested in WAP and also potential overlaps between categories were evaluated. By performing the reviews independently, we were also able to identify ambiguities in the categories that could lead to differences in classification. The case study review thus led to several changes and clarifications of the original proposal, leading to the categorization shown in this paper.

Since the scheme is intended for practical use in the industry, we have endeavored to make it as pragmatic as possible by making the most use of information from accident reports from the industry that it is intended for. Besides, our categorization was as far as possible exhaustive and we ensured coherence of information by using key terms that are familiar to the industries. Furthermore, we arranged the work process in a sequential pattern such that the starting point of an accident process can be traced to the point where it manifests.

A further attestation to the suitability of the scheme is that it is currently being applied on a much wider set of cases. The objective of this work is to determine to what extent maintenance has been a cause of major accidents in the hydrocarbon and chemical process

Table 3
Latent failures definitions.

Latent failures	Definitions	Comments
Deficient regulatory oversight	Inadequacies of regulatory bodies in directing, guiding, inspecting, auditing and sanctioning companies under their watch.	Regulatory bodies like OSHA, HSE and PSA have the responsibility of overseeing the activities of the companies under their watch.
Deficient risk assessment	Inadequacies in identifying hazards, analyzing and evaluating associated risks.	Process hazard analysis, environmental impact assessment, workplace hazard assessment etc. should be directed by the management.
Deficient implementation of requirements	This refers to inadequacies in adopting external requirements.	Safety requirements are expected to be implemented by the company's management.
Deficient Management of Change (MOC)	Inadequacies in handling changes, especially non-routine permanent and temporary changes in physical systems, organizations, operations and the operational environment.	It is important to have a situation-specific procedure for non-routine organization of personnel and plant before maintenance linked to dangerous transitory phases.
Deficient documentation	Inadequacies in safety-related documentation	Safety policies and safe work procedures should be included in personnel orientation program.
Deficient design, organization or resource management	Inadequacies in design, layout, coordination, communication, safety culture and management of human, material and financial resources etc.	Designs/layouts should aim to achieve inherent safety. Asset integrity program, effective hiring, coordination, training, safety program, safety culture, communication etc. are vital.
Unbalanced safety and production goals	This is the disproportionate allocation of resources to production at the expense of safety.	The management has to see both goals as concomitant.
Deficient monitoring of performance	This covers inadequacies in measuring performance and detecting trends.	Monitoring is expected to be performed by the company's management continuously in order to detect safety-related deviations on time.
Deficient audit	Inadequacies in checking the conformity of the status of personnel, organization, systems and processes to established requirements.	This may be performed by the company on itself or by an external organization.
Deficient learning	Inadequacies in learning from safety reviews, safety audit reports, industry news, etc.	Management review meetings are necessary for organizational learning and continuous improvement.

Table 4
Work and Accident Process (WAP) classification scheme.

Hydrocarbon/ Chemical process accidents from The U.S. CSB	Maintenance related	Accident process based class.														Work process based class.					
		Active failures				Latent failures															
		Lack of barrier maintenance	Maintenance directly breaching barriers	Maintenance induces new hazards	Maintenance being an initiating event	Deficient regulatory oversight	Deficient risk assessment	Deficient implementation of requirements	Deficient Management of Change (MOC)	Deficient documentation	Deficient design, organization or resource management	Unbalanced safety & production goals	Deficient monitoring of performance	Deficient audit	Deficient learning	Deficient planning/scheduling/fault diagnosis	Deficient mobilization /shutdown	Deficient preparation for maintenance	Deficient performance of maintenance work	Deficient startup	Deficient normal operation
Texas City Refinery Explosion, USA March 23, 2005	1	1	1	0	0	0	0	1	1	0	1	1	1	0	1	1	0	0	1	1	0
Allied Terminals Tank Collapse, USA Nov. 12, 2008	1	0	0	0	1	0	1	1	0	1	0	0	0	0	0	1	0	0	1	0	0
Hoeganaes Metal Dust Flash Fire, USA Jan. 31, 2011	1	1	0	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0	1	1	0
Hoeganaes Metal Dust Flash Fire, USA March 29, 2011	1	1	0	0	0	1	1	1	0	1	1	0	0	0	1	1	0	0	1	0	0
Hoeganaes Hydrogen Explosion, USA May 27, 2011	1	0	0	1	0	1	1	1	0	1	1	0	0	0	1	1	0	1	0	0	0
DuPont Flammable Vapor Explosion, USA Nov. 10, 2010	1	1	0	0	1	1	1	1	0	1	1	0	0	0	0	1	0	1	1	0	0
Goodyear Ammonia Release, USA June 11, 2008	1	0	1	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	1	0	1
Giant Oil Refinery Fire and Explosion USA April 8, 2004	1	0	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	1	1	0	0
EEI Hydrogen Sulfide Release, USA Dec. 11, 2002	1	1	0	0	0	0	1	1	0	1	1	0	0	0	1	0	0	0	0	0	1
Kleen Energy Gas Explosion, USA Feb. 7, 2010	1	1	0	0	1	1	1	0	0	0	1	0	0	0	0	1	0	0	0	1	0
ConAgra Gas Explosion, USA June 9, 2009	1	0	0	0	1	1	1	1	0	0	1	0	0	0	0	1	0	0	0	1	0
Bayer CropScience Tank Explosion, USA Aug. 28, 2008	1	1	1	0	0	0	1	1	1	0	1	0	0	0	0	1	0	0	0	1	0
DuPont Toxic 2Chemical Release Jan. 23, 2010	1	1	0	0	0	0	1	1	1	0	1	0	0	0	1	1	1	0	0	0	0
Total	**13**	**8**	**4**	**1**	**4**	**6**	**10**	**12**	**4**	**7**	**12**	**1**	**1**	**0**	**5**	**9**	**1**	**3**	**7**	**5**	**2**

industries over the years between 2000 and 2012. The most current statistics is about 25 years old and needs to be revised. This work is still under way, but experience is that the proposed categories are robust and that information to categorize cases usually can be found in accident reports.

6. Conclusion and recommendation

This paper is part of an ongoing study to gain more insight into how maintenance can be a causal factor in major accidents in the hydrocarbon and chemical process industries. The first task in this study has been to establish a suitable classification scheme that can form a basis for analyzing the influence on historical accidents. This will again enable identification of where improvements will be most effective.

Classification schemes from a variety of industries such as nuclear, marine, railway and aviation have been considered for useful contributions to the hydrocarbon and chemical process industries. The schemes focus on different aspects, and are valuable to a smaller or larger extent. Based on this review, experience from the process industry and based on the objectives of the ongoing study, a novel classification scheme, the Work and Accident Process (WAP) scheme has been developed.

WAP is based on a combination of an accident process and work process classification scheme. The accident process consists of explicit and comprehensive barrier-based and organizational causes of maintenance related major accidents. Barriers are indispensable and critical to the prevention of major accidents. The work process perspective identifies both the origin and manifestation phase of the accident. It is imperative to know both how maintenance can cause barriers to fail and which phase of the work process is most frequently involved in order to improve major accident prevention strategies.

WAP is comprehensive, complete and finely categorized to address specific industrial challenges. It adequately addresses technical, human and organizational factors. This will be useful for a comprehensive analysis and guidance on the control of maintenance-related major accidents. It will enhance the identification of the underlying and contributing maintenance-related causes, which is the first step in the prevention of the associated major accidents.

WAP has been tested on some accident cases of the U.S. Chemical Safety Board with success. The testing has also served as a basis for improving the scheme. There is further work ongoing to apply the scheme on a much larger data set and it is the intention to report the results from this work in a later paper.

References

CAA. (2008). *Aviation safety review, CAP 780*. Tech. rep.. West Sussex: Civil Aviation Authority

Comlaw. (2007). *Occupational health and safety (safety standards) regulations 1994*. Tech. rep. Canberra: Australian Government. URL:. http://www.comlaw.gov.au/Details/F2007C00737.

EC. (2005). *Guidance on the preparation of a safety report to meet the requirements of directive 96/82/EC as amended by directive 2003/105/EC (Seveso II)*. Report EUR 22113 EN. Tech. rep. European Commission.

Edkins, G. D., & Pollock, C. M. (1997). The influence of sustained attention on railway accidents. *Accident Analysis and Prevention, 29*(4), 533–539.

Evans, A. W. (2000). Fatal train accidents on Britain's mainline railways. *Royal Statistical Society, 163*, 99–119.

Goldman, S. M., Fiedler, E. R., & King, R. E. (2002). *General aviation maintenance-related accidents: A review of ten years of NTSB data*. Report No. DOT/FAA/AM-02/23. Tech. rep. Oklahoma City: FAA Civil Aerospace Medical Institute.

Gran, B., Bye, R., Nyheim, O., Okstad, E., Seljelid, J., Sklet, S., et al. (May 2012). Evaluation of the risk OMT model for maintenance work on major offshore process equipment. *Journal of Loss Prevention in the Process Industries, 25*(3), 582–593.

Hale, A., Heming, B., Smit, K., Rodenburg, F., & van Leeuwen, N. (Feb. 1998). Evaluating safety in the management of maintenance activities in the chemical process industry. *Safety Science, 28*(1), 21–44.

Hitchcock, C. (2011). Probabilistic causation. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Winter ed.). Stanford: Stanford University. URL: http://plato.stanford.edu/archives/win2011/entries/causation-probabilistic/.

HSE. (1987). *Dangerous maintenance. A study of maintenance accidents and how to prevent them*. Tech. rep. London: Health and Safety Executive, HMSO.

HSE. (1992). *A guide to the offshore installations (safety case) regulations 1992*. Tech. rep. London: Health and Safety Executive.

IAEA. (2003). *Accident analysis of nuclear power plants with pressurized water reactors*.

IAEA. (2005). *Accident analysis for nuclear power plants with graphite moderated boiling water RBMK reactors*.

IAEA. (2008). *INES – The International Nuclear and Radiological Event Scale user's manual*. Tech. rep. (2008 ed.). Vienna: International Atomic Energy Agency

IATA. (2012). *Guidance for turbulence management*. Tech. rep.. International Air Transport Association. URL: https://www.iata.org/whatwedo/safety/Documents/guidance-on-turbulence-management.pdf

Khan, F. (Sep. 1999). Major accidents in process industries and an analysis of causes and consequences. *Journal of Loss Prevention in the Process Industries, 12*(5), 361–378.

Kjellen, U. (1984). The deviation concept in occupational accident control – I. *Accident Analysis and Prevention, 16*, 289–306.

Larsson, T. J. (1990). *Accident information and priorities for injury prevention*. Doctoral. Sweden: KTH. URL: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-37325.

Lortie, M., & Rizzo, P. (1999). The classification of accident data. *Safety Science, 31*, 31–57.

Maguire, R. (2007). Comparing and contrasting some of the approaches in UK and USA safety assessment processes. In F. Redmill, & T. Anderson (Eds.), *The safety of systems* (pp. 117). London: Springer.

Malmén, Y., Nissilä, M., Virolainen, K., & Repola, P. (Mar. 2010). Process chemicals – an ever present concern during plant shutdowns. *Journal of Loss Prevention in the Process Industries, 23*(2), 249–252.

Mullai, A. (2006). *Maritime transport and risks of packaged dangerous goods*. Tech. rep.. Turku: DaGoB

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling. (2011). *Final Report, Deepwater, the Gulf oil disaster and the future of offshore drilling*. Report to the President. Tech. rep.

NEA. (2001). *Inspection of maintenance on safety systems during NPP operation*. Tech. rep. Paris: OECD Nuclear Energy Agency (NEA).

NOPSA. (2008). *NOPSA annual report 2007–08*. Tech. rep. Australia: National Offshore Petroleum Safety Authority.

OGP. (2008). *Asset integrity – The key to managing major incident risks*. Tech. Rep. 415. International Association of Oil and Gas Producers.

Øien, K., Schjølberg, P., Meland, O., Leto, S., & Spilde, H. (2010). Correct maintenance prevents major accidents. *MaintWorld*, 26–28.

Okoh, P., & Haugen, S. (2012). The effect of maintenance seen from different perspectives on major accident risk. In *IEEE international conference on industrial engineering and engineering management*. Hong Kong: IEEEXplore.

Pitblado, R. (Jan. 2011). Global process industry initiatives to reduce major accident hazards. *Journal of Loss Prevention in the Process Industries, 24*(1), 57–62.

PSA. (2010). *Trends in risk level in the petroleum activity*. Tech. rep. Norway, Stavanger: Petroleum Safety Authority.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science, 27*(2/3), 183–213.

Rausand, M. (2011). *Risk assessment: Theory, methods, and applications* (1st ed.). New Jersey: John Wiley & Sons.

Reason, J. (1980). *Human error*. Cambridge: Cambridge University Press.

Reason, J. (1997). *Managing the risks of organisational accidents*. Hampshire.

Reisinger, D. (2008). The art of accident classification. In *61st annual international air safety seminar. No. October 2008* (pp. 1–29). Honolulu: Flight Safety Foundation.

Røed, W., Mosleh, A., Vinnem, J. E., & Aven, T. (Feb. 2009). On the use of the hybrid causal logic method in offshore risk analysis. *Reliability Engineering & System Safety, 94*(2), 445–455.

Saleh, J. H., Marais, K. B., & Cowlagi, R. V. (2010). Highlights from the literature on accident causation and system safety: review of major ideas, recent contributions, and challenges. *Reliability Engineering & System Safety, 95*, 1105–1116.

Sanders, R. (2005). Maintenance-induced accidents and process piping problems. In *Chemical process safety: Learning from case histories* (3rd ed.). (pp. 91–123) Elsevier Inc.

Sklet, S. (2006a). Hydrocarbon releases on oil and gas production platforms: release scenarios and safety barriers. *Journal of Loss Prevention in the Process Industries, 19*(5), 481–493.

Sklet, S. (2006b). Safety barriers: definition, classification, and performance. *Journal of Loss Prevention in the Process Industries, 19*(5), 494–506.

Sklet, S., Vinnem, J. E., & Aven, T. (Sep. 2006). Barrier and operational risk analysis of hydrocarbon releases (BORA-Release) part I. Method description. *Journal of Hazardous Materials, 137*, 681–691.

Sklet, S., Vinnem, J., & Aven, T. (2006). Barrier and operational risk analysis of hydrocarbon releases (BORA-Release) part II: results from a case study. *Journal of Hazardous Materials, 137*, 692–708.

Skogdalen, J. E., & Vinnem, J. E. (May 2012). Combining precursor incidents investigations and QRA in oil and gas industry. *Reliability Engineering & System Safety, 101*, 48–58.

Smith, E. J., & Harris, M. J. (Jun. 1992). The role of maintenance management deficiencies in major accident causation. *ARCHIVE: Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering, 1989–1996 (vols. 203–210) 206*(15), 55–66.

Swain, A. D., & Guttmann, H. E. (1983). *Handbook of human reliability analysis with emphasis on nuclear power plant applications*. Tech. rep. Washington, DC: Nuclear Regulatory Commission.

The BP U.S. Refineries Independent Safety Review Panel. (2007). *The report of the BP U.S. refineries independent safety review panel*. Tech. rep. Texas.

Turner, B. A. (1978). *Man-made disasters*. London: Wykeham Science Series.

UK. (1999). *The control of major accident hazards regulations 1999*. Tech. rep. London: United Kingdom. URL:. http://www.legislation.gov.uk/uksi/1999/743/regulation/2/made.

U.S. Chemical Safety and Hazard Investigation Board. (2007). *Investigation Report, Refinery explosion and fire, (15 killed, 180 injured), BP, Texas City, Texas, March 23, 2005*. Report No. 2005-04-I-TX. Tech. rep., Texas.

USEPA-OSHA. (1996). *MOU between the United States Environmental Protection Agency, Office of Solid Waste and Emergency Response, Office of Enforcement and Compliance Assurance and the United States Department of Labor, Occupational Safety and Health Administration*. URL: http://www.osha.gov/pls/oshaweb/owadisp.show_document%20p_table=MOU\&P_id=246.

Vinnem, J. E. (Jul. 2012). On the analysis of hydrocarbon leaks in the Norwegian offshore industry. *Journal of Loss Prevention in the Process Industries, 25*(4), 709–717.

Vinnem, J. E. (May 2013). On the development of failure models for hydrocarbon leaks during maintenance work in process plants on offshore petroleum installations. *Reliability Engineering & System Safety, 113*, 112–121.

Vinnem, J., Bye, R., Gran, B., Kongsvik, T., Nyheim, O., Okstad, E., et al. (Mar. 2012). Risk modelling of maintenance work on major process equipment on offshore petroleum installations. *Journal of Loss Prevention in the Process Industries, 25*(2), 274–292.

Vinnem, J., Seljelid, J., Haugen, S., & Husebø, T. (2007). Analysis of hydrocarbon leaks on offshore installations. In *Proceedings of ESREL* (pp. 1559–1566).

Wallace, S., & Merritt, C. (2003). Know when to say 'when': a review of safety incidents involving maintenance issues. *Process Safety Progress*, (4), 212–219.

Article 3

Article 3

A study of maintenance-related major accident cases in the 21st century
–In *Process Safety and Environmental Protection*

Process Safety and Environmental Protection 92 (2014) 346–356

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

A study of maintenance-related major accident cases in the 21st century

Peter Okoh, Stein Haugen*

Department of Production and Quality Engineering, Norwegian University of Science and Technology, NO 7491 Trondheim, Norway

ABSTRACT

This paper is based on a review of 183 detailed, major accident investigation and analysis reports related to the handling, processing and storage of hydrocarbons and hazardous chemicals over a decade from 2000 to 2011. The reports cover technical, human and organizational factors. In this paper, the Work and Accident Process (WAP) classification scheme is applied to the accident reports with the intention of investigating to what extent maintenance has been a cause of major accidents and what maintenance-related causes have been the most frequent.

The main objectives are: (1) to present more current overall statistics of maintenance-related major accidents, (2) to investigate the trend of maintenance-related major accidents over time, and (3) to investigate which maintenance-related major accident causes are the most frequent, requiring the most attention in the drive for improvement.

The paper presents statistical analysis and interpretation of maintenance-related major accidents' moving averages as well as data related to the types of facility, hazardous substances, major accidents and causes. This is based on a thorough review of accident investigation reports.

It is found that out of 183 major accidents in the US and Europe, maintenance was linked to 80 (44%) and that the accident trend is decreasing. The results also show that "lack of barrier maintenance" (50%), "deficient design, organization and resource management" (85%) and "deficient planning/scheduling/fault diagnosis" (69%) are the most frequent causes in terms of the active accident process, the latent accident process and the work process respectively.

Keywords: Maintenance; Major accident; Statistics; Hydrocarbon; Chemical; Process

1. Introduction

The handling, processing and storage of hydrocarbons and hazardous chemicals by industries whether small or large scale, inherently implies a potential for major accidents. Maintenance can keep the integrity of safety barriers and thus contribute to the prevention of major accidents. On the contrary, it can also be a cause of the major accidents themselves through insufficiency, incorrectness, new hazard inducement or being an initiating event for an accident scenario (Okoh and Haugen, 2013a, 2013).

Several investigations reveal that 30–40% of all accidents and precursor events in the chemical process industry are maintenance related. The UK's Health and Safety Executive linked maintenance to 30% of all accidents (a mixture of major accidents, occupational accidents and serious incidents) in the chemical process industry between 1982 and 1985 (HSE, 1987; Smith and Harris, 1992). As reported by Hale et al. (1998), out of 30–40% of serious accidents in the chemical process industry, 17% occurred during preparation for maintenance, 76% during maintenance itself and 7% during or soon after handback to production, whereas at least 8% of the chemical process accidents occurred in other phases (start-up, shutdown or normal operations) due to technical failures influenced by inadequate maintenance. In the same reference by Hale et al. (1998), Koehorst's report of 1989 based on the analysis of accidents

* *Corresponding author*. Tel.: +47 40309367.
E-mail addresses: peter.okoh@ntnu.no, okohpee@yahoo.com (P. Okoh).
Received 11 December 2013; Received in revised form 1 March 2014; Accepted 6 March 2014
http://dx.doi.org/10.1016/j.psep.2014.03.001

in FACTS database (formerly of TNO, The Netherlands) indicates that 38.5% of accidents involving chemical releases were linked to maintenance. Furthermore, as cited by Hale et al. (1998), the 1991 report of Hurst et al. links 38.7% of 900 accidents associated with piping failures in the chemical industry to maintenance. In the hydrocarbon industry reports, there are also some statistics showing maintenance contribution. A report from Australia indicates that 33% of hydrocarbon topside gas releases between 1985 and 1988 in Australia were linked to maintenance (NOPSA, 2008). A similar study of gas releases in the Norwegian offshore industry shows that over 65% of major hydrocarbon leaks on the Norwegian sector of the North Sea were linked to maintenance (Vinnem et al., 2007). Furthermore, a study of 242 accidents in relation to storage tanks in both industries between 1960 and 2003 reveals that about 30% of such accidents were caused by human errors including poor operation and maintenance (Chang and Lin, 2006).

Most of the aforementioned statistics are about 25 years old. In addition, the most recent statistics do not cover all equipment, being limited to storage tanks only. The data in this paper are recent and cover all types of equipment. The objectives of this paper are: (1) to present more current overall statistics of maintenance-related major accidents, (2) to investigate what the accident trend has been over the period 2000–2011, and (3) to determine which causes are the most frequent, requiring the most preventive efforts. To this end, the Work and Accident Process (WAP) classification scheme (Okoh and Haugen, 2013a) will be applied to 183 major accident cases consisting of 63 from the U.S. Chemical Safety Board (CSB) reports (Chemical Safety Board, 2013) and 120 from the BARPI's ARIA database (Bureau for Analysis of Industrial Risks and Pollution, 2013). The accident reports cover technical, human and organizational factors associated with the handling, processing and storage of hydrocarbons and hazardous chemicals in the process industries. Many of the accident reports also point to other causes than just maintenance. However, our intention in this paper is to focus on only the maintenance-related causes.

The rest of the paper is structured as follows. The paper will discuss the concept of major accident and present statistical analysis and interpretation of maintenance-related major accidents trend as well as data and interpretations related to the types of incident facility, hazardous substances, major accidents, causes and combination of causes. This will be followed by discussion and recommendations, and finally, concluding remarks will be presented.

The study is carried out by both authors independently and with iterative scrutiny. The Work and Accident Process (WAP) scheme is applied after having sorted the major accidents from the occupational accidents and identified the maintenance-related major accidents among the overall major accidents. The WAP scheme has defined accident causation categories. Each accident report has been revised and relevant causation categories were identified. Based on this, we could identify which causes and combination of causes occurred most. The study is also applied in relation to the chosen definition of a major accident. The usability and suitability of WAP had been verified in the previous paper (Okoh and Haugen, 2013a), being comprehensive, complete and finely categorized to address the peculiar challenges of industries (Okoh and Haugen, 2013a). Besides, the accident investigation reports which are the source of this study, are detailed and comprehensive.

Several significant contributions from researches related to major accidents have been recorded in the chemical process industry. These include the works of Kidam and Hurme (2013), Cheng et al. (2013) and Fabiano and Currò (2012).

2. Various views on major accident in relation to the process industry

There is no conventionally accepted definition of the term "major accident" across authorities linked to the process industry. The Norwegian Petroleum Safety Authority (PSA) (PSA, 2010), the European Commission (in relation to Seveso II directive) (EC, 2005) and the UK government (in relation to the Control of Major Accident Hazards regulations) (UK, 1999) have quite similar definitions for a major accident, which can be summarized as follows: an acute/adverse event such as emission/discharge/release, fire or explosion resulting in a serious loss with regards to human life/health, the environment and material assets.

The International Association of Oil and Gas Producers – OGP (OGP, 2008) and the Commonwealth of Australia (Commonwealth of Australia, 2009) also have similar definitions for a major accident, which can be summarized as follows: events connected with an installation having the potential to cause multiple fatality/serious damage inside or away from the facility.

The definitions of a major accident by the UK's Health and Safety Executive (HSE) (HSE, 1992) and the US Occupational Safety and Health Administration (OSHA)/US Environmental Protection Agency (USEPA) (USEPA-OSHA, 1996) also have expressions that imply the potential for serious loss and that the effects may be felt inside or outside the facility. Similarly, the US Department of Energy (DOE) [6] defines an incident as "an unplanned event that may or may not result in injuries and/or loss" and an accident/accident event sequence as "an unplanned event or sequence of events that has an undesirable consequence."

We have chosen to include also events with the potential to cause large consequences in our definition. The benefit is that the database is extended significantly. This introduces some uncertainty since there may be differences in causes of events involving losses and events that could have involved losses, but this is considered to be a limited problem. The consequences are usually defined by more or less arbitrary factors not connected to the causes at all, such as whether an ignition source is present at the time of a combustible gas release. Hence, a major accident as applied in this paper is "an unexpected event that causes or has the potential to cause serious consequences such as several serious casualties, extensive environmental or asset damage, with immediate or delayed effects experienced, within or outside the incident facility" (Okoh and Haugen, 2013a).

The term "process accident" is also often used with more or less the same meaning as the term "major accident" in the process industries. Accidents related to modification and maintenance are some of the types of process accidents that occur. Modification-related accidents are connected with the changing of the required function of an item to a new required function, whereas maintenance-related accidents are connected with an item being retained in or restored to a state in which it can perform it's original required function (EN 13306, 2010).

Table 1 – Geographical locations of maintenance-related major accidents.

Year	USA	Moving average	Europe	Moving average	USA &Europe	Moving average
2000	0		7		7	
2001	3		3		6	
2002	4	2.3	5	5.0	9	7.3
2003	6	4.3	6	4.7	12	9.0
2004	4	4.7	5	5.3	9	10.0
2005	2	4.0	6	5.7	8	9.7
2006	2	2.7	2	4.3	4	7.0
2007	2	2.0	2	3.3	4	5.3
2008	4	2.7	4	2.7	8	5.3
2009	1	2.3	3	3.0	4	5.3
2010	3	2.7	2	3.0	5	5.7
2011	3	2.3	1	2.0	4	4.3
Total	34		46		80	

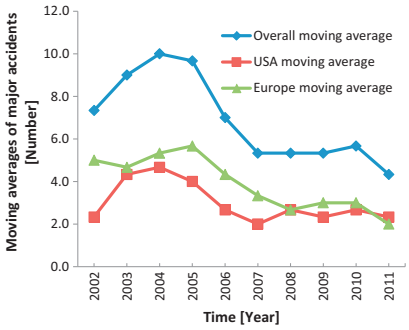


Fig. 1 – Trends of moving averages of maintenance-related major accidents over time.

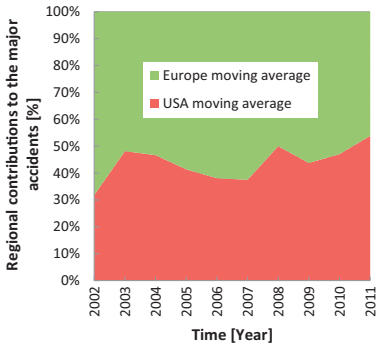


Fig. 2 – Trends in the proportion of each of the major accidents series over time.

3. Overall statistics

According to the U.S. Chemical Safety Board (2013), from the year 2000 to 2011 the US experienced 74 major accidents in the process industry, 64 of which investigations were completed at the time of preparing this paper. Out of the 64 major accidents, 34 (i.e. 53%) are maintenance-related (see Table 1).

Based on information from the Bureau for Analysis of Industrial Risks and Pollution (2013), from the year 2000 to 2011, 120 major accidents occurred in Europe which were completely investigated. Out of the 120 major accidents, 46 (i.e. 38%) are maintenance related (see Table 1).

As regards trends, some useful conclusions can be drawn from the charts in Figs. 1 and 2. Since investigations are still pending on 10 major accidents that occurred in the US in 2008 (2 accidents), 2009 (3 accidents) and 2010 (5 accidents), it will be incorrect to draw a conclusion on the trends over the period 2002–2011. However, we can conclude that Fig. 1 shows that there has been a reduction of maintenance-related major accidents over the period 2002–2007. Fig. 2 shows that of the overall total, the US contributes about 40% and Europe about 60% to the major accidents.

The aforementioned moving averages were calculated using the Microsoft's Excel function, AVERAGE. We used the moving average of 3 years (i.e. 2000–2002, 2001–2003, 2002–2004, etc.). The series of averages helps us to understand how the trend is by smoothing out short-term fluctuations. Shorter length moving averages (e.g. order 3) are more sensitive and identify new trends earlier than longer ones. Besides, the smaller the interval, the closer the moving averages are to the actual data points and this limits the loss of information unlike in higher order moving averages. However, using no moving averages or order 2 would obviously give less smooth curves (for trending). The alternative to using moving averages is trend lines or the raw data. We have included the raw data and it is possible to plot them directly. But we have chosen to use moving averages for the reasons given.

As shown in Fig. 3, most of the maintenance-related major accidents occurred in chemical manufacturing plants (46%). The chemical plant category includes petrochemical plants. The "Others" category includes waste treatment, fossil-fuel power and food processing plants. The second and third most frequently involved plants are petroleum refinery (15%) and storage/terminals (14%) respectively.

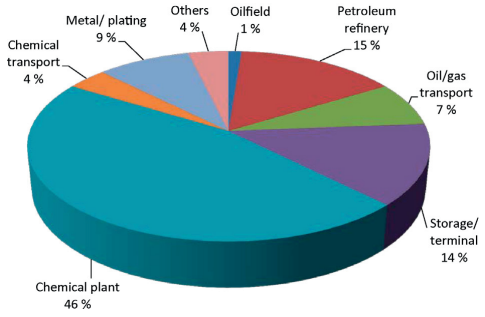


Fig. 3 – Types of plants where accidents occurred.

Table 2 – Type of maintenance-related major accidents.

Year	Fire	Explosion	Emission/discharge	Structural failure or loss of stability
2000	1	3	5	0
2001	4	3	4	0
2002	2	5	5	0
2003	3	5	8	0
2004	4	3	7	0
2005	2	2	5	0
2006	4	3	1	0
2007	1	1	2	1
2008	2	2	6	1
2009	1	3	2	0
2010	0	3	2	0
2011	3	2	1	0
Total	27	35	48	2

In Fig. 4, it is seen that the frequencies of involvement of hazardous substances are in the following order: toxic substances (26%), petrochemicals (22%) and crude oil/natural gas (18%) etc. The total number of substances involved in the 80 maintenance-related major accidents is 82 because two of the accidents each involved two hazardous substances. The fact that toxic substances (e.g. chlorine) are dangerous when in contact with living species and may tend to be corrosive to containments (leading to release), explosive in pressurized containments or support combustion is probably a reason for their being most involved in the major accidents. It could also be that toxic substances are the most common.

According to Table 2, out of the 80 maintenance-related major accidents, "emission/discharge" is involved in the most (60%). This is followed by "explosion" (44%), "fire" (34%) and "structural failure/loss of stability" (3%). Some of the accidents involved combinations of fire and explosion, emission and fire or emission, fire and explosion etc. The structural failure/loss of stability recorded did not result from fire or explosion. The fact that emission/discharge may be toxic, ignitable or explosive probably explains it's most frequent involvement in major accidents. The low number of "structural failure/loss of stability" (only 2) suggests that the structural integrity of the installations have been high enough to withstand the effects of maintenance deficiencies for a long time. Virtually all the cases associated with major damages to structures were as a result of the impact of fire and explosion.

4. Causes of maintenance-related major accidents

In the following subsections, the causes of maintenance-related major accidents will be reviewed based on the Work and Accident Process (WAP) classification scheme (Okoh and Haugen, 2013a). The scheme was developed based on some essential criteria for classification (Lortie and Rizzo, 1999; Kjellen, 1984; Okoh and Haugen, 2013a). The classification scheme consists of both the accident process and maintenance work process parts. The accident process part is related to both the active failure pathway which refers to the direct/immediate route to the manifestation of a major accident and the latent failure pathway which refers to the indirect/dormant route to the manifestation of the major accident (Reason, 1997). The maintenance work process part reflects the various phases of the work process in which something can wrong and it shows what can go wrong in each phase (Hale et al., 1998; Malmén et al., 2010).

4.1. *The work process*

The maintenance work process may be deficient in one or more phases (Okoh and Haugen, 2013a): (1) deficient planning/scheduling/fault diagnosis, (2) deficient mobilization or shutdown, (3) deficient preparation for maintenance, (4) deficient performance of maintenance work, (5) deficient startup and (6) deficient normal operation. The work process aspect identifies the various phases of a work process whose deficiencies can lead to an accident and in what order, for example, deficient planning being undetected during the performance of the maintenance work renders the former deficient and manifests as an accident during normal operation. The work process aspect will enable more specific and effective risk management for a particular kind of phase-wise scenario rather than relying on more general operational information or merely ignoring a phase as not critical to the development of an accident (Okoh and Haugen, 2013a). Analyzing the chain of events from the originating phase through intermediate phases (if applicable) to the manifestation phase gives a better insight into the underlying and contributing causes of the accidents and hence promote prevention efforts (Lortie and Rizzo, 1999).

4.2. *The accident process*

The accident process encompasses the pathways by which both active and latent failures interact and develop into major

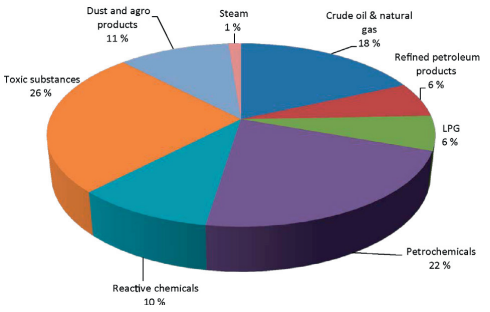


Fig. 4 – Types of substances stored, handled or processed.

Table 3 – Occurrence of active failures.

Year	Lack of barrier maintenance	Maintenance error directly breaching barriers	Maintenance induces new hazards	Maintenance being an initiating event
2000	4	4	0	2
2001	1	0	3	4
2002	5	0	2	2
2003	3	2	1	6
2004	4	3	1	1
2005	6	4	0	1
2006	2	1	2	2
2007	4	0	0	0
2008	3	3	0	3
2009	1	0	1	3
2010	4	0	1	3
2011	3	0	1	0
Total	40	17	12	27

accidents. Major accidents manifest in active failures and the probability of their occurrence are influenced by the degree of latent failures/conditions. The occurrence of these two types of failures which are described further in the following, give additional insights into the underlying and contributing causes of the accidents.

4.2.1. *The active failures*

The active failure pathway represents the direct/immediate route to the occurrence of a major accident. There are four main active-failure scenarios associated with the causes of maintenance-related major accidents, namely (Okoh and Haugen, 2013a, 2013): (1) *lack of barrier maintenance* – lack of barrier maintenance which allows barriers to be breached by failure mechanisms (e.g. unreadable pressure gauge due to lack of cleaning), (2) *barrier maintenance error* – maintenance error directly breaching safety barriers (e.g. bypassing safety systems without applying suitable compensating measures during critical phases of operation), (3) *new hazard* – maintenance introduces new hazards, which may be triggered by events (e.g. the use of hot tapping in line stopping), and (4) *initiating event* - maintenance being an initiating event for an accident scenario (e.g. dangerous release due to the wrong valve being operated as part of preparation for pipeline pigging). A maintenance related major accident will occur when "lack of barrier maintenance" or "barrier maintenance error" occurs in combination with "new hazard", "initiating event" or other non-maintenance related causes (Okoh and Haugen, 2013a).

4.2.2. *The latent failures*

The latent failure pathway represents the indirect/dormant route to the occurrence of the major accident (Reason, 1997) and they have been classified into the following (Okoh and Haugen, 2013a): (1) deficient regulatory oversight, (2) deficient risk assessment, (3) deficient implementation of requirements, (4) deficient management of change (MOC), (5) deficient documentation, (6) deficient design, organization and resource management, (7) unbalanced safety and production goals, (8) deficient monitoring of performance, (9) deficient audit, and (10) deficient learning.

4.3. *Occurrence of active failures*

According to Table 3, out of the 80 maintenance-related major accidents, "lack of barrier maintenance" is the most frequent active cause (50%). This is followed by "maintenance being an initiating event for an accident scenario" (34%), "maintenance error directly breaching barriers" (21%) and "maintenance introduces new hazards" (15%). Some of the accidents involved the failure of multiple barriers through several causes.

4.3.1. *Combinations of active failures*

According to Table 4, the most frequent combination of active failures is "maintenance introduces new hazards – maintenance being an initiating event" (42% of all the combinations). This combination is highly probable for safety-critical maintenance work in plants with significant amounts of hazardous substances. The new hazards are those generated by maintenance e.g. through the application of new, unvalidated procedures, processes, conditions and equipment or existing undervalidated ones. These may become triggered by events (e.g. certain maintenance interventions) that favor their development to an accident. An example can be seen in the Partridge-Raleigh oilfield explosion and fire in the US in 2006, in which "an open-ended piping left unisolated after a previous maintenance session" (*new hazard*) was in combination with "the act of welding a piping connection to it on resumption of maintenance work" (*initiating event*) (Chemical Safety Board, 2013). The second most frequent combination is "lack of barrier maintenance – maintenance error directly breaching barriers" (32% of all the combinations). An example of this can be seen in the Texas City refinery explosion in the US in 2005, in which "failure to clean sight glass" (*lack of barrier maintenance*) was in combination with "failure to calibrate level transmitter correctly" (*barrier maintenance error*). This is

Table 4 – Combinations of active failures (number of occurrences).

	Maintenance error directly breaching barriers	Maintenance induces new hazards	Maintenance being an initiating event
Lack of barrier maintenance	6	2	3
Maintenance introduces new hazards			8

followed by "lack of barrier maintenance – maintenance being an initiating event" (16% of all the combinations) and "lack of barrier maintenance – maintenance introduces new hazards" (11% of all the combinations). When "maintenance being an initiating event for an accident scenario" occurs, the percentage of it in combination with "maintenance introduces new hazards" is 30%. When "maintenance being an initiating event for an accident scenario" occurs, the percentage of it in combination with "lack of barrier maintenance" is 11%. When "lack of barrier maintenance" occurs, the percentage of it in combination with "maintenance errors directly breaching barriers" is 15%. When "lack of barrier maintenance" occurs, the percentage of it in combination with "maintenance introduces new hazards" is 5%.

4.4. *Occurrence of latent failures*

According to Table 5, out of the 80 maintenance related major accidents, "deficient design/organization/resource management" is the most frequent latent cause (85%). This is followed by "deficient risk analysis" (70%), "deficient documentation" (51%), "deficient implementation of requirements" (44%), "deficient monitoring of performance" (23%), "deficient management of change" (21%), "deficient learning" (19%), "deficient regulatory oversight" (16%), "deficient audit" (11%) and "unbalanced safety and production goals" (5%). Some of the accidents involved several latent failures. Disregarding the period between 2008 and 2011 for which some accident investigations have yet to be completed, we can see improvements in "risk assessment", "management of change", "monitoring of performance" and "learning" in at least a period of 4 years leading to 2007. However, it can be seen that there was no improvement in "regulatory oversight" in a period of 3 years leading to 2007.

4.4.1. *Combinations of latent failures*

As shown in Table 6, the most frequent combination of latent failures is "deficient risk assessment – deficient design, organization and resource management" (36% of all the combinations). These two sets of elements are such that they can influence each other: deficient risk assessment may influence deficient design and on the other hand deficient organization and resource management may influence risk assessment. An example can be seen in the DSM Chemical Plant Explosion in the Netherlands in 2003 in which "deficient risk assessment" was in combination with "deficient design, organization and resource management" (Bureau for Analysis of Industrial Risks and Pollution, 2013; Okoh and Haugen, 2013).

The second most frequent combination is "deficient design, organization and resource management – deficient implementation of requirements" (22% of all the combinations). It is obvious that deficient organization and resource management can hamper the implementation of requirements stipulated by regulatory bodies, manufacturers, experts etc. An example can be seen in the Texas City refinery explosion in the US in 2005, in which "deficient design, organization and resource management" was in combination with "deficient implementation of requirements" (Chemical Safety Board, 2013).

The third most frequent combination is "deficient risk assessment – deficient documentation" (21% of all the combinations). Deficient risk assessment may occur in a plant due to lack of procedural risk management strategies in the form of elements of safety management systems being kept and

Table 5 – Occurrence of latent failures.

Year	Deficient regulatory oversight	Deficient risk assessment	Deficient implementation of requirements	Deficient management of change (MOC)	Deficient documentation	Deficient design, organisation or resource management	Unbalanced safety &production goals	Deficient monitoring of performance	Deficient audit	Deficient learning
2000	0	2	2	0	2	6	0	3	0	0
2001	0	4	3	2	4	5	0	2	1	2
2002	0	6	1	2	5	9	0	1	4	2
2003	3	9	7	3	6	12	1	3	1	2
2004	0	7	3	3	2	6	0	2	0	1
2005	1	4	2	1	3	7	1	2	1	1
2006	1	3	2	1	4	3	1	1	1	1
2007	2	3	3	0	1	3	0	1	1	0
2008	0	5	4	2	5	6	0	1	0	3
2009	1	4	2	1	3	3	1	1	0	0
2010	2	5	3	2	2	4	0	0	0	1
2011	3	4	3	0	4	4	0	1	0	2
Total	13	56	35	17	41	68	4	18	9	15

Table 6 – Combinations of latent failures (number of occurrences).

	Deficient documentation	Deficient design, organisation or resource management	Deficient monitoring of performance
Deficient risk assessment	28	48	
Deficient implementation of requirements		30	5
Deficient management of change (MOC)	9		
Deficient monitoring of performance		14	

disseminated through soft or print media. An example can be seen in the explosion of a tank in TDI production unit in Italy in 2002 in which "deficient risk assessment" was in combination with "deficient documentation" (Bureau for Analysis of Industrial Risks and Pollution, 2013).

The fourth most frequent combination is "deficient design, organization and resource management – deficient monitoring of performance" (11% of all the combinations). Deficient monitoring of performance may be influenced by deficient organization (encompassing communication, coordination etc.) and/or by deficient resource management (encompassing poor hiring, poor training, insufficient manning, insufficient motivation etc). An example can be seen in the Texas City refinery explosion in the US in 2005, in which "deficient design, organization and resource management" was in combination with "deficient monitoring of performance" (Chemical Safety Board, 2013).

The fifth most frequent combination is "deficient management of change – deficient documentation" (7% of all the combinations). Deficient management of change (MOC) will most probably occur in the absence of documented MOC procedures necessary to guide the MOC process. An example can be seen in the BP Amoco thermal decomposition incident in the US in 2001, in which "deficient management of change" was in combination with "deficient documentation" (Chemical Safety Board, 2013).

When "deficient risk assessment" occurs, the percentage of it in combination with "deficient design, organization or resource management" is 86%. When "deficient implementation of requirements" occurs, the percentage of it in combination with "deficient design, organization or resource management" is 86%. When "deficient monitoring of performance" occurs, the percentage of it in combination with "deficient design, organization or resource management" is 78%. When "deficient documentation" occurs, the percentage of it in combination with "deficient risk analysis" is 68%. When "deficient documentation" occurs, the percentage of it in combination with "deficient management of change" is 22%. When "deficient monitoring of performance" occurs, the percentage of it in combination with "deficient implementation of requirements" is 28%.

4.5. *Occurrence of accidents in relation to the work process*

According to Table 7, out of the 80 maintenance-related major accidents, "deficient planning/scheduling/failure diagnosis" is the most frequent work-process-based cause (69%). This is followed by "deficient normal operation" (48%), "deficient performance of the maintenance work" (39%), "deficient startup" (13%), "deficient preparation for maintenance" (11%) and the least is "deficient mobilization/shutdown" (9%). Some of the accidents involved several phases of the work process.

4.5.1. *Combinations of work phases*

In Table 8, it is shown that the most frequent combination of causes in relation to the work process is "deficient Planning/scheduling/fault diagnosis – deficient normal operation" (33% of all the combinations). Deficient planning/scheduling/fault diagnosis can lead to an accident directly in the normal operation phase. An example can be seen in the Imperial sugar refinery explosion in the US in 2008, in which "the failure to plan the maintenance of sugar and cornstarch conveying equipment to minimize the release of sugar dust into the work area" *(deficient planning/scheduling/fault diagnosis)* was in combination with "operating in the presence of significant accumulation of sugar dust" *(deficient normal operation)* (Chemical Safety Board, 2013). The second most frequent combination is "deficient planning/scheduling/fault diagnosis – deficient performance of maintenance work" (25% of all the combinations). Situations abound where erroneous plans result in accidents when undetected during the actual performance of the maintenance work in safety-critical operations. An example can be seen in the Partridge-Raleigh oilfield explosion and fire in the US in 2006, in which "deficient planning/scheduling/fault diagnosis" was in combination with "the welding of a piping connection, leading to the accident" (Chemical Safety Board, 2013). The third most frequent combination is "deficient performance of maintenance work – deficient normal operation" (12% of all the combinations). It is also possible to have a work performance phase with failures induced by personnel therein and leading to an accident in the normal operation phase. An example can be seen in the Goodyear heat exchanger and ammonia release incident in the US in 2008, in which "the failure of maintenance workers to reopen an isolation valve" was in combination with "increasing ammonia pressure during process piping cleaning being performed by the operators" (Chemical Safety Board, 2013). Further more, deficient plan may introduce failures in the work performance phase that will manifest during normal operation as an accident. When "deficient planning/scheduling/fault diagnosis" occurs, the percentage of it in combination with "deficient normal operation" is 49%. When "deficient planning/scheduling/fault diagnosis" occurs, the percentage of it in combination with "deficient performance of maintenance work" is 36%. When "deficient planning/scheduling/fault diagnosis" occurs, the percentage of it in combination with "deficient startup" is 13%. When "deficient planning/scheduling/fault diagnosis" occurs, the percentage of it in combination with "deficient preparation for maintenance" is 7%. When "deficient planning/scheduling/fault diagnosis" occurs, the percentage of it in combination with "deficient mobilization/shutdown" is 7%. When "deficient performance of maintenance work" occurs, the percentage of it in combination with "deficient normal operation" is 32%. When "deficient preparation for maintenance" occurs, the percentage of it in combination with "deficient normal operation" is 11%.

Table 7 – Occurrence of accidents in relation to the work process.

Year	Deficient planning/scheduling/fault diagnosis	Deficient mobilization/shutdown	Deficient preparation for maintenance	Deficient performance of maintenance work	Deficient start-up	Deficient normal operation
2000	3	2	1	4	0	3
2001	5	0	0	4	0	1
2002	5	0	1	1	0	7
2003	9	2	1	4	3	5
2004	4	0	3	3	0	5
2005	6	2	0	2	2	4
2006	4	0	0	3	0	2
2007	3	0	0	1	0	3
2008	6	0	0	4	1	5
2009	4	0	0	1	2	1
2010	4	1	2	2	1	1
2011	2	0	1	2	1	1
Total	55	7	9	31	10	38

5. Discussion and recommendations

The main intention in this paper is to identify the most challenging causes of maintenance-related major accidents in the process industries in order to motivate intervention with the most preventive effort. However, potential areas for more usefulness can still be suggested. One of the possible ways in which the outcome of this research may be applied to maintenance management is by adapting it to a process FMEA (Failure Mode and Effect Analysis). A process FMEA is a systematic method that can be used in advance to identify, analyze and eliminate or reduce potential failures from a process (e.g. a maintenance process). It deals with problems emanating from how an item is manufactured, maintained or operated (Rausand and Høyland, 2004). The style of the suggested FMEA is inspired by an application from the healthcare industry (ISMP, 2005; Cohen et al., 1994; Williams and Talley, 1994) where the FMEA is used to investigate medical processes for potential failures and to prevent the failures by correcting the defective processes proactively. We may identify the suggested FMEA as WAP-FMEA (Work and Accident Process Failure Modes and Effects Analysis), i.e. a FMEA which integrates the maintenance work process with the accident process for the purpose of prevention of maintenance related major accidents. Sample worksheets of the suggested WAP-FMEA are illustrated in Table 9.

The illustration of the WAP-FMEA (in Table 9), generally presents a range of possible modes, causes and effects of failure as well as preventive actions in e.g. the maintenance process of an offshore riser system. The list of potential latent causes and work-process related deficiencies were obtained from the observations where they have been linked to different types of active failures. Practically, it is expected that a single failure mode will be treated at a time. The tabulated results in the earlier sections can inform about the probability of failure modes mentioned in Table 9. As regards ranking in order to prioritize preventive efforts, the illustrations in Table 9 indicate a range from highest risk score (corresponding to highest priority) to lowest risk score (corresponding to lowest priority).

Furthermore, the research findings may also find usefulness in maintenance-related, major accident risk modeling applications in the process industries. A typical situation is expressing the likelihood of a particular maintenance-related major accident occurring within a given period. This can be done by using the failure frequency databases of previous similar accidents to establish an annual probability of occurrence (i.e. the statistical probability that the accident will occur during a one-year period) using suitable formulas (Rausand and Høyland, 2004).

Table 8 – Combinations of work phases (number of occurrences).

	Deficient mobilization/shutdown	Deficient preparation for maintenance	Deficient performance of maintenance work	Deficient start-up	Deficient normal operation
Deficient planning/scheduling/fault diagnosis	4	4	20	7	27
Deficient mobilization/shutdown		1	1		
Deficient preparation for maintenance			4		1
Deficient performance of maintenance work				2	10

Table 9 – An illustration of maintenance WAP-FMEA for the prevention of maintenance-related major accidents in an offshore riser system.

Process	Potential failure modes	Potential failure causes			Failure effects that can lead to major accidents	Probability of failure[a]	Severity of failure effects[a]	Risk score[a]	Actions for the elimination or reduction of failure modes
		Accident-process related		Work-process related					
		Active causes	Latent causes						
Maintenance process, e.g. Maintenance processes of an offshore riser system – various preventive, repair, replacement and precommissioning processes	Failure to repair, hydrotest, pig or inspect etc.	Lack of barrier maintenance: absence or insufficiency in update of status of maintenance program and administrative tools	Deficient regulatory oversight, deficient risk assessment, deficient implementation of requirements, deficient documentation, deficient design, organization or resource management, deficient monitoring of performance, deficient learning	Deficiencies in planning/scheduling/fault diagnosis (originating phase of accident), mobilization/shutdown, preparation for maintenance, performance of maintenance work, startup or normal operation (manifestation phase of accident)	Overload, corrosion, material degradation, leak, rupture	0.0249	4 fatalities	0.0996	Review of management policy, audit, etc. Review of the management of resources, information, change etc. Review of maintenance plan/program
	Welding error, parts mismatch, omission of components and incorrect installation, repair or isolation etc.	Barrier maintenance error: procedures, parts or techniques are inappropriate or applied wrongly to barriers	Deficient implementation of requirements, deficient management of change (MOC), deficient documentation, deficient design, organization or resource management, deficient learning	Deficiencies in planning/scheduling/fault diagnosis (originating phase of accident), mobilization/shutdown, preparation for maintenance, performance of maintenance work, startup or normal operation (originating or manifestation phase of accident)	Leak from weld, flange or valve etc.	0.0232	3 fatalities	0.0696	Review of welding procedure specification (WPS), work execution procedure, evaluation of work performance and personnel qualification

	Accumulated ratcheting of bolts in live hydrocarbon piping, presence of maintenance intervention with ignition sources but no flame arrestor	New hazard: the resource being used for maintenance introduces hazards which interact with existing hazards or are triggered by events	Deficient regulatory oversight, deficient risk assessment, deficient implementation of requirements, deficient documentation, deficient design, organization or resource management, deficient monitoring of performance, unbalanced safety &production goals, deficient learning	deficiencies in plan-ning/scheduling/fault diagnosis (originating phase of accident), preparation for maintenance, performance of maintenance work, startup or normal operation (originating or manifestation phase of accident)	Leak from flange or valve and ignition of flammable substances	0.0162	3 fatalities	0.0486	Review of safe operating procedure (SOP), evaluation of work performance, personnel qualification, simultaneous operations (SIMOPS), work permit system
	Loss of containment due to a wrong valve being operated as part of preparations, fire/explosion from maintenance in process area adjacent to riser maintenance area, collision of work-class ROV with riser system	Initiating event: an accidental maintenance related event disrupts a planned maintenance, initiating an accident scenario	Deficient regulatory oversight, deficient risk assessment, deficient implementation of requirements, deficient management of change (MOC), deficient documentation, deficient design, organization or resource management, deficient audit	Deficiencies in plan-ning/scheduling/fault diagnosis (originating phase of accident), mobiliza-tion/shutdown, preparation for maintenance, performance of maintenance work, startup or normal operation (originating or manifestation phase of accident)	Leak, rupture	0.0238	4 fatalities	0.0952	Review of safe operating procedure (SOP), Simultaneous operations (SIMOPS), work permit system or emergency response system

[a] The figures in the columns are arbitrary values for demonstration purpose only. The probability may be determined from the failure frequency, the severity may be defined in terms of the expected damage and the risk score may be defined as the product of the probability and severity ((ISMP, 2005)). The ranking is discussed afterwards.

6. Conclusion

In this paper, 183 major accidents in the hydrocarbon and chemical process industries in the period from 2000 to 2011 have been studied in relation to the Work and Accident Process (WAP) classification scheme (Okoh and Haugen, 2013a). The overall objective has been to look at how maintenance influences major accidents, the trend and the degree and distribution of the causes.

It has been found that out of 183 accidents, 80 (44%) are maintenance-related. Most of the maintenance-related major accidents occurred in chemical manufacturing plants (46%). The most frequently involved hazardous substances are toxic substances (26%) and the most frequent type of accident is "emission/discharge" (60%). "lack of barrier maintenance" (50%), "deficient design, organization and resource management" (85%) and "deficient planning/scheduling/fault diagnosis" (69%) are the most frequent causes in terms of the active accident process, the latent accident process and the work process respectively. As regards combination of causes, "maintenance introduces new hazards – maintenance being an initiating event" (42% of all the active-failure combinations), "deficient risk assessment – deficient design, organization and resource management" (36% of all the latent-failure combinations) and "deficient planning/scheduling/fault diagnosis – deficient normal operation" (33% of all the deficient work-phase combinations) are the most frequent.

The results also show a decreasing trend in maintenance-related major accidents in the period from 2002 to 2007 and that the contributions of the US and Europe to the 80 maintenance-related major accidents are about 40% and 60% respectively.

As regards the applicability of the statistical findings, the frequencies can be used to determine probabilities which in turn will be useful in maintenance-related, major accident risk modeling and in the suggested WAP-FMEA (Work and Accident Process Failure Modes and Effects Analysis), i.e. a FMEA which integrates the maintenance work process with the accident process for the purpose of prevention of maintenance related major accidents. The validity of the statistics, however, is constrained by the uncertainty associated with the assumption that future failures will occur at the same rate being established currently based on previous experience.

References

Bureau for Analysis of Industrial Risks and Pollution, 2013. Detailed sheets. http://www.aria.developpement-durable.gouv.fr/Detailed-sheets-1333.html

Chang, J.I., Lin, C.-C., 2006. A study of storage tank accidents. J. Loss Prevent. Process Ind. 19 (1), 51–59.

Cheng, C.-W., Yao, H.-Q., Wu, T.-C., 2013. Applying data mining techniques to analyze the causes of major occupational accidents in the petrochemical industry. J. Loss Prevent. Process Ind. 26 (6), 1269–1278.

Cohen, M., Senders, J., Davis, N., 1994. Failure mode and effects analysis: a novel approach to avoiding dangerous medication errors and accidents. Hosp. Pharm. 29 (4), 319–330.

Commonwealth of Australia, 2009. Offshore Petroleum (Safety) Regulations 2009. Select Legislative Instrument 2009 No. 382. Tech. rep. Commonwealth of Australia, Canberra.

D.O.E., 2004. DOE Handbook, DOE-HDBK-1100-2004: Chemical Process Hazard Analysis. Tech. rep. US Department of Energy, Washington, DC.

EC, 2005. Guidance on the Preparation of a Safety Report to meet the Requirements of Directive 96/82/EC as amended by Directive 2003/105/EC (Seveso II), Report EUR 22113 EN. Tech. rep. European Commission.

EN 13306, 2010. Maintenance: Maintenance Terminology. Tech. rep. European Committee for Standardization, Brussels.

Fabiano, B., Currò, F., 2012. From a survey on accidents in the downstream oil industry to the development of a detailed near-miss reporting system. Process Saf. Environ. Protect. 90 (5), 357–367.

Hale, A., Heming, B., Smit, K., Rodenburg, F., van Leeuwen, N., 1998. Evaluating safety in the management of maintenance activities in the chemical process industry. Saf. Sci. 28 (1), 21–44.

HSE, 1987. Dangerous maintenance. A study of maintenance accidents and how to prevent them. Tech. rep. Health and Safety Executive, London.

HSE, 1992. A guide to the Offshore Installations (Safety Case) Regulations 1992. Tech. rep. Health and Safety Executive, London.

ISMP, 2005. FMEA of PCA. Tech. rep. Institute for Safe Medication Practices, Horsham, USA http://www.ismp.org/tools/FMEAofPCA.pdf

Kidam, K., Hurme, M., 2013. Analysis of equipment failures as contributors to chemical process accidents. Process Saf. Environ. Protect. 91 (1/2), 61–78.

Kjellen, U., 1984. The deviation concept in occupational accident control – I. Accid. Anal. Prevent. 16, 289–306.

Lortie, M., Rizzo, P., 1999. The classification of accident data. Saf. Sci. 31, 31–57.

Malmén, Y., Nissilä, M., Virolainen, K., Repola, P., 2010. Process chemicals – an ever present concern during plant shutdowns. J. Loss Prevent. Process Ind. 23 (2), 249–252.

NOPSA, 2008. NOPSA Annual report 2007–08. Tech. rep. National Offshore Petroleum Safety Authority, Perth, Australia.

OGP, 2008. Asset integrity – the key to managing major incident risks. Tech. Rep. 415. International Association of Oil and Gas Producers, London.

Okoh, P., Haugen, S., 2013a. Maintenance-related major accidents: classification of causes and case study. J. Loss Prevent. Process Ind. 26, 1060–1070.

Okoh, P., Haugen, S., 2013. The influence of maintenance on some selected major accidents. Chem. Eng. Trans. 31, 493–498, http://dx.doi.org/10.3303/CET1331083.

PSA, 2010. Trends in risk level in the petroleum activity. Tech. rep. Petroleum Safety Authority, Stavanger, Norway.

Rausand, M., Høyland, A., 2004. System Reliability Theory: Models, Statistical Methods, and Applications, 2nd ed. John Wiley & Sons, New Jersey.

Reason, J., 1997. Managing the Risks of Organisational Accidents. Ashgate, Aldershot, UK.

Smith, E.J., Harris, M.J., 1992. The role of maintenance management deficiencies in major accident causation. Proc. Inst. Mech. Eng. E: J. Process Mech. Eng. 206 (15), 55–66.

UK, 1999. The Control of Major Accident Hazards Regulations 1999. Tech. rep. The British Government, London http://www.legislation.gov.uk/uksi/1999/743/regulation/2/made

U.S. Chemical Safety Board, 2013. Completed Investigations. http://www.csb.gov/investigations/completed-investigations/?Type=2

USEPA-OSHA, 1996. MOU Between The United States Environmental Protection Agency, Office of Solid Waste and Emergency Response, Office of Enforcement and Compliance Assurance and The United States Department of Labor, Occupational Safety and Health Administration. http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=MOU&P_id=246

Vinnem, J., Seljelid, J., Haugen, S., Husebø, T., 2007. Analysis of hydrocarbon leaks on offshore installations. In: Vinnem, A. (Ed.), Risk, Reliability and Societal Safety. Taylor & Francis Group, London, pp. 1559–1566.

Williams, E., Talley, R., 1994. The use of failure mode effect and criticality analysis in a medication error subcommittee. Hosp. Pharm. 29 (4), 331–332, 334–336, 339.

Article 4

Is not included due to copyright

Article 4

Maintenance optimization for major accident risk reduction
–Submitted to *Journal of Loss Prevention in The Process Industries*

Article 5

Article 5

The Effect of Maintenance Seen From Different Perspectives on Major Accident Risk

–In *IEEE International Conference on Industrial Engineering and Engineering Management*

The Effect of Maintenance Seen From Different Perspectives on Major Accident Risk

P. I. Okoh, S. Haugen
Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway
(peter.okoh@ntnu.no)

Abstract - **Societies worldwide have been surprised and saddened by the occurrence of certain major unwanted events after having made considerable efforts to control the dynamics of whatever organization or systems they manage. Texas City Refinery Explosion (2005) and the Piper Alpha Disaster (1988) are two examples of maintenance-related major accidents with highly devastating consequences.**

Major accidents may be viewed from the following perspectives: Energy-Barrier, Normal Accident, High Reliability Organization (HRO), Man-made Disaster, Conflicting Objectives, and Resilience Engineering. In reality, few of these perspectives are actually used in practical risk management – it is the energy-barrier principle which is dominating completely.

The objectives of this paper are: (1) To find out how maintenance fits into the aforementioned perspectives on major accidents, and (2) To discuss how the perspectives can influence maintenance.

Keywords - **Maintenance, Major accident, Organization, Risk**

I. INTRODUCTION

Countries and companies have expressed surprises and sadness at the occurrence of major unwanted events that have defied existing controls of organizational and systemic dynamics. In many cases, maintenance has been identified as playing a role in the accidents, directly or indirectly. The Texas City Refinery Explosion (2005) and the Piper Alpha disaster (1988) are just two examples of maintenance-related major accidents with highly devastating consequences. With increasing complexity and increasing dependency on technical systems, the needs for and the importance of maintenance also increases. At the same time, maintenance may also represent a risk, because accidents may be initiated by maintenance itself [1, 2]. A better understanding of how maintenance influences major accident risk is therefore considered to be necessary, to be able to reduce risk.

For this purpose, the term "major accidents" is not defined explicitly but covers accidents which cause severe losses, in terms of loss of life, environmental loss and/or economic losses. The focus of the paper is on major accidents in technological organizations and systems.

Over the years, a number of different views or perspectives have been proposed to explain the phenomenon of major accidents. An overview of different perspectives is provided by Rosness *et al.* [3]. The perspectives that are discussed are the Energy-Barrier model, Normal Accident Theory (NAT), High Reliability Organizations (HRO), the Man-made Disaster (MMD) theory, Conflicting Objectives and Resilience Engineering. The different perspectives may be regarded as "competing," in the sense that they give different explanations of how and why accidents occur. An alternative view is to regard the different perspectives more as supplementary pictures of major accidents, which together may give a more comprehensive understanding of this phenomenon than any single perspective will give. This is also a background for this paper, where we discuss that the choice of perspective may have important implications for how the management of major accident risk is approached. It may therefore also influence our view on maintenance, both as a means to reduce risk and as a cause of accident. It is noted however, that few of these perspectives have had significant influence on practical risk management. The energy-barrier principle dominates completely, although aspects of HRO and resilience are being used in some contexts.

In this paper, we will give a brief overview of the different perspectives, one by one, and provide some comments on how maintenance will be viewed within the different perspectives.

II. ENERGY-BARRIER PERSPECTIVE

A. Energy-barrier perspective

The energy-barrier perspective, which is based on the hazard-barrier-target model of Gibson [4], depicts a linear progression of events from the release of energy (hazard) through supposedly interposed barriers to the interaction between the energy (hazard) and the target (victim). The model is hinged on the concepts of linearity and monocausality, i.e., the transfer of a given energy from the source to the target. This model also forms the basis for Reason's Swiss Cheese Model [1] and the "defence in depth" principle. An example of how this has been institutionalized in risk management can be found in the Norwegian regulations for offshore installations, where a separate section in the Management Regulations is dedicated to barriers [5].

The model basically has three main risk control strategies: (1) Control of the hazard, (2) Control of the barrier, and (3) Control of the target's situation/condition.

978-1-4673-2945-3/12/$31.00 ©2012 IEEE

B. The effect of maintenance

The energy-barrier perspective is about establishing barriers (often technical) and ensuring that these barriers remain intact and effective for as long as they are needed. Maintenance will be an important contributor to maintaining the integrity of the barriers. With this realization, focus on maintenance also increases and maintenance will in itself be a key element in managing risk. In the Norwegian offshore industry, it is quite common to have various safety indicators related to maintenance, in particular maintenance on safety critical equipment. An example is "Hours of backlog on maintenance." Maintenance is also often regarded as a barrier in itself. This perspective will therefore clearly bring out the importance of sufficient and correct maintenance.

III. NORMAL ACCIDENT PERSPECTIVE

A. Normal Accident Theory

The normal accident theory (NAT), proposed by Perrow, expresses the concept of accident proneness (i.e natural tendency towards accidents) owing to the inter-active complexities (technological and organizational) and tight couplings that evolve as our world of technologies continue to expand [6]. The Normal accident perspective is hinged on complexity and multicausality. Perrow believes that the multiple barriers and redundancies that characterize such high-risk technologies (which are being managed on the premise of the energy-barrier model) could offer some level of safety, but will subsequently increase the system's degree of complexity and tightness of couplings. Complexity and coupling are not very precise terms [7], but being able to delay processing time is an example of loose coupling, while the opposite is a tight coupling [6]. According to [8], "as the list of regularities characterizing a given system's operation increases, that system becomes more complex." It can be inferred that the simpler we keep our technologies, the safer we are bound to be, and this is the basis for Perrow's conclusion that certain technologies should be scrapped in their current composition because we cannot think of any organization that has the capacity to sufficiently control them. The reason for this is that Perrow claims that a system of interactive complexity can be effectively controlled only by a decentralized organization and a system of tight couplings can be effectively controlled only by a centralized organization, thus making it impossible to devise an organization that can control the system effectively. The policy reversal in Germany (driven by the Fukushima disaster in Japan) that will see all her nuclear power plants abandoned by 2022 [9] may be seen as a logical and necessary result of NAT.

NAT is not a general theory of major accidents since it is limited to specific technologies, those with high complexity and tight couplings. Further, accidents within such systems need not necessarily be classified as normal accidents either. Perrow himself presents numerous examples of this in his book [6]. Criticism of the theory has been raised [7] and HRO theory (see next section) argues that systems indeed can be both complex and tightly coupled, still having an excellent safety record.

B. The effect of maintenance

Perrow believes that some accidents are preventable through certain improved factors, including better equipment or the effects of accidents may be possible to minimize or limit to local effects through safety systems. In both of these cases, maintenance will play a role in ensuring that the equipment and safety systems are kept in operating order and with high reliability. However, since accidents are associated with complexity and tight coupling, the focus of risk management will be on reducing complexity and also loosening coupling within the system being considered. This has a least two implications.

First of all, regardless of the frequency and quality with which maintenance is performed, it can only contribute to preserve a certain level of safety. Further improvement will not be possible as long as the system has the undesirable properties that Perrow pointed out. Maintenance can therefore serve only as a safeguard for the individual parts of high-risk systems, but not ensure the safety of the whole system. NAT has an organizational perspective and maintenance is therefore not central in the same way as for Energy-Barrier perspective.

Secondly, it may be argued that maintenance can be regarded as adding complexity to a system because it implies more activities that need to be performed safely, coordinated with other activities and monitored in a suitable manner. Maintenance optimization may also add tight couplings.

IV. HIGH RELIABILITY ORGANIZATION (HRO) PERSPECTIVE

A. HRO Theory

The High-Reliability Organization (HRO) Theory has been developed from studies of organizations which, according to Normal Accident Theory, should experience major accidents, but which still have excellent safety records [10]. The foremost example used to illustrate this is aircraft carriers, but other organizations, like hospital emergency rooms, have also been studied. A number of technologies we have today have great productive potential and at the same time great destructive potential, such that the avoidance of a significant failure is imperative [10]. These technologies include the high-risk technologies referred to by Perrow [6] as having interactive complexities and tight couplings, although the

HRO perspective expresses the possibility of managing such technologies unlike Perrow's pessimistic position [3, 11]. An objection to Perrow's pessimism is provided by the HRO perspective in the possibility of switching from centralization during normal operations to decentralization in hazardous situations and consulting expert judgment [11]. According to Sagan [12], HRO organizations inherently possess the best safety records of all high-risk technologies. The characteristics of HROs as identified by several theorists may be summed up in the following: (i) Diligence in failure analysis and organizational learning, (ii) Mutual agreement on production and safety as being concurrent organizational objectives, (iii) Decentralization and centralization of authorities, and (iv) Personnel and technical redundancy [11]. HRO theorists believe that through management commitment to safety, the establishment of safety culture, the maintenance of relatively closed systems, functional decentralization supported by constant training, technical and organizational redundancies, and organizational learning supplemented by anticipation and simulation (trial-and-error process), organizations could achieve the consistency and stability required to support failure-free operations [13, 10, 12, 11].

B. The effect of maintenance

HRO is a theory about organizational aspects that covers all levels of the organization, from top level management (the "blunt end") to the operators performing the work in the field (the "sharp end"). The focus tends to be on high risk operations which require vigilance and correct performance (aircraft carriers, emergency rooms). One may speculate that there is a potential for developing a culture where the "heroes" are those which run the operations, and where maintenance is seen as a routine activity with less importance. On the other hand, at least two of the characteristics listed above – (i) Diligence in failure analysis and organizational learning and (iv) Personnel and technical redundancy – will also be contributing to put focus on maintenance. HRO organizations are proactive in avoiding failures and this should also extend to ensuring good maintenance, to avoid technical failures.

V. MAN-MADE DISASTER PERSPECTIVE

A. Man-made disaster perspective

The man-made disaster (MMD) theory considers accidents to be the result of accumulated flaws in information processing between various organizational units, including the administrative, managerial and operational units [14]. Turner, the initiator of the theory, calls the period of accumulation an incubation period (i.e. a period of maturity). At the end of the incubation period, the perceived organizational quality is unable to co-exist with the accumulated organizational deviations, thus leading to an accident. A key point in this theory is that there exist warning signs within the organization that could have been used to prevent accidents, if it had been accumulated and communicated in the right way and to the right people. This perspective is hinged on multicausality, for according to Turner [14], "accidents are neither chance events, nor acts of God, nor triggered by a few events and unsafe human acts immediately before they occur." The concept behind the theory is sociological; it holds that accidents are not just a technological phenomenon [13].

B. The effect of maintenance

This perspective focuses on lack of information flow as the cause of accidents. The status of technical systems, including their maintenance status would be an example of the type of information that is relevant in this context. This perspective will therefore contribute to emphasize the importance of ensuring that this type of information is available. The Piper Alpha disaster [15] is an example of an accident where information about maintenance was not brought to the attention of all who needed to know. However, maintenance performance as such, and in particular the importance of correct performance of maintenance will not be at the centre of attention in this perspective.

VI. CONFLICTING OBJECTIVES, ADAPTATION AND DRIFT PERSPECTIVE

A. Conflicting objectives perspective

The conflicting objectives/goals (or decision-making) perspective was proposed by Rasmussen [16] and considers major accidents to be the result of organizational objectives clashing with each other. The result of this conflict is an organization in a state of dilemma that may drift over time due to lack of information or inability to balance the objectives correctly. Examples of organizational objectives that may come into conflict include production objectives, safety objectives etc. The basic resource used to drive the realization of these objectives is money and the application of this resource must create a balance between objectives to guarantee the survival of the organization. The balance between production (economic objective) and protection (safety objective) was also discussed by Reason [1]. The concept of adaptation involves tradeoff, i.e. sacrificing one quality or aspect of something in return for gaining another quality or aspect.

B. The effect of maintenance

Maintenance is a clear example of an area where there will be conflicting objectives: The saved cost of not doing it versus the (indirect) risk reduction achieved when doing it. Maintenance objectives are a means of achieving

production and safety objectives, but sometimes the sharing of maintenance resources between production and safety systems may be disproportional, or the allocation of maintenance resources to both may be inadequate. Reducing maintenance is a typical example of a cost that is reduced as much as possible due to pressures to operate as cheaply as possible. Although this may have a positive impact on at least production in terms of profit in the short term, it may tend to have a negative impact on both production and safety in the medium or long term. Optimizing maintenance is crucial to optimizing production without compromising safety. This perspective helps to highlight potential pressures that may exist to reduce maintenance.

VII. RESILIENCE ENGINEERING PERSPECTIVE

A. Resilience engineering perspective

The word "Resilience" is derived from the Latin word "resilire" (to leap back), and according to [17], denotes a system's "ability to recover from challenges or disrupting events." In [11], the term "recoverability" is considered as a synonym for resilience. In [18], resilience is defined as "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions."

Resilience engineering describes the ability of organizations to achieve ultra-high levels of safety and response to the dynamics of other organizational values (e.g. production, operations, economy etc.) despite complexities, high risks, major accidents, disturbances, disruptions, continuous pressure and change [17, 3]. Accidents, according to this perspective, are not the product of normal system malfunction or breakdown, but rather a breakdown in the adaptive capacity necessary to cope with the real world of complexity [13]. According to [8], the ratio between order and chaos is the critical factor in determining the capacity of a system to adapt successfully to systemic surprises. Adaptive capacity (or adaptability) refers to the ability of individuals and organizations to adjust their performance to the current condition [19]. The resilience engineering perspective encompasses core topics from the five perspectives described earlier; it is a synthesis of ideas bordering on barriers, complexity, conflicting goals and HRO [3, 13].

The abilities that constitute resilience can be summarized as follows [20]:

(1) Anticipation – Addressing the potential: Foreseeing the changing shape of risk, before failure and harm results,

(2) Monitoring – Observing the critical: Recognizing how close the organization is to the safety boundary,

(3) Responding – Coping with the actual: Adapting or being flexible to changes, disruptions and opportunities, and

(4) Learning – Updating with the factual: Review of performance based on new knowledge.

B. The effect of maintenance

Since this perspective draws on elements from the earlier perspectives, the conclusions with regard to how maintenance is viewed will also tend to coincide with elements from the earlier discussions, in particular the discussion about HRO Theory. Anticipation and Learning can both be pointed out as abilities that will rely among others on maintenance and maintenance records as a basis for achieving this. Barrier maintenance is part of this, but not any different from the Energy-Barrier perspective. Monitoring is a question of detecting early warnings and weak signals, of which lack of maintenance may be one of such signals.

VIII. CONCLUSION

The purpose of this paper has been to look at how the different perspectives on major accidents that have been proposed over the years will give us different views, and thereby also different insight, into how maintenance influences such accidents. The energy-barrier perspective places focus very clearly on the importance of maintenance as a means of ensuring continued operation and reliability of barriers to prevent accidents, while other perspectives will highlight other aspects. The man-made disaster perspective by Turner shows that performing maintenance is not enough, making sure that the right people have access to information is also important while the conflicting objectives perspective of Rasmussen shows that there will be forces that will tend to reduce maintenance to cut costs (or achieve other objectives).

The focus here has been on maintenance, but a general lesson that can be drawn from this exercise is that none of these perspectives can be regarded as "right" or "wrong." They focus on different aspects of how we manage risk and avoid accidents, and thereby they should all help us, to a smaller or greater degree, to reduce future losses associated with major accidents. Subscribing to just one of them and discarding the others as incomplete, useless, or obsolete will limit our view of the problem area.

The paper is one in a planned series of publications dedicated to a research project titled "Maintenance Strategies for Major Accidents Prevention." Further work related to the paper is planned to involve reanalysis of selected major accidents, with the objective of demonstrating if and how the aforementioned perspectives relate such accidents to the effects of maintenance. Additionally, the extent to which maintenance has been a cause of major accidents could be investigated. Besides, it would be pertinent to analyze how maintenance can contribute to more robust systems and organizations. In addition, it would be interesting to investigate how future operating philosophies may

influence the present state and whether they may create new challenges. Furthermore, there is the need to analyze how maintenance should be optimized to manage the major accident risk.

REFERENCES

[1] Reason, J., "Managing the risks of organisational accidents," Hampshire, 1997.

[2] Haugen, S., Vinnem, J.E., Seljelid, J.: "Analysis of Causes of Hydrocarbon Leaks from Process Plants," SPE paper 140808, SPE Europe HSE Conference, Vienna, February 2011

[3] Rosness et al, "Organisational accidents and resilient organisations: Six perspectives," Revision 2, SINTEF Technology and Society, Trondheim, 2010.

[4] Haddon, W., "The basic strategies for reducing damage from hazards of all kinds," Hazard Prevention, 1980.

[5] Petroleum Safety Authority (Norway): Management Regulations, 2010

[6] Perrow, C., "Normal Accidents: Living with High-Risk Technologies," Princeton University Press, New Jersey, 1984.

[7] Hopkins 1999: The limits of Normal Accident Theory, Safety Science, 32(2-3), 93-102

[8] Gell-Mann, M., "The Quark and the Jaguar: Adventures in the Simple and the Complex," W.H. Freeman and Company, New York, 1994.

[9] BBC, "Germany: Nuclear power plants to close by 2022," URL http://www.bbc.co.uk/news/world-europe-13592208, 2011, accessed on May 5, 2012.

[10] LaPorte, Todd R.; Consolini, P. M., "Working in Practice but Not in Theory: Theoretical Challenges of 'High-Reliability Organizations'," Public Administration Research and Theory 1 (1), 19–47, 1991.

[11] Saleh, J. H.; Marais, K. B.; Cowlagi, R. V., "Highlights from the literature on accident causation and system safety: Review of major ideas, recent contributions, and challenges," Reliability Engineering & System Safety 95, 1105–1116, 2010.

[12] Sagan, S. D., "The Limits of Safety: Organizations, Accidents, and Nuclear Weapons," Princeton University Press, New Jersey, 1993.

[13] Dekker, S., Hollnagel, E., Woods, D., Cook, R., "Resilience Engineering: New directions for measuring and maintaining safety in complex systems," Tech. Rep., Lund University School of Aviation, 2008.

[14] Turner, B. A., "Man-Made Disasters," Wykeham Science Series, London, 1978.

[15] The Hon Lord Cullen: "The public inquiry into the Piper Alpha Disaster," HMSO, 1990

[16] Rasmussen, J., "Risk Management in A Dynamic Society: A Modelling Problem," Safety Science 27 (2/3), 183-213, 1997.

[17] Woods, D., "Resilience engineering: Redefining the culture of safety and risk management," Human Factors and Ergonomics Society Bulletin 49 (12), 1–3, 2006.

[18] Hollnagel, Erik; Paries, Jean; Woods, David D.; Wreathall, J., "Resilience Engineering in Practice: A Guide Book," Ashgate, Surrey, 2011.

[19] Hollnagel, Erik; Woods, David D.; Leveson, N., "Resilience Engineering: Concepts and Precepts," Ashgate, Surrey, 2006.

[20] Johnson, C., Herd, A., "The application of resilience engineering to human space flight for the advancement of space safety," International Association for the Advancement of Space Safety Conference, Huntsville, Alabama, May 2010.

Article 6

Article 6

Improving the robustness and resilience properties of maintenance
–In *Process Safety and Environmental Protection*

Process Safety and Environmental Protection 94 (2015) 212–226

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

Improving the robustness and resilience properties of maintenance

Peter Okoh, Stein Haugen*

Department of Production and Quality Engineering, Norwegian University of Science and Technology, NO 7491 Trondheim, Norway

ABSTRACT

Industries with major accident potential, e.g. the process industries, are usually characterized by high degree of technological and organizational complexity, and hence are fortified with layers of protection (barriers). The energy-barrier risk control model is dominant and tends to be applied by such industries over time, sometimes without paying attention to the vulnerability of the complex organizational setting encompassing production, maintenance, support and the environment. In the same vein, process industries may prioritize production at the expense of safety systems and the organizational network. Maintenance is known to be a key means of keeping safety systems functional, yet, in this paper we wish to explore how its values can be further uncovered to improve the robustness and resilience of the socio-technical system as a whole.

This paper intends to investigate what robustness and resilience properties exist in maintenance and how these can be improved in relation to maintenance interaction with other areas such as production and support and in turn improve the robustness and resilience of the process industries organization. The objective is to improve the robustness and resilience of the organization as a whole. This is realized on the basis of the perspectives of organizational accidents: energy-barrier model, normal accident theory (NAT), high reliability organizations (HRO) theory, man-made disaster (MMD) theory, conflicting objectives, adaptation and drift (COAD) theory and resilience engineering. Based on this, recommendations for improving the maintenance robustness and resilience were proposed.

Keywords: Maintenance; Robustness; Resilience; Organization; Organizational accident; Process industry

1. Introduction

The purpose of maintenance is to retain systems in or to restore them to a functioning state. Maintenance also contributes to improved system knowledge and inter-discipline coordination that may benefit the entire organization. This may indicate that maintenance may be a contributor to robust and resilient organizations and systems whose ability to prevent or limit unexpected events is improved. It is therefore of interest to investigate how maintenance can be performed to gain this "added" value of increased organizational robustness and resilience.

Industries with major accident potential, e.g. the hydrocarbon and chemical process industries, are usually characterized by high degree of technological and organizational complexity (Okoh and Haugen, 2013a,b). It is common practice in such industries to install layers of independent safety barriers that are capable of preventing the occurrence or mitigating the consequences of unexpected events in accordance with the energy-barrier principle (Gibson, 1961).

The energy-barrier principle is dominant among the organizational accident perspectives (Rosness et al., 2010; Okoh and Haugen, 2012) and tends to be applied by high-risk industries over time. Focus is often on technical issues, sometimes without paying attention to the vulnerability of the complex organizational setting encompassing production, maintenance, support and the environment. In the same vein, process industries may prioritize production at the expense of safety systems and the organizational network. This was the case in the Texas City refinery explosion (CSB, 2007; Okoh and

* *Corresponding author*. Tel.: +47 40309367.
E-mail addresses: peter.okoh@ntnu.no, okohpee@yahoo.com (P. Okoh).

Available online 1 July 2014
http://dx.doi.org/10.1016/j.psep.2014.06.014

Haugen, 2014c) and the Macondo blowout (SINTEF, 2011). The safety and production objectives of industries cannot be realized to the fullest without the personnel relating appropriately and adequately with each other, the environment and the systems. The application of a suitable combination (a mix of both the technologically and organizationally biased) of the accident perspectives can improve safety significantly (Pitblado, 2011; Rosness et al., 2010; Okoh and Haugen, 2012).

Several authors have highlighted the importance of maintenance to physical asset management and suggested ways to improve maintenance in relation to improved dependability of the assets (Okoh, 2010; Øien et al., 2010; Wilson, 2002). However, the potential of maintenance to improve the robustness and resilience of the organization itself has yet to be uncovered. The hypothesis is, by virtue of its interaction with the other departments and the environment, maintenance could also improve the robustness and resilience of the organization, not only systems.

Some studies have been done on robustness (Anderies et al., 2004; Nielsen and Holmefjord, 2004; Boissieres and Marsden, 2005; Pavard et al., 2007). Few of them have analyzed organizational robustness in relation to organizational accident (Nielsen and Holmefjord, 2004) or maintenance (Boissieres and Marsden, 2005). The latter focused on the telecommunications industry, whereas the former focused on a hydrocarbon industry's emergency preparedness organization – a subset of the entire industrial organization. However, this paper will explore the process industry organization from a broader perspective. Various industrial sectors are characterized by different configurations of independent and coordinated units aimed at realizing the set of organizational goals. It is important to address this situation specifically to achieve a better solution for a given industry.

In this paper, we intend to investigate what robustness and resilience properties exist in maintenance and how these can be improved in relation to maintenance interaction with other areas such as production and support and in turn improve the robustness and resilience of the process industries organization. The methodology is based on the application of the six perspectives of organizational accidents, i.e. energy-barrier model, normal accident theory (NAT), high reliability organizations (HRO), man-made disaster (MMD) theory, conflicting objectives, adaptation and drift (COAD) theory and resilience engineering (Rosness et al., 2010). Several of the perspectives focus on how accidents are not caused only by technical failures of physical systems, but in some cases by human and organizational factors or a combination of these. Hence, it is pertinent to investigate the maintenance-related contribution to organizational robustness and resilience in light of these factors. The contribution of maintenance to the organizational robustness and resilience will be derived by mapping the factors that influence robustness and resilience (according to each of the organizational accident perspectives) to the links between maintenance and production, maintenance and support, and maintenance and the environment. The paper will focus on the hydrocarbon and chemical process industries.

The rest of the paper is structured as follows: Section 2 will define robustness and resilience and present various views about organizational robustness and resilience from different authors, Section 3 will analyze the structure of the industry and the associated dependencies, Section 4 will describe a maintenance work process applicable to the hydrocarbon and chemical process industries, Section 5 will ascertain whether and what robustness and resilience properties are obtainable from maintenance, Section 6 will investigate how the robustness and resilience of maintenance and the organization can be improved in relation to maintenance interaction with production, support and the environment, and Section 7 will present a summary of the findings.

2. The concept of robustness and resilience

Robustness is the noun form of the English adjective "robust" which originates from the Latin "robustus" – it simply means firm, hard, strong. However, in scientific use there are different definitions of robustness (Jen, 2005), and as yet, there is no universally accepted definition. There may never be a unified definition, because different disciplines may choose to use the term differently, so we have to be careful about choosing definitions from very different applications. Besides, robustness tends to be misconstrued for resilience sometimes (Pavard et al., 2007).

Robust systems, according to Asbjørnslett and Rausand (1999), are characterized by (i) resistance to accidental events, (ii) restoration of functionality and (iii) retention of original stability (Asbjørnslett and Rausand, 1999). This view is consistent with that of Ferdows (1997) – "The ability to cope with changes in the competitive environment without resorting to changes in the structure" (Ferdows, 1997) and that of Chandra and Grabis (2007) – "The ability to withstand external and internal shocks" (Chandra and Grabis, 2007). As viewed by Agarwal et al. (2007), a system is robust if it does not yield to any damage characterized by significant loss of form and function, and even a single mode of vulnerability renders a system unrobust no matter whether the system is acceptable under other kinds of demand (Agarwal et al., 2007). Furthermore, robustness as seen by Pavard et al. (2007) is the ability of a system "to adapt its behavior to unforeseen situations, such as perturbation in the environment, or to internal dysfunctions in the organization of the system" (Pavard et al., 2007).

Resilience as defined by Foster (1993) is "the ability to accommodate change without catastrophic failure, or the capacity to absorb shocks gracefully" (Foster, 1993). According to Asbjørnslett and Rausand (1999), it is characterized by transition to a new stable situation after the unexpected events, and this is consistent with that of Woods (2006a) – a quality encompassing "monitoring the boundary conditions of the current model for competence (how strategies are matched to demands) and adjusting or expanding that model to better accommodate changing demands" (Woods, 2006a). Furthermore, resilience is also seen by several other authors in the following ways:

According to Hollnagel (2011): Resilience is "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions". He points out that the engineering of resilience is dependent on the application and management of "the ability to respond to events, to monitor ongoing developments, to anticipate future threats and opportunities, and to learn from past failures and successes alike".

As stated by Hollnagel and Sundström (2006): "A resilient system, or, organization is able to withstand the effects of stress and strain and to recover from adverse conditions over long time periods".

In the opinion of Paries (2011): Resilience is "a combination of readiness and creativity, and of anticipation and serendipity", implying being prepared both for the expected and the unexpected. He also classifies resilience into two: (1) resilience features designed into a system as a whole and (2) resilience features of the elements or the agents (e.g. human agents) that interact with the system. He views the systemic resilience as emerging from the interaction of individual agents' behavior, and the resilience of the individual agents themselves as being partially influenced by the systemic resilience, emphasizing that the best strategy is a waste if it cannot be implemented by the skillful operators at the "sharp end" of the system. Besides, Paries (2011) suggests a hierarchical "defence in depth" strategy as a means of achieving the combination of anticipation and serendipity, such that a failure in a line of defence activates "a tactical retreat behind the next one, with operating procedures shifting from detailed protocols for normal situations, to a generic action framework for emergency situations."

As indicated by Woods (2011): A resilient system can be seen as a system with the quality of ascertaining whether the current adaptive capacity is enough to meet future demands, implying that an insufficiency of this quality makes the system vulnerable to sudden collapse and failures. He suggests the following as patterns of anticipation: (1) Being "able to recognize that adaptive capacity is falling", (2) being able to identify "the threat of existing buffers and reserves", (3) being "able to recognize when to shift priorities across goal tradeoffs", and (4) being "able to make perspective shifts and contrast diverse perspectives that go beyond their nominal system condition".

In the view of Leveson et al. (2006): Leveson et al. classify resilience into reactive resilience and preventive resilience. According to them, the former involves "the ability to continue operations or recover a stable state after a major mishap or event", whereas the latter involves the "ability of systems to prevent or adapt to changing conditions in order to maintain (control over) a system property".

Quoting from McDonald (2006): "Resilience represents the capacity (of an organizational system) to anticipate and manage risk effectively, through appropriate adaptation of its actions, systems and processes, so as to ensure that its core functions are carried out in a stable and effective relationship with the environment".

On the authority of Wreathall (2006): "Resilience is the ability of an organization (system) to keep, or recover quickly to, a stable state, allowing it to continue operations during and after a major mishap or in the presence of continuous significant stresses". He suggests that financial or other important goals should also be considered in addition to safety which is often focused on.

The African elephant and the hydra can serve the purpose of analogies for robustness and resilience, respectively. The elephant is sturdy enough to bulldoze its way through trees without succumbing to deliberate and accidental impacts – this demonstrates robustness. In the case of a hydra, if the body is bisected horizontally, the upper half will develop a new foot and the lower half will develop a new head (Galliot and Chera, 2010). Being bisected can be seen as an accidental event to the hydra, the bisected state can be seen as an unstable state of the hydra, and the regenerated state consisting of two new hydras can be seen as a new stable state; this is demonstrative of resilience. A hydra with the head and foot both severed will also grow a new head and new foot (Galliot and Chera, 2010), showing a transition from a stable state with a head and a foot both intact, through the interaction with the accidental event (the instance of being cut off), through an unstable state with no head and foot, to a new stable state characterized by regenerated structure – this also demonstrates resilience.

Vulnerability is a key term that is sometimes taken to mean the opposite of robustness or resilience. Hence, it is relevant to delineate vulnerability as well. Vulnerability, in the context of Agarwal et al. (2007), indicates a potential to experience consequence which is disproportionately large compared to the amount of damage or perturbation causing it. However, vulnerability according to Asbjørnslett and Rausand (1999), refers to "the properties of . . .a system that may weaken or limit its ability to endure threats and survive accidental events that originate both within and outside the system boundaries." Similarly, NS 5814:2008 defines vulnerability as "the inability of an object to resist the impacts of an unwanted event and to restore it to its original state or function following the event" (NS5814, 2008). Furthermore, ISO Guide 73:2009 defines vulnerability as "intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence" (ISO, 2009).

Robustness, as applied in this paper, is the ability to resist or counteract accidental events. Furthermore, resilience, as applied in this paper, is about being able to adapt to or recover from accidental events, while stability is acquired in a new state.

In light of the potential for accidental events in the process industries and how the effects can be resisted or counteracted by an organization or how an organization can adapt itself to or recover from them, we can, as will be demonstrated later, investigate maintenance contribution to organizational robustness and resilience by using the various perspectives of organizational or major accidents.

In order to analyze how the robustness and resilience properties of maintenance can be improved in relation to other departments within the process industries, it is necessary to define typical organizational components, their boundaries and how they interact with each other (internal) and with the environment (external). This will be covered in the following section.

3. Organizational composition of the process industries

We may consider the hydrocarbon or chemical process industry as an organization or socio-technical system characterized by "interaction between the technical structure of the system and the social and organizational structure of the operators who run the system" (Boissieres and Marsden, 2005).

The organization can be seen as a system consisting of three elements, i.e. production, maintenance and support Wilson (2002). Fig. 1 depicts the relationships between the various elements of this system and the environment.

According to Fig. 1, the opportunities for maintenance to realize improved robustness and resilience properties within the process industries are shown in the following links: (1) the link between maintenance and production, (2) the link between maintenance and support and (3) the link between maintenance and external forces. The links represent means by which maintenance can interact in harmony with other elements. These relationships at the elemental level

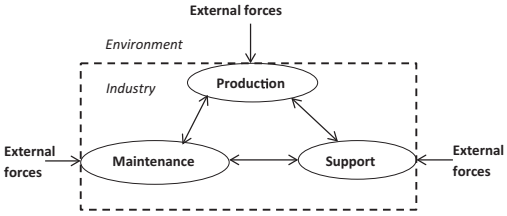


Fig. 1 – A conceptual model of an industrial organization.

will contribute to realizing the organization's goals (Rescher, 2005).

3.1. *The link between maintenance and production*

Maintenance and production are functions whose relationship with each other are critical to the success of a producer organization (Swanson, 1997; Duffuaa, 1995; Jonsson, 1997). A weak link between them can lead to economic loss in repairs and downtime or increased risk to personnel and the environment (Okoh, 2010). Some examples of likely sources of failure include: (i) production staff overusing machines, thus affecting maintainability, (ii) maintenance team not getting data (such as equipment runtime) requested from the production team, (iii) production being in charge of maintenance, and (iv) maintenance staff blaming its ineffectiveness on production not providing adequate budget, accessibility and cooperation.

There is the need for both production and maintenance departments to strive for a common goal – plant profitability. This goal is the basis for continuous existence of both. Maintenance cannot survive in isolation without budget from production and production cannot generate substantial revenue from the customer/market without the guarantee of uptime by maintenance (Duffuaa, 1995). To achieve the production objectives, the maintenance strategy should not necessarily be fixed but depend on the dynamics of the business climate. In order to reduce production cost due to equipment failure, a company may choose to do maintenance optimization or go for renewal. In the same vein, to reduce production cost for other reasons, a company may consider Total Productive Maintenance (TPM), maintainability improvement, etc., which requires cooperation between maintenance, production and/or support (Swanson, 1997). In the case of TPM, there is substantial evidence that it is being applied to a large extent by refineries in Japan and Saudi Arabia (JCCP, 2009a,b, 2012), although the original focus of the method was the manufacturing industry.

In addition, the production and maintenance staff have to cooperate to achieve the organization's safety objective which contributes to the overall business objective. There is the need for the production staff to make adequate preparations for maintenance (Okoh and Haugen, 2014a), e.g. by ensuring that residual hazardous materials are evacuated from equipment to be maintained and by selecting and securing isolation points, and so on (Wallace and Merritt, 2003). Computerized Maintenance Management System (CMMS) and Permit To Work (PTW) systems are some tools that can facilitate coordination and communication between maintenance and production.

3.2. *The link between maintenance and support*

Support for maintenance is critical to the performance of maintenance activities and it constitutes a parameter for measuring the effectiveness of maintenance. It is important for maintenance personnel to be supported also by personnel other than production personnel when called upon, e.g. by Information Technology (IT) personnel. According to EN 13306 (2010), maintenance supportability is "the ability of a maintenance organization to have the correct maintenance support at the necessary place to perform the required maintenance activity when required".

A maintenance support system may consist of (i) sensors on production equipment which help to prevent unplanned downtime by alerting maintenance personnel on time about equipment failure modes, (ii) a computerized maintenance management system (CMMS) which enables maintenance personnel to organize maintenance activities efficiently, (iii) radio frequency identification (RFID) devices which enable ease of identification of spare parts in a store, (iv) electronic permit to work systems (e-PTW) which promotes safety management, and (v) emergency response team for crisis management, and so on. These systems require information technology support to be regularly functional. Supply and logistics are other forms of support for maintenance.

3.3. *External forces on maintenance*

Maintenance performance can be hindered by external forces such as concurrent activities in neighboring sites and severe weather conditions (e.g. winter or arctic conditions), and the negative impact will translate to production and safety limitations. The arctic environment, for e.g. can increase equipment failure rates, failure modes and failure mechanisms, thus necessitating increased diversity and frequency of preventive maintenance in addition to increased frequency of corrective maintenance (Homlong, 2010). Exposure to cold is another factor that is unfavorable to the maintenance crew with its attendant effects on work performance, occupational health and quality (ORIOH, 2001).

Other forms of external forces such as regulatory oversight (e.g. deficiencies in standard/safe operating procedures for maintenance), legislation (e.g. phasing out a given repair technology), disputes (e.g. with environmental activists, host communities, trade unions, etc.), government policies (e.g. exorbitant duties on tools, materials or spare parts), market dynamics (e.g. price fluctuation of tools, materials or spare parts) and technological advancement (e.g. leading to obsolescence of spare parts) can also influence maintenance.

3.4. *Final comment*

In addition to the knowledge of the kind of interactions that exist between maintenance and the other aforementioned units within a process industry organization, it is important to understand the maintenance work process itself since such interactions will actually take place in relation to the various phases of the maintenance work process. Hence, the following section will be used to describe a typical maintenance work process in the process industries.

4. A typical maintenance work process

The maintenance work process in the process industries may vary depending on the situation of the plant, whether the decision to maintain a part of or the whole plant is being taken at the time the item is in service or out of service.

If an item in service requires maintenance, it can be shut down before maintenance or maintenance can be carried out while it is still in service. If an item requires shutdown for maintenance, the organization may follow a maintenance work process as shown in Table 1. If an item is already inoperative, the same process applies except for shutdown.

The phases of the maintenance work process presented in this section can be seen as the various aspects of maintenance that can be influenced by the other organizational units (i.e. production and support) and they will be used as a basis for investigating the improvement of the robustness and resilience properties of maintenance in relation to production and support as will be seen later.

5. Investigating robustness and resilience properties in maintenance

In this section, the intention is to investigate, based on the organizational accident perspectives, what robustness and resilient properties are obtainable from maintenance. The organizational accident perspectives present bases for organizational accident causation. Besides, maintenance is known to be a key contributor to organizational accident prevention. Hence, it is possible for maintenance to possess certain qualities implied in the perspectives by which organizational accidents may be prevented. This is a hypothesis that will be tested in the following. We will first describe the organizational accidents perspectives, analyze their significance to maintenance and then identify the robustness and resilience properties in maintenance.

5.1. *Description of the organizational accident perspectives*

5.1.1. *The energy-barrier perspective*

The energy-barrier perspective, which is based on the hazard-barrier-target model of Gibson (1961), depicts a linear progression of events from the release of energy (hazard) through supposedly interposed barriers to the interaction between the energy (hazard) and the target (victim). The model is hinged on the concepts of linearity and monocausality, i.e. the transfer of a given energy from the source to the target. This model also forms the basis for Reason's Swiss Cheese Model (Reason, 1997) and the "defence in depth" principle. An example of how this has been institutionalized in risk management can be found in the Norwegian regulations for offshore installations, where a separate section in the Management Regulations is dedicated to barriers (PSA, 2010). The model basically has three main risk control strategies: (1) control of the hazard, (2) control of the barrier, and (3) control of the target's situation/condition.

5.1.2. *The normal accident theory (NAT)*

The normal accident theory (NAT), proposed by Perrow (1984), expresses the concept of accident proneness (i.e. natural tendency toward accidents) owing to the interactive complexities (technological and organizational) and tight couplings that evolve as our world of technologies continue to expand (Perrow, 1984). The Normal accident perspective is hinged on complexity and multicausality. Perrow (1984) believes that the multiple barriers and redundancies that characterize such high-risk technologies (which are being managed on the premise of the energy-barrier model) could offer some level of safety, but will subsequently increase the system's degree of complexity and tightness of couplings. Complexity and coupling are not very precise terms (Hopkins, 1999), but being able to delay processing time is an example of loose coupling, while the opposite is a tight coupling (Perrow, 1984). According to Gell-Mann (1994), "as the list of regularities characterizing a given system's operation increases, that system becomes more complex." It can be inferred that the simpler we keep our technologies, the safer we are bound to be, and this is the basis for Perrow's conclusion that certain technologies should be scrapped in their current composition because we cannot think of any organization that has the capacity to sufficiently control them. The reason for this is that Perrow (1984) claims that a system of interactive complexity can be effectively controlled only by a decentralized organization and a system of tight couplings can be effectively controlled only by a centralized organization, thus making it impossible to devise an organization that can control the system effectively. The policy reversal in Germany (driven by the Fukushima disaster in Japan) that will see all her nuclear power plants abandoned by 2022 (BBC, 2011) may be seen as a logical and necessary result of NAT. NAT is not a general theory of major accidents since it is limited to specific technologies, those with high complexity and tight couplings. Further, accidents within such systems need not necessarily be classified as normal accidents either. Perrow himself presents numerous examples of this in his book (Perrow, 1984). Criticism of the theory has been raised (Hopkins, 1999) and HRO theorists argue that systems indeed can be both complex and tightly coupled, still having an excellent safety record.

5.1.3. *High reliability organization (HRO) perspective*

The HRO theory has been developed from studies of organizations which, according to normal accident theory, should experience major accidents, but which still have excellent safety records (LaPorte and Consolini, 1991). The foremost example used to illustrate this is aircraft carriers, but other organizations, like hospital emergency rooms, have also been studied. A number of technologies we have today have great productive potential and at the same time great destructive potential, such that the avoidance of a significant failure is imperative (LaPorte and Consolini, 1991). These technologies include the high-risk technologies referred to by Perrow (1984) as having interactive complexities and tight couplings, although the HRO perspective expresses the possibility of managing such technologies unlike Perrow's pessimistic position (Rosness et al., 2010; Saleh et al., 2010). An objection to Perrow's pessimism is provided by the HRO perspective in the possibility of switching from centralization during normal operations to decentralization in hazardous situations and consulting expert judgment (Saleh et al., 2010). According to Sagan (1993), HRO organizations inherently possess the best safety records of all high-risk technologies. The characteristics of HROs as identified by several theorists may be summed up in the following: (i) diligence in failure analysis and organizational learning, (ii) mutual agreement on production and safety as being concurrent organizational objectives, (iii) decentralization and centralization of authorities, and

Table 1 – Definition of the maintenance work process elements.

Maintenance work process elements	Definition
Planning/scheduling/failure diagnosis	Planning is the organization and documentation of a set of tasks that include the activities, procedures, resources and time scale required to carry out maintenance, whereas scheduling is the predetermined detailing of when a specific maintenance task should be carried out and by who (EN 13306, 2010). Failure diagnosis refers to actions taken for fault detection, fault localization and identification of causes (EN 13306, 2010)
Mobilization/shutdown	Mobilization is the supply, movement and deployment of resources. Shutdown is outage implemented in advance for maintenance, or other purposes (EN 13306, 2010)
Preparation for maintenance work	Provision of required information and applying the requirements (e.g. Permit to work-PTW, Lockout/Tagout-LOTO procedure, hazardous material evacuation, securing of isolation points, etc.) that will enable maintenance to be performed effectively and safely
Performance of the maintenance work	Hands-on actions taken to retain an item in or restore it to a state in which it can perform its required functions
Startup	A state in which a maintained item is being made "live", i.e. the item is being activated or actuated
Normal operation	A state in which an item is in service

(iv) personnel and technical redundancy (Saleh et al., 2010). HRO theorists believe that through management commitment to safety, the establishment of safety culture, the maintenance of relatively closed systems, functional decentralization supported by constant training, technical and organizational redundancies, and organizational learning supplemented by anticipation and simulation (trial-and-error process), organizations could achieve the consistency and stability required to support failure-free operations (LaPorte and Consolini, 1991; Saleh et al., 2010; Sagan, 1993; Dekker et al., 2008).

5.1.4. *Man-made disaster perspective (MMD)*

The man-made disaster (MMD) theory considers accidents to be the result of accumulated flaws in information processing between various organizational units, including the administrative, managerial and operational units (Turner, 1978). Turner (1978), the initiator of the theory, calls the period of accumulation an incubation period (i.e. a period of maturity). At the end of the incubation period, the perceived organizational quality is unable to co-exist with the accumulated organizational deviations, thus leading to an accident. A key point in this theory is that there exist warning signs within the organization that could have been used to prevent accidents, if it had been accumulated and communicated in the right way and to the right people. This perspective is hinged on multicausality, for according to Turner (1978), "accidents are neither chance events, nor acts of God, nor triggered by a few events and unsafe human acts immediately before they occur." The concept behind the theory is sociological; it holds that accidents are not just a technological phenomenon (Dekker et al., 2008).

5.1.5. *Conflicting objectives, adaptation and drift perspective*

The conflicting objectives/goals (or decision-making) perspective was proposed by Rasmussen (1997) and considers major accidents to be the result of organizational objectives clashing with each other. The result of this conflict is an organization in a state of dilemma that may drift over time due to lack of information or inability to balance the objectives correctly. Examples of organizational objectives that may come into conflict include production objectives, safety objectives, etc. The basic resource used to drive the realization of these objectives is money and the application of this resource must create a balance between objectives to guarantee the survival of the organization. The balance between production (economic objective) and protection (safety objective) was also discussed by Reason (1997). The concept of adaptation involves tradeoff, i.e. sacrificing one quality or aspect of something in return for gaining another quality or aspect.

5.1.6. *Resilience engineering perspective*

Resilience engineering describes the ability of organizations to apply the principles of responding, monitoring, anticipating and learning to adapt to or recover from accidental events, while stability is acquired in a new state. The word "resilience" is derived from the Latin word "resilire" (to leap back), and according to Woods (2006b), denotes a system's "ability to recover from challenges or disrupting events." In (Saleh et al., 2010), the term "recoverability" is considered as a synonym for resilience. In Hollnagel (2011), resilience is defined as "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions." Resilience engineering describes the ability of organizations to achieve ultra-high levels of safety and response to the dynamics of other organizational values (e.g. production, operations, economy, etc.) despite complexities, high risks, major accidents, disturbances, disruptions, continuous pressure and change (Rosness et al., 2010; Woods, 2006b). Accidents, according to this perspective, are not the product of normal system malfunction or breakdown, but rather a breakdown in the adaptive capacity necessary to cope with the real world of complexity (Dekker et al., 2008). According to Gell-Mann (1994), the ratio between order and chaos is the critical factor in determining the capacity of a system to adapt successfully to systemic surprises. Adaptive capacity (or adaptability) refers to the ability of individuals and organizations to adjust their performance to the current condition. The resilience engineering perspective encompasses core topics from the five perspectives described earlier; it is a synthesis of ideas bordering on barriers, complexity, conflicting goals and HRO (Rosness et al., 2010; Dekker et al., 2008). The abilities that constitute resilience can be summarized as follows (Hollnagel, 2009, 2011): (1) anticipation – addressing the potential: foreseeing the changing shape of risk, before failure and harm results, (2) monitoring – observing the critical: recognizing how close the organization is to the safety boundary, (3)

Table 2 – Robustness and resilience properties.

Properties	Meanings	Perspectives
Proactivity	Foreseeing what can go wrong and deploying barriers in advance	Energy-barrier, HRO and resilience engineering
Redundancy	Deploying more than one means to a required function	Energy-barrier and HRO
Simplicity	Making the design of organizational interactions simple	Normal accident
Loose couplings	Allowing slacks, variant sequences, alternative means and independent events in organizations	Normal accident
Learning	Reviewing incidents and nearmisses, sharing/updating situation or industry knowledge	HRO and resilience engineering
Decisiveness	Successfully balancing goals, e.g. production-safety goals	Conflicting objectives, adaptation and drift
Communication and coordination	Exchanging information and acting on it harmoniously	Man-made disaster
Emergency response	The quality to readily intervene in accidental events	Resilience engineering
Management of change	Management of organizational-related, operational and environmental changes	Resilience engineering

responding – coping with the actual: adapting or being flexible to changes, disruptions and opportunities, and (4) learning – updating with the factual: review of performance based on new knowledge.

5.2. *The significance of the organizational accident perspectives in relation to maintenance*

5.2.1. *Energy-barrier in relation to maintenance*

The energy-barrier perspective is about establishing barriers (often technical) and ensuring that these barriers remain intact and effective for as long as they are needed. Maintenance will be an important contributor to maintaining the integrity of the barriers. With this realization, focus on maintenance also increases and maintenance will in itself be a key element in managing risk. In the Norwegian offshore industry, it is quite common to have various safety indicators related to maintenance, in particular maintenance on safety critical equipment. An example is "Hours of backlog on maintenance." Maintenance is also often regarded as a barrier in itself. This perspective will therefore clearly bring out the importance of sufficient and correct maintenance.

5.2.2. *NAT in relation to maintenance*

Perrow (1984) believes that some accidents are preventable through certain improved factors, including better equipment or the effects of accidents may be possible to minimize or limit to local effects through safety systems. In both of these cases, maintenance will play a role in ensuring that the equipment and safety systems are kept in operating order and with high reliability. However, since accidents are associated with complexity and tight coupling, the focus of risk management will be on reducing complexity and also loosening coupling within the system being considered. This has at least two implications. First of all, regardless of the frequency and quality with which maintenance is performed, it can only contribute to preserve a certain level of safety. Further improvement will not be possible as long as the system has the undesirable properties that Perrow (1984) pointed out. Maintenance can therefore serve only as a safeguard for the individual parts of high-risk systems, but will not ensure the safety of the whole system. NAT has an organizational perspective and maintenance is therefore not central in the same way as for energy-barrier perspective. Secondly, it may be argued that maintenance can be regarded as adding complexity to a system because it implies more activities that need to be performed safely, coordinated with other activities and monitored in a suitable manner. Maintenance optimization may also add tight couplings.

5.2.3. *HRO in relation to maintenance*

HRO is a theory about organizational aspects that covers all levels of the organization, from top level management (the "blunt end") to the operators performing the work in the field (the "sharp end"). The focus tends to be on high risk operations which require vigilance and correct performance (aircraft carriers, emergency rooms). One may speculate that there is a potential for developing a culture where the "heroes" are those which run the operations, and where maintenance is seen as a routine activity with less importance. On the other hand, at least two of the characteristics listed above – (i) diligence in failure analysis and organizational learning and (iv) personnel and technical redundancy – will also be contributing to put focus on maintenance. HRO organizations are proactive in avoiding failures and this should also extend to ensuring good maintenance, to avoid technical failures.

5.2.4. *MMD in relation to maintenance*

This perspective focuses on lack of information flow as the cause of accidents. The status of technical systems, including their maintenance status would be an example of the type of information that is relevant in this context. This perspective will therefore contribute to emphasize the importance of ensuring that this type of information is available. The Piper Alpha disaster (Cullen, 1990) is an example of an accident where information about maintenance was not brought to the attention of all who needed to know. However, maintenance performance as such, and in particular the importance of correct performance of maintenance will not be at the center of attention in this perspective.

5.2.5. *Conflicting objectives, adaptation and drift in relation to maintenance*

Maintenance is a clear example of an area where there will be conflicting objectives: The saved cost of not doing it versus the (indirect) risk reduction achieved when doing it.

Table 3 – Maintenance contribution to organizational robustness.

Maintenance-related work process	Links	Proactivity	Decisiveness	Learning	Communication and coordination	Simplicity	Loose couplings	Redundancy	Management of change (MOC)	Emergency response
Planning/ scheduling/ failure diagnosis	Between maintenance and production	Joint Job Safety Analysis (JSA) or toolbox meetings prior to inter-departmental related work	Advising on a joint site visit to avoid discrepancies. Joint agreement on guidelines for potential trade-offs that will not create imbalance between business and safety objectives	Joint planning of HSE review meetings, participation in HSE workshops and other related forums	Cooperation on PTW, CMMS, HAZID, safety planning and maintenance/production interface lead	Simplification of production–maintenance interfaces and elimination of bureaucracies in the network between production–maintenance	Putting joint alternative operational plans in place and being tolerant of delays, errors and failures in mutual interaction	Joint agreement on training and keeping standby personnel who are multi-skilled in both production and maintenance regardless of any existing outsourcing policy	Collaboration on any required reorganization process related to operational staff. Joint development of MOC procedure relevant to maintenance–production relations	Joint emergency exercises/drills planning, emergency maintenance planning for deficient safety critical equipment, etc.
	Between maintenance and support	Anticipating the obsolescence of critical items and hence doing timely upgrade	Decisiveness on whom between the user and manufacturer is responsible for deciding on and confirming parts replacement	Training of maintenance staff for the ability to verify critical parts before and after supply	Cooperation on availability of critical maintenance related resources and on e-PTW and CMMS software support	Agreeing on redesign for dependability improvement	Decentralizing the supply of critical resources related to maintenance and allowing some delay in delivery	Keeping redundant suppliers of critical maintenance related resources on vendors list	Development of MOC procedure relevant to maintenance-support relations	Joint emergency exercises/drills planning, emergency maintenance planning for deficient emergency response equipment, etc.
	Between maintenance and the environment	Optimizing maintenance to mitigate the effects of adverse environmental conditions	Adaptability of maintenance to installations' host communities	Training of maintenance staff for contingency management	Maintenance of communication channels with the environment and exchange of information	Reduce complexity in maintenance in relation to concurrent activities in neighboring sites	Decentralizing maintenance for speedy response to effects from external forces so as to mitigate losses		Development of MOC procedure relevant to maintenance-related environmental changes	Emergency maintenance planning to prevent or mitigate the effects of unsafe environmental conditions

Table 3 (*Continued*)

Maintenance-related work process	Links	Proactivity	Decisiveness	Learning	Communication and coordination	Simplicity	Loose couplings	Redundancy	Management of change (MOC)	Emergency response
Mobilization/ shutdown	Between maintenance and production	Pre-mobilization inspection and awareness on likelihood of residual process chemicals	Joint agreement on partial or total shutdown	Ensure real-time supervision for hazardous on-the-job training	Cooperation on hazard control at shutdown. Use of PTW, HAZID, checklist, etc.			If bypassing redundant safety systems, apply suitable safety alternative	Applying changes specified by MOC procedure	Agreeing on shutting down to limit state of emergency, etc.
	Between maintenance and support								Applying changes specified by MOC procedure	
	Between maintenance and the environment	Warning third parties off hazardous activities and work areas			Cooperation with host community by paying attention to culture-sensitive issues being raised				Applying changes specified by MOC procedure	Performing emergency maintenance to prevent or mitigate the effects of unsafe environmental conditions
Preparation for maintenance work	Between maintenance and production	Identifying and securing isolation points, and evacuation of hazardous materials	Joint agreement on optimal isolation and advising against unmanning of control rooms	Ensure real-time supervision for hazardous on-the-job training	Cooperation on use of PTW, checklists, HAZID tools, etc.			If bypassing redundant safety system, apply suitable safety alternative	Applying changes specified by MOC procedure	
	Between maintenance and support								Applying changes specified by MOC procedure	Joint emergency exercise/drill execution

Maintenance objectives are a means of achieving production and safety objectives, but sometimes the sharing of maintenance resources between production and safety systems may be disproportional, or the allocation of maintenance resources to both may be inadequate. Reducing maintenance is a typical example of a cost that is reduced as much as possible due to pressures to operate as cheaply as possible. Although this may have a positive impact on at least production in terms of profit in the short term, it may tend to have a negative impact on both production and safety in the medium or long term. Optimizing maintenance is crucial to optimizing production without compromising safety. This perspective helps to highlight potential pressures that may exist to reduce maintenance.

5.2.6. *Resilience engineering in relation to maintenance*

Since this perspective draws on elements from the earlier perspectives, the conclusions with regard to how maintenance is viewed will also tend to coincide with elements from the earlier discussions, in particular the discussion about HRO theory. Anticipation and learning can both be pointed out as abilities that will rely among others on maintenance and maintenance records as a basis for achieving this. Barrier maintenance is part of this, but not any different from the energy-barrier perspective. Monitoring is a question of detecting early warnings and weak signals, of which lack of maintenance may be one of such signals.

Furthermore, according to Grote (2011), tools that support the assessment and promotion of the basic requirements for resilience (i.e. responding, monitoring, anticipating, and learning) encompass "training emergency management, handling fatigue of system operators, supporting preventive maintenance, providing better rules for managing conflicting goals, or improving incident reporting".

5.3. *Prevention of drift*

Hale and Heijer (2006), like Leveson et al. (2006), also recognize two aspects of resilience: prevention of loss of control over risk and recovery from that loss of control. Based on Rasmussen's model (Rasmussen, 1997) which explains the concept of drift to failure, Hale and Heijer (2006) define the former aspect of resilience as "the ability to steer the activities of an organization so that it may sail close to the area where accidents will happen, but always stays out of that dangerous area" (Hale and Heijer, 2006). This, according to them (Hale and Heijer, 2006), implies knowing where an organization stands in relation to the danger area and activating efficient and effective response when indications of impending or actual danger are detected. Drifting into failure, itself, as explained by (Dekker, 2006), is "a metaphor for the slow, incremental movement of systems operation toward (and eventually across) the boundaries of their safety envelope" (Dekker, 2006).

One way of preventing maintenance-related drift is by avoiding maintenance postponement of safety-critical elements. An instance where postponement could be forced on maintenance is when a company wants to continue production to satisfy a time-based demand of a customer rather than lose the order to its competitors. If this happens repeatedly, the company will continue to drift toward the edge/boundary of their safety envelope and eventually experience an accident.

Drift is also indicative in accumulated errors in maintenance-related decision making, e.g. accumulated

Table 4 – Maintenance contribution to organizational robustness.

Maintenance-related work process	Links	Proactivity	Decisiveness	Learning	Communication and coordination	Simplicity	Loose couplings	Redundancy	Management of change (MOC)	Emergency response
Performance of the maintenance work	Between maintenance and production	Use of Job Hazard Analysis	Joint agreement on substituting a part with a non-original one	Ensure real-time supervision for hazardous on-the-job training	Cooperation on hazard control during the maintenance phase. Use of PTW, checklists, HAZID, etc. Reject unmanning of control rooms			If bypassing redundant safety systems, apply suitable safety alternative	Applying changes specified by MOC procedure	
	Between maintenance and support								Applying MOC procedure	
	Between maintenance and the environment	Warning third parties off hazardous activities and work areas			Cooperation with host community by paying attention to culture-sensitive issues being raised				Applying changes specified by MOC procedure	Performing emergency maintenance to prevent or mitigate the effects of unsafe environmental conditions
Startup	Between maintenance and production	Doing Pre-Startup Safety Review (PSSR)	Joint agreement on optimal deisolation. Advising against unmanning of control rooms	Ensure real-time supervision for hazardous on-the-job training	Cooperation on use of PTW, HAZID, checklists, etc.			If bypassing redundant safety systems, apply suitable safety alternative	Applying changes specified by MOC procedure	
	Between maintenance and support								Applying changes specified by MOC procedure	

	Between maintenance and the environment	Warning third parties off hazardous activities and work areas			Cooperation with host community by paying attention to culture-sensitive issues being raised			Applying changes specified by MOC procedure	Performing emergency maintenance to prevent or mitigate the effects of unsafe environmental conditions
Normal operation	Between maintenance and production	Use of Job Hazard Analysis	Joint agreement on on-line maintenance procedure. Advising against unmanning of control rooms	Ensure real-time supervision for hazardous on-the-job training	Cooperation on use of PTW, HAZID, checklist, etc.		If bypassing redundant safety systems, apply suitable safety alternative	Applying changes specified by MOC procedure	
	Between maintenance and support							Applying changes specified by MOC procedure	
	Between maintenance and the environment	Warning third parties off hazardous activities and work areas			Cooperation with host community by paying attention to culture-sensitive issues being raised			Applying changes specified by MOC procedure	Performing emergency maintenance to prevent or mitigate the effects of unsafe environmental conditions

errors in P–F (potential failure–functional failure) interval determination, critical spare parts management, maintenance task selection or maintenance interval determination. This can be prevented by using effective maintenance management tools.

The potential of maintenance to expose its personnel to major hazard facilities and to introduce new hazards, new failures and initiating events for accident scenarios will increase with increasing frequency (i.e. reducing interval) of maintenance. This implies an increasing annual risk (i.e. probability of fatality per hour × maintenance duration in hours × number of maintenance intervals in a year × number of personnel exposed) and a drift to failure. A way to prevent this is to optimize maintenance intervals in terms of risk with the objective of minimizing the maintenance-related major accident risk.

5.4. *Final comment*

Based on the aforementioned analysis, we have identified and defined some maintenance-related robustness and resilience properties in relation to the organizational accident perspectives and these are shown in Table 2.

6. How the robustness and resilience of maintenance and the organization can be improved

In Tables 3 and 4, the steps in the maintenance process have been combined with the organizational properties associated with resilience and robustness. For each step and each property, it has been evaluated whether the maintenance process can contribute to strengthen the property. As far as possible, concrete examples/suggestions have been provided.

In the following three subsections, some examples from Tables 3 and 4 are brought out and briefly presented.

6.1. *Between maintenance and production*

The maintenance unit can pursue improvements in the following: (1) proactivity to risk management in maintainable production systems, (2) decisiveness in discouraging risky imbalances between maintenance and production, (3) a learning culture that promotes safety in maintenance of hazardous production systems, (4) communication and coordination between maintenance and production staff in the maintenance work process of safety-critical production systems, (5) simplicity in maintenance planning, procedures and organization in relation to safety-critical production systems (Okoh and Haugen, 2014b), (6) looseness of couplings in maintenance organization to tolerate shortcomings in production organization, (7) organizational and technical redundancy for safety-critical production systems, (8) management of change related to alterations in the maintenance–production network, and (9) emergency preparedness and response to accidental events arising from maintenance–production interactions. Some of these and more examples are presented in Tables 3 and 4.

6.2. *Between maintenance and support*

The maintenance unit can pursue improvements in the following: (1) proactivity to management of obsolescence of critical parts, (2) decisiveness in confirming the responsible party for critical part replacement between maintenance and external technical support, (3) learning on critical part verification, (4) communication and coordination for technical support via server-based maintenance management systems, (5) simplicity of maintenance support systems, e.g. maintenance-related cyber-physical systems, (6) looseness of couplings in relation to fault tolerance of e.g. computerized maintenance management systems, (7) organizational redundancy in relation to suppliers of critical parts, (8) management of change with respect to alterations in the maintenance-support network, and (9) emergency preparedness in conjunction with the dedicated emergency response department. These feature more prominently in the planning/scheduling/failure diagnosis phase of the maintenance work process as shown in Table 3.

However, in the other phases of the maintenance work process, one tends to see more of the adaptability of maintenance to support, through the application by the maintenance unit, of the management of change (MOC) procedure related to both. This is also shown in Tables 3 and 4.

6.3. *Between maintenance and the environment*

The maintenance unit can pursue improvements in the following: (1) proactivity to management of unsafe environmental conditions arising during maintenance, e.g. through maintenance optimization in relation to dynamic grouping of maintenance activities (Wildeman et al., 1997), (2) decisiveness in adapting maintenance operations to the livelihood of the host community, e.g. through diligent waste management and site reinstatement efforts, (3) learning on keeping a conducive working environment, (4) communication and coordination on weather forecast and cultural issues related to the host community, (5) simplicity in maintenance operations in relation to concurrent activities in neighboring areas, (6) looseness of couplings with respect to decentralizing maintenance for speedy response to hazardous effects from environmental forces, (7) management of change (MOC) procedure relevant to maintenance-related environmental changes, and (8) emergency maintenance to prevent or mitigate the effects of sudden environmental hazards. Some of these and more examples are presented in Tables 3 and 4.

The contents of Tables 3 and 4 represent some recommended best practices that will serve as opportunities for maintenance to contribute to the robustness and resilience of the process industry organization. Some of the recommendations are peculiar to a given phase of the maintenance work process, whereas others necessarily cut across some phases.

7. Conclusion

This paper is one among several intended to give more insight into how to make the best out of maintenance in the process industries. The direction in this paper has been focused on what robustness and resilience properties exist in maintenance and how these can be improved in relation to maintenance interaction with other areas such as production and support and in turn improve the robustness and resilience of the process industries organization. Over time, maintenance has been a proven contributor to the robustness of the physical systems in the industries, but whether maintenance can also contribute to the robustness and resilience of the organization had yet to be investigated. Hence, the hypothesis

that maintenance can also improve organizational properties that influence the ability to resist or counteract accidental events as well as the ability to adapt and recover from such events had to be investigated. This would enable us to see whether there is a possibility of developing new knowledge for the exploitation of additional maintenance values.

The fact that robustness can be seen as the ability to resist or counteract accidental events motivated the use of the various perspectives of organizational accidents (i.e. energy-barrier model, normal accident theory (NAT), high reliability organizations (HRO), man-made disaster (MMD) theory, conflicting objectives, adaptation and drift (COAD) theory and resilience engineering theory) as bases for the investigation. Besides, some of these perspectives have explained that accidents are not caused only by technical failures of physical systems, but in some cases by human and organizational factors or a combination of these.

The contribution of maintenance to organizational robustness and resilience, based on the improvement of the robustness and resilience properties of maintenance, were derived by mapping robustness and resilience properties (based on the accident perspectives) to the maintenance work process (i.e. Planning/scheduling/failure diagnosis, mobilization and shutdown, preparation for maintenance work, performance of the maintenance work, startup and normal operation) and the links between maintenance and production, maintenance and support, and maintenance and the environment. A given industry was considered as a triplet organization consisting of the maintenance unit, the production unit and the support unit all in contact with the environment.

It has been shown in this paper how maintenance can improve robustness and resilience in organizations. The operational links between maintenance and each of the other elements (i.e. production, support and the environment) possess the potential for additional robustness and resilience to the organization. The links represent means by which maintenance can interact in harmony with other units for the purpose of improving organizational robustness and resilience. As supported by Rescher (2005), such harmonious relationships at the elemental level will contribute to realizing the organization's goal. Recommendations to the maintenance management of process industries for strengthening these links in order to achieve added robustness and resilience have also been proposed.

References

Agarwal, J., Blockley, D.I., Woodman, N.J., 2007. Vulnerability of systems. Civil Eng. Environ. Syst. 18, 141–165.

Anderies, J.M., Janssen, M.A., Ostrom, E., 2004. A framework to analyze the robustness of social-ecological systems from an institutional perspective. Ecol. Soc. 9 (1).

Asbjørnslett, B., Rausand, M., 1999. Assess the vulnerability of your production system. Prod. Plan. Control 10 (3), 219–229.

BBC, 2011. Germany: Nuclear Power Plants to Close by 2022. http://www.bbc.co.uk/news/world-europe-13592208

Boissieres, I., Marsden, E., 2005. Organisational factors of robustness. In: Proceedings of the 2nd International ISCRAM Conference, Brussels, pp. 117–122.

Chandra, C., Grabis, J., 2007. Supply Chain Configuration: Concepts, Solutions, and Applications, 1st ed. Springer, New York.

CSB, 2007. Investigation Report, Refinery Explosion and Fire (15 Killed, 180 Injured), BP, Texas City, Texas, March 23, 2005. Report No. 2005-04-I-TX. Tech. Rep. U.S. Chemical Safety Board, Texas.

Cullen, L., 1990. The Public Inquiry into the Piper Alpha Disaster, Vols. 1 and 2 (Report to Parliament by the Secretary of State for Energy by Command of Her Majesty, November 1990). Tech. Rep. Her Majesty's Government, London.

Dekker, S., 2006. Resilience engineering: chronicling the emergence of confused consensus. In: Hollnagel, E., Woods, D.D., Leveson, N. (Eds.), Resilience Engineering: Concepts and Precepts. Ashgate, Surrey, pp. 77–92 (Chapter 7).

Dekker, S., Hollnagel, E., Woods, D.D., Cook, R., 2008. Resilience Engineering: New Directions for Measuring and Maintaining Safety in Complex Systems, Tech. Rep. November. Lund University School of Aviation.

Duffuaa, S.O., 1995. Maintenance and quality: the missing link. J. Qual. Maint. Eng. 1 (1), 20–26.

EN 13306, 2010. Maintenance: Maintenance Terminology. Tech. Rep. European Committee for Standardization, Brussels.

Ferdows, K., 1997. Making the most of foreign factories. Harv. Bus. Rev., 73–88.

Foster, H.D., 1993. Resilience theory and system evaluation. In: Wise, J.A., Hopkin, V.D., Stager, P. (Eds.), Verification and Validation of Complex Systems: Human Factors Issues. Springer, Berlin, pp. 35–60.

Galliot, B., Chera, S., 2010. The Hydra model: disclosing an apoptosis-driven generator of Wnt-based regeneration. Trends Cell Biol. 20 (9), 514–523.

Gell-Mann, M., 1994. The Quark and the Jaguar: Adventures in the Simple and the Complex. W.H. Freeman and Company, New York.

Gibson, J.J., 1961. The contribution of experimental psychology to the formulation of the problem of safety-a brief for basic research. Behav. Approaches Accid. Res., 77–89.

Grote, G., 2011. Reviews for resilience engineering in practice. In: Hollnagel, E., Paries, J., Woods, D.D., Wreathall, J. (Eds.), Resilience Engineering in Practice: A Guidebook. Ashgate, Surrey.

Hale, A., Heijer, T., 2006. Defining resilience. In: Hollnagel, E., Woods, D.D., Leveson, N. (Eds.), Resilience Engineering: Concepts and Precepts. Ashgate, Surrey, pp. 35–40 (Chapter 3).

Hollnagel, E., 2009. Safety Culture, Safety Management, and Resilience Engineering. Tech. Rep. MINES ParisTech, Paris http://www.atec.or.jp/Forum_09_Hollnagel.pdf

Hollnagel, E., 2011. Prologue: the scope of resilience engineering. In: Hollnagel, E., Paries, J., Woods, D.D., Wreathall, J. (Eds.), Resilience Engineering in Practice: A Guidebook. Ashgate, Surrey.

Hollnagel, E., Sundström, G., 2006. States of resilience. In: Hollnagel, E., Woods, D.D., Leveson, N. (Eds.), Resilience Engineering: Concepts and Precepts. Ashgate, Surrey, pp. 339–346 (Chapter 21).

Homlong, E., 2010. Reliability, Availability, Maintainability and Supportability Factors in an Arctic Offshore Operating Environment: Issues and Challenges. Stavanger (Ph.D. Thesis).

Hopkins, A., 1999. The limits of normal accident theory. Safety Sci. 32, 93–102.

ISO, 2009. ISO Guide 73:2009 – Risk Management – Vocabulary. International Organization for Standardization, Geneva.

JCCP, 2009a. Customized Program in Japan on "Maintenance & Safety Management" for Saudi Aramco. Tech. Rep. Japan Cooperation Center, Petroleum, Tokyo.

JCCP, 2009b. Seminar on "Refinery Maintenance Management and TPM" Held at Saudi Aramco's Ras Tanura Refinery. Tech. Rep. Japan Cooperation Center, Petroleum, Tokyo.

JCCP, 2012. CPO Seminar on Total Productive Maintenance Management (TPM) Held Jointly with Saudi Aramco. Tech. Rep. Japan Cooperation Center, Petroleum, Tokyo http://www.jccp.or.jp/english/wp-content/uploads/cpo_tpm_saudi-aramco.pdf

Jen, E., 2005. Stable or robust? What's the difference? In: Jen, E. (Ed.), Robust Design: A Repertoire of Biological, Ecological and Engineering Case Studies. Oxford University Press, Oxford, p. 7 (Chapter 1).

Jonsson, P., 1997. The status of maintenance management in Swedish manufacturing firms. J. Qual. Maint. Eng. 3 (4), 233–258.
LaPorte, T., Consolini, P., 1991. Working in Practice but Not in Theory: Theoretical Challenges of High-Reliability Organizations. Publ. Admin. Res. Theory 1 (1), 19–47.
Leveson, N., Dulac, N., Zipkin, D., Cutcher-Gershenfeld, J., Carroll, J., Barrett, B., 2006. Engineering resilience into safety-critical systems. In: Hollnagel, E., Woods, D.D., Leveson, N. (Eds.), Resilience Engineering: Concepts and Precepts. Ashgate, Surrey, pp. 95–123 (Chapter 8).
McDonald, N., 2006. Organisational resilience and industrial risk. In: Hollnagel, E., Woods, D.D., Leveson, N. (Eds.), Resilience Engineering: Concepts and Precepts. Ashgate, Surrey, pp. 155–180 (Chapter 11).
Nielsen, L., Holmefjord, A.,2004. How to design a robust emergency preparedness organisation for offshore drilling. In: The Seventh SPE International Conference on Health, Safety, and Environment in Oil and Gas Exploration and Production. Society of Petroleum Engineers, Calgary, pp. 1–4.
NS5814, 2008. NS 5814: Requirements for Risk Assessment, Norwegian ed. Standard Norge, Oslo.
Øien, K., Schjølberg, P., Meland, O., Leto, S., Spilde, H., 2010. Correct maintenance prevents major accidents. MaintWorld, 26–28.
Okoh, P., 2010. Maintenance Concept Database Solution (MCDS). Norwegian University of Science and Technology (NTNU), Trondheim (Master Thesis). http://ntnu.diva-portal.org/smash/record.jsf?pid=diva2:427941
Okoh, P., Haugen, S.,2012. The effect of maintenance seen from different perspectives on major accident risk. In: IEEE International Conference on Industrial Engineering and Engineering Management. IEEEXplore, Hong Kong, pp. 917–921.
Okoh, P., Haugen, S., 2013a. Maintenance-related major accidents: classification of causes and case study. Loss Prev. Process Ind. 26, 1060–1070.
Okoh, P., Haugen, S., 2013b. The influence of maintenance on some selected major accidents. Chem. Eng. Trans. 31, 493–498, http://dx.doi.org/10.3303/CET1331083.
Okoh, P., Haugen, S., 2014a. A study of maintenance-related major accident cases in the 21st century. Process Safety Environ. Prot, http://dx.doi.org/10.1016/j.psep.2014.03.001.
Okoh, P., Haugen, S., 2014b. Application of inherent safety to maintenance-related major accident prevention on offshore installations. Chem. Eng. Trans. 36, 175–180, http://dx.doi.org/10.3303/CET1436030.
Okoh, P., Haugen, S., 2014c. The implication of maintenance in major accident causation. Loss Prev. Bull. (236), 11–14.
ORIOH, 2001. Risk Assessment and Management of Cold Related Hazards In Arctic Workplaces: Network of Scientific Institutes Improving Practical Working Activities. Tech. Rep. Oulu Regional Institute of Occupational Health (ORIOH), Oulu.
Paries, J., 2011. Resilience and the ability to respond. In: Hollnagel, E., Paris, J., Woods, D.D., Wreathall, J. (Eds.), Resilience Engineering in Practice: A Guidebook. Ashgate, Surrey, pp. 1–8, 9–27 (Chapter 1).
Pavard, B., Dugdale, J., Saoud, N.B.B., Darcy, S., Salembier, P., 2006. Design of Robust Socio-Technical Systems. Resilience Engineering, Juan les Pins, France, http://www.resilience-engineering-association.org/download/resources/symposium/symposium-2006%282%29/Pavard_et_al_R.pdf
Perrow, C., 1984. Normal Accidents: Living with High-Risk Technologies. Princeton University Press, NJ.
Pitblado, R., 2011. Global process industry initiatives to reduce major accident hazards. J. Loss Prev. Process Ind. 24 (1), 57–62.
PSA, 2010. Management Regulations. Tech. Rep. Petroleum Safety Authority, Stavanger, Norway.
Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. Safety Sci. 27 (2/3), 183–213.
Reason, J., 1997. Managing the Risks of Organisational Accidents. Ashgate, Aldershot, UK.
Rescher, N., 2005. Cognitive Harmony: The Role of Systemic Harmony in the Constitution of Knowledge. University of Pittsburgh Press, Pittsburg http://digital.library.pitt.edu/cgi-bin/t/text/text-idx?idno=31735062136340;view=toc;c=pittpress
Rosness, R., Grøtan, T., Guttormsen, G., Herrera, I., Steiro, T., Størseth, F., Tinmannsvik, R., Wærø, I., 2010. Organisational Accidents and Resilient Organisations: Six Perspectives, Revision 2 Edition. SINTEF Industrial Management, Trondheim.
Sagan, S.D., 1993. The Limits of Safety: Organizations, Accidents, and Nuclear Weapons. Princeton University Press, NJ.
Saleh, J., Marais, K., Cowlagi, R., 2010. Highlights from the literature on accident causation and system safety: review of major ideas, recent contributions, and challenges. Reliab. Eng. Syst. Safety 95, 1105–1116.
SINTEF, 2011. The Deepwater Horizon accident: Causes, Lessons Learned and Recommendations for the Norwegian Petroleum Activity. Tech. Rep. SINTEF Society and Technology, Trondheim.
Swanson, L., 1997. An empirical study of the relationship between production technology and maintenance management. Int. J. Prod. Econ. 53, 191–207.
Turner, B.A., 1978. Man-Made Disasters. Wykeham Science Series, London.
Wallace, S., Merritt, C., 2003. Know when to say 'when': a review of safety incidents involving maintenance issues. Process Safety Prog. 22 (4), 212–219.
Wildeman, R.E., Dekker, S., Smit, A., 1997. A dynamic policy for grouping maintenance activities. Eur. J. Oper. Res. 99 (3), 530–551.
Wilson, A., 2002. Asset Maintenance Management: A Guide to Developing Strategy and Improving Performance, 1st ed. Industrial Press Inc., New York.
Woods, D.D., 2006a. Essential characteristics of resilience. In: Hollnagel, E., Woods, D.D., Leveson, N. (Eds.), Resilience Engineering: Concepts and Precepts. Ashgate, Surrey, pp. 21–34 (Chapter 2).
Woods, D.D., 2006b. Resilience engineering: redefining the culture of safety and risk management. Hum. Factors Ergon. Soc. Bull. 49 (12), 1–3.
Woods, D.D., 2011. Resilience and the ability to anticipate. In: Hollnagel, E., Paries, J., Woods, D.D., Wreathall, J. (Eds.), Resilience Engineering in Practice: A Guidebook. Ashgate, Surrey, pp. 121–125 (Chapter 9).
Wreathall, J., 2006. Properties of resilient organisations: an initial view. In: Hollnagel, E., Woods, D.D., Leveson, N. (Eds.), Resilience Engineering: Concepts and Precepts. Ashgate, Surrey, pp. 275–285 (Chapter 17).