Accident precursors : pro-active identification of safety risks in the chemical process industry

Accident precursors:
pro-active identification of safety risks in the chemical process industry

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de
Technische Universiteit Eindhoven, op gezag van de
Rector Magnificus, prof.dr. R.A. van Santen, voor een
commissie aangewezen door het College voor
Promoties in het openbaar te verdedigen
op 22 maart 2004 om 16:00 uur

door

Patrick Maria Wilhelmus Körvers

geboren te Hunsel

Dit proefschrift is goedgekeurd door de promotoren:

prof.dr.ir A.C. Brombacher
en
prof.dr.ir. H.J. Pasman

copromotor:
dr.ir. P.J.M. Sonnemans

CIP-DATA LIBRARY TECHNISCHE UNIVERSITEIT EINDHOVEN

Körvers, Patrick M.W.

Accident precursors: pro-active identification of safety risks in the chemical process industry / by Patrick Maria Wilhelmus Körvers. – Eindhoven: Technische Universiteit Eindhoven, 2004. – Proefschrift.

ISBN 90-386-1868-9
NUR 952

Keywords: reliability / safety management / accident analysis / operational control processes / chemical industry

Technische Universiteit Eindhoven, 2004
Press: Universiteitsdrukkerij, Technische Universiteit Eindhoven

PREFACE

This thesis is the result of my assignment as a research assistant in the department of Technology Management of the Technische Universiteit Eindhoven. I would like to use this opportunity to thank those who have in one way or another contributed to my work.

First of all I would like to thank my supervisors, Aarnout Brombacher and Hans Pasman, who provided me with the opportunity to conduct this research and always stimulated me by their enthusiasm. Secondly, I would like to thank Peter Sander and Tjerk van der Schaaf for their various critical comments during the final stage of this research, spurring the improvement of this thesis. I am also grateful to Trevor Kletz, Dimitrios Karydas, Henk Leegwater, Joop Halman, and Theo Logtenberg for participating in the dissertation committee. Finally, my special thanks goes to my 'co-promoter,' Peter Sonnemans. Without the talks about life, food, drinks, the numerous lectures in which he encouraged and expressed his believe in me, and his help and companionship during the entire project, this thesis would never have been finished, thanks Peter.

Furthermore, I would like to thank all the people from the department of industrial safety of TNO-MEP in Apeldoorn and TNO who initiated this research in the first place. Especially I would like to thank the following people who were involved in this research during my two year stay and many visits to Apeldoorn; Theo Logtenberg, Piet van Beek, and Johan Reinders.

For reasons of confidentiality, I am unable to mention the names of the organizations that supported the case studies, though the people involved I can thank, especially; Stefan Arts, Aad Brouwer, Jaap de Bruin, Marcel Schreudergoedheijt, Ad Simoen, and Geert van Uden. Without their help this research would not have been possible. This also applies to the master students, who helped me collecting, building and testing the ideas in practice; Michiel van den Goolberg, Pieter de Mulder, Loes Achten and Roland de Smit.

For the 'academic diner sessions' in Apeldoorn, Amersfoort, or Eindhoven, I would like to thank Gerrit Kroon and Lex Stax. They always listened to me and provided me with ideas and encouraged me to proceed. For the discussions during lunch and morning coffee, I would like to thank my colleagues from the Quality of Products & Processes (PPK) Section in the department of Technology Management.

For reading and correcting the first versions of this thesis I would like to thank Jan Rouvroye and again Theo Logtenberg. My special thanks for reading and correcting this thesis and especially polishing up my English goes to Bill Dryden and his wife Doris, who I can't thank enough for all their efforts made during the final stages.

Finally, for still believing in me I would like to express my thanks to my parents, family, friends, and especially to my girlfriend Melanie, who always fully encouraged and supported me wherever possible.

SUMMARY

Despite the many safety indicators and measures deployed in today's chemical process industry, accidents still occur. This thesis was prompted by the need to understand the background of this problem. Research shows that these accidents are not usually caused by one single factor, but more often by a combination of factors related to technical, human, and organizational domains. Understanding these factors is important, but deriving related pre-warning signs may be even more important as armed with this knowledge it is not only possible to understand accidents but also to pro-actively prevent them. Therefore, the aim of this thesis is to establish relationships between pre-warning signs and potential accidents and pro-actively intervene to prevent the corresponding accidents.

The first goal and research question of the research described in this thesis relates to the existence of such pre-warning signs (called 'precursors') resulting in the question: do precursors exist? However, even with identified precursors, accidents will still occur as long as the actual root causes, responsible for these precursors, are not properly addressed in the corresponding (business) process. Therefore, the second research question was formulated as: what are the root causes of the precursors, in terms of the underlying (business) process. When both questions have been answered, a better understanding can be obtained of why accidents still exist in spite of the existing precursors. This is the subject of the third research question. Finally, the last intriguing research question automatically arises: how to combine the precursors and root causes in such a way that accidents can be pro-actively identified and prevented.

To obtain an answer to the research questions posed, pro-active safety indicators used in today's chemical process industry were analysed and the deviations upon which they are based were compared with deviations present in the accident trajectories of 70 recent accidents. By comparing these two sets of deviations, it was observed that although re-occurring deviations with no 'direct' perceived safety related consequences were present in the majority of accident trajectories they were never-the-less not addressed by the commonly used pro-active safety indicators. These so-called 'indirect' perceived safety related deviations may therefore be more important indications of a possible accident than was thought previously.
Based on the results of the analysis the first research question could be answered affirmative. Precursors (defined as re-occurring deviations in an operational process) do exist and can often be obtained from everyday quality, maintenance and reliability data.

The answer to the second question was obtained by using models from organizational control theory. A deviation can re-occur due to ineffective operation of the organization's control process. A theoretical model of this control process, in which causes of precursors can be expressed in terms of ineffective control elements of the organization's control process, was derived from existing models in literature. However, as safety literature shows, there are certain conditions shaping a situation that make these control elements ineffective. These conditions, sometimes called 'latent conditions' in safety literature are the actual root causes of precursors and possible accidents. In this thesis a classification has been developed which identifies six main types of latent conditions (these six latent conditions are context related but

general enough to identify them in different organizations). This answers the second research question by explaining the existence of the root causes of the corresponding precursors in terms of latent conditions. Thus explaining the complete chain of the existence of precursors and how the corresponding accidents can evolve through the deteriorating effect of the latent conditions and precursors on the existing safety barriers.

With the developed concepts, a number of field experiments were conducted in the chemical process industry. A first experiment was carried out in a small company in The Netherlands. From this first trial, it was evident that the concepts of precursors, the model of the organisational control process and the structure of these concepts had to be adapted to obtain better and more reliable results. The improvements led to the development of a structured protocol of seven clearly defined stages. By applying this 7-stage protocol to the data of the small company, safety risks could pro-actively be identified and the accidents which the company had already experienced, could be explained.
To verify the developed concepts underlying the structured 7-stage protocol in a reactive way, they were applied to an analysis of recent accidents in the Dutch chemical process industry. Despite the limitations in the information available from the accident database, it could be deduced that all accidents were preceded by precursors, and even that similar precursors had led to similar accidents, implying that companies had failed to learn from these re-occurring deviations which were in fact pre-warning signs of impeding accidents.
Moreover, while analysing the accidents and their precursors it was shown that often accidents are inadvertently caused by the higher control levels (i.e. the tactical and strategic level) in organizations, as had already been observed in the first experiment of the small company. The second experiment reconfirmed the strength of the developed 7-stage protocol.

To finally verify the 7-stage protocol pro-actively, three case studies were carried out in the Dutch chemical process industry, where the 7-stage protocol was applied. From the results it was shown how different decisions, especially on the higher organizational control levels led to situations in which several safety barriers were negatively affected, clearing the way for an accident to occur. The answer to the third question was derived from these case studies: actors, although familiar with the daily re-occurring deviations, do not recognise these precursors as pre-warning signs of accidents. In this way, precursors and their underlying latent conditions are ‘allowed’ to exist and degrade the safety barriers. Consequently, an accident will evolve if all available safety barriers are breached.
The case studies revealed a lack of overview regarding precursors, their underlying organizational root causes (the latent conditions) and their possible effects on safety barriers. This lack of overview created the opportunity for safety risks in the operational process, despite the presence of many safety indicators and measures.

In conclusion, and answering the final question, this research demonstrates that the developed 7-stage protocol can explicitly and pro-actively indicate safety risks and help organizations to direct their resources to improve safety, which includes their control structure (their normal way of working), effectively.

SAMENVATTING

Ondanks het feit dat er binnen de huidige chemische industrie een grote hoeveelheid aan veiligheidsindicatoren en maatregelen gebruikt wordt, gebeuren er nog steeds ongevallen. Dit proefschrift richt zich op de diepere oorzaken van dit probleem. Onderzoek toont aan dat ongevallen gewoonlijk niet veroorzaakt worden door één enkele factor, maar door een combinatie van factoren in het technische, menselijke en organisatorische domein. Het begrijpen van deze factoren is belangrijk, maar door naar gerelateerde waarschuwingssignalen voorafgaande aan een ongeval te zoeken, ontstaat er niet alleen meer inzicht in het voortraject van ongevallen, maar ook in mogelijkheden om deze te voorkomen. Daarom is het doel van dit proefschrift het leggen van relaties tussen waarschuwingssignalen en mogelijke ongevallen. Dit om uiteindelijk ongevallen te voorkomen.

De eerste onderzoeksvraag beschreven in dit proefschrift refereert aan het bestaan van mogelijke waarschuwingssignalen, precursors genaamd. De vraag is als volgt geformuleerd: is het mogelijk het bestaan van precursors te bewijzen? Zouden deze precursors werkelijk bestaan, dan zullen ongevallen nog steeds blijven voorkomen als de werkelijke oorzaken, die medeverantwoordelijk zijn voor het ontstaan van de precursors, niet worden aangepakt in het bedrijfsproces. Daarom luidt de tweede onderzoeksvraag: wat zijn de oorzaken van precursors in termen van het bedrijfsproces? De beantwoording van beide onderzoeksvragen leidt tot de derde onderzoeksvraag: waarom komen ongevallen nog steeds voor ondanks de aanwezigheid van precursors? Tenslotte is er een vierde onderzoeksvraag welke automatisch voorvloeit uit de vorige vragen: hoe kan met behulp van precursors en onderliggende oorzaken, een potentieel ongeval daadwerkelijk worden aangeduid en voorkomen?

Om de onderzoeksvragen te beantwoorden is er eerst gekeken naar de bestaande veiligheidsindicatoren in de chemische industrie. De onderliggende verstoringen waar deze indicatoren op gebaseerd zijn, zijn vervolgens vergeleken met de verstoringen die voorafgaand aanwezig waren bij 70 recent gebeurde ongevallen. Bij het vergelijken van deze twee sets van verstoringen, bleek dat herhaalde verstoringen, waarvan men denkt dat deze geen directe gevolgen voor de veiligheid hebben, in de meeste gevallen mede verantwoordelijk zijn voor een ongeval, maar niet meegenomen worden door de huidige veiligheidsindicatoren. Gebaseerd op de resultaten van de analyse, is hiermee de eerste onderzoeksvraag positief beantwoord. Precursors van ongevallen (gedefinieerd als herhaalde verstoringen in het operationele proces) bestaan en zijn vaak terug te vinden in gegevens die betrekking hebben op de kwaliteit, onderhoud en betrouwbaarheid van de operationele processen.

Het antwoord op de tweede onderzoeksvraag is verkregen door modellen uit de organisatorische controle (= beheersings-) theorie te halen. Een verstoring herhaalt zich doordat de organisatie zijn processen niet goed beheerst. Er wordt een, uit de bestaande literatuur bekend, theoretisch organisatorisch beheersmodel gebruikt, waarin oorzaken van precursors worden uitgedrukt in ineffectieve beheerselementen. Er zijn echter, zoals de veiligheidsliteratuur laat zien, condities die een situatie creëren waaronder het organisatorische beheerselement ineffectief is. Deze condities, ook wel latente condities genoemd, zijn de werkelijke oorzaken van precursors en daarmee van mogelijke ongevallen. In dit proefschrift is er een onderscheid gemaakt in 6 typen

latente condities, welke gerelateerd zijn aan het organisatorische beheersmodel en daarmee enerzijds context specifiek, maar anderzijds ook generiek genoeg zijn om ze in verschillende organisaties aan te kunnen treffen. Hiermee is de tweede onderzoeksvraag beantwoord. Ook wordt een verklaring gegeven voor de situatie waarin een ongeval tot stand komt. De latente condities tasten samen met de precursors aanwezige veiligheidsbarrières in een organisatie aan en maken zo de weg vrij voor een ongeval.

Met de ontwikkelde concepten zijn een aantal veldexperimenten uitgevoerd in de chemische procesindustrie. Een eerste experiment werd in een klein Nederlands chemisch bedrijf uitgevoerd. Hieruit bleek dat de concepten precursor en organisatorische beheersmodel, alsmede de samenhang ertussen, aangepast moest worden om meer betrouwbare en betere resultaten te verkrijgen. Dit leidde tot de ontwikkeling van een gestructureerd protocol bestaande uit zeven expliciete stappen. Door dit 7-stappen protocol toe te passen op de data van het eerste experiment, konden er vooraf veiligheidsrisico's worden geïdentificeerd en de ongevallen die in het verleden hadden plaatsgevonden worden verklaard.
Om de concepten van het 7-stappen protocol te valideren is een tweede experiment uitgevoerd, waarin achteraf gekeken is waardoor bepaalde ongevallen in de Nederlandse chemische industrie zijn veroorzaakt. Ondanks de beperkte data konden er in alle gevallen precursors worden onderscheiden. Uit het experiment bleek zelfs dat bij één en hetzelfde bedrijf dezelfde precursors bij herhaling voorafgingen aan (vrijwel) identieke ongevallen. Dit betekent dat bedrijven niet leren van de herhaalde verstoringen zijnde waarschuwingssignalen voor mogelijke ongevallen.
Verder kwam naar voren dat de ongevallen in veel gevallen hun oorsprong vonden in de hogere organisatorische beheersingsprocessen (op het tactisch en strategisch niveau) binnen een organisatie, wat in overeenstemming is met de resultaten uit het eerste experiment.

Om het 7-stappen protocol 'definitief' te valideren is het protocol ten slotte toegepast op drie case studies in de Nederlandse chemische industrie. Hieruit bleek hoe verschillende beslissingen, vooral in de hogere organisatorische beheersingsprocessen, leiden tot situaties waarin verscheidene veiligheidsbarrières negatief beïnvloed worden, om zo de weg voor een ongeval vrij te maken. Het antwoord op de derde onderzoeksvraag volgt uit de resultaten van deze drie cases: de cases bevestigden dat mensen herhaalde verstoringen wel zien, maar deze niet erkennen als mogelijke precursors voor een op handen zijnde ongeval. Daardoor worden de latente condities niet gezien en samen met de precursors blijven ze bestaan, waardoor veiligheidsbarrières ineffectief worden en er uiteindelijk een ongeval optreedt.
De case studies lieten zien dat er een gebrek was aan een overzicht van precursors, hun onderliggende organisatorische oorzaken (de latente condities) en de effecten op de veiligheidsbarrières. Hierdoor is het mogelijk dat er bepaalde veiligheidsrisico's blijven bestaan in het operationele proces, ondanks de grote hoeveelheid aan veiligheidsindicatoren en maatregelen.

Ten slotte, en hiermee is tevens de laatste onderzoeksvraag beantwoord, heeft dit onderzoek laten zien dat het ontwikkelde 7-stappen protocol expliciet en tijdig veiligheidsrisico's kan aanduidden. Organisaties kunnen zo hun middelen effectief inzetten om de veiligheid met behulp van het organisatorische beheersingsproces (dagelijkse manier van werken) te verbeteren.

TABLE OF CONTENTS

ACRONYMS AND DEFINITIONS

accidents	Unexpected sudden sequences of events, with undesired outcomes inflicting damage to people, property and/or the environment.
active failures	failures made by those in the *operational process*, that result into *deviations*.
ALARP	As Low As Reasonably Possible
BRZO	Besluit Risico Zware Ongevallen (Dutch): Dutch Seveso II directive
control process	The process that adapts to the environment by regulating *deviations* to reach the desired outcome set by the *organizational values and norms*.
deviation	A transformation or its input, output, or resource which deviates from the present *espoused theory* and/or the individual's image of the transformation's *theory-in-use*.
double loop learning	A way of regulating in a *control process* by questioning the *organizational values and norms*, to correct the *deviations* and to reach the desired outcome set by the *organizational values and norms*.
espoused theory	The prescribed way people should act in an organization.
FACTS	Failure and ACcidents Technical information System
F&EI	Fire & Explosion Index
GFT	General Failure Type
HAZOP	HAZard and OPerability
HRO	High Reliability Organizations
HSE	Health & Safety Executives
IEC	International Electrotechnical Commission

incidents	The combined set of *accidents* and *near misses*.
intervention	An element in the *control process*, situated behind the *judgement* element. Its purpose is to intervene in the input, resources or output of a transformation according to the *organizational values and norms*.
IRMA	Integrated Risk Management Audit
judgement	An element in the *control process*, situated behind the *observation* element and before the *intervention* element. Its purpose is to determine if an observed *deviation* is serious enough to intervene or not according the *organizational values and norms*.
latent condition	Conditions removed in time and space from the *deviations* in the *operational process*, creating conditions for *active failures* to be made.
LTI	Lost Time Injury
MIR based SLM	Maturity Index on Reliability based Safety Lifecycle Management
MORT	Management Oversight and Risk Tree
MTC	Medical Treatment Case
near miss	A sequence of events which is prevented from developing further into undesired outcomes inflicting damage to people, property and/or the environment.
observation	An element in the *control process*, situated before the *judgement* element. Its purpose is to monitor if the transformation and that the output of the transformation are according to the *organizational values and norms*.
operational control level	The *control process* of the *operational process*.
operational process	The process that consists of the *primary* and the parts of the *secondary process* directly interacting with the *primary process*, e.g. maintenance, internal transportation, etc.

organizational values and norms	The rule-governed ways of deciding, delegating and setting boundaries of an organization present in an *espoused theory* and a *theory-in-use*.
OSHA	Occupational Safety & Health Administration
PHA	Process Hazard Analysis
precursors	Pre-warning signs of accidents, which are defined as re-occurring *deviations* in an *operational process*.
primary process	The process responsible for realising the primary output or function needed to satisfy the environment, e.g. products, goods, or services.
PRISMA	Prevention and Recovery Information System for Monitoring and Analysis
PSM	Process Safety Management
SADT	Structured Analysis and Design Technique
safety barrier	Technical, human, or organizational functions that are able to arrest an *accident/incident* evolution so that the next event in the chain will not be realised.
SAM	Systems, Actions, Management
SCHAZOP	Safety Culture HAZard and OPerability
secondary process	The process responsible for taking care of the resources.
SI	Safety Indicator
single loop learning	A way of regulating in a *control process* by changing the strategies and assumptions made from the *organizational values and norms*, to correct the observed deviation and to reach the desired outcome set by the *organizational values and norms*.
SMS	Safety Management System
steering	An element in the *control process*, which provides the *organizational values and norms* to the other elements in the *control process*.

strategic control level	The *control process*, providing the steering for the *tactical control level*.
SOP	Standard Operating Procedure
tactical control level	The *control process*, receiving the *steering* from the *strategic control level* and providing the steering for the *operational control process*.
tertiary process	See *control process*.
theory-in-use	The actual way individuals act in an organization.
TNO	Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek (Dutch): Netherlands organization for Applied Scientific Research
WPAM	Work Process Analysis Model

Chapter 1

INTRODUCTION

The research described in this thesis deals with safety management in complex and high-risk organizations. Companies in the chemical process industry handling hazardous substances are chosen as the subject of study. In particular this thesis will focus on the current safety indication process, and how this safety indication process works and its shortfalls. An unreliable indication process, leads automatically to wrong reactions and measures to prevent possible accidents. Increased understanding of this process helps in providing a better basis from which effective measures to prevent accidents can be derived.
This Chapter starts with an example of an actual accident, that occurred in spite of all the measures and indicators implemented to prevent it from happening. Subsequently, some important safety concepts are defined to prevent confusion and misinterpretations. Then it is discussed why in spite of the developments in safety scope and environment since the industrial revolution measuring safety is still a problem. The Chapter ends by presenting the research scope and the derived research questions.

1.1 Setting the scene

On September 25th, 1998 an accident occurred at a gas plant in Longford, Australia, killing two men, injuring eight others and cutting Melbourne's gas supply for two weeks, Hopkins (Hopkins, 2000). The incorrect operation of a bypass valve caused a failure of the warm oil pumps. This led to a metal heat exchanger becoming super cold and therefore brittle. When operators restarted the warm oil flow, the heat exchanger fractured, allowing a large volume of gas to escape and ignite. Following standard industry practice, the gas plant used lost-time injury (LTI) frequency rate, as the principal indicator for safety performance. In terms of this indicator their record was enviable. The LTI statistics from 1990 to 1998 was well ahead of the industry average and the plant had won an industry award for its performance, Smith (Smith, 1997).
In addition to the excellent LTI statistics, several other safety measures and indicators were in place. The company had collected a high numbers of near misses, which was one of the issues management was constantly emphasizing in toolbox meetings. The company had operated for six months without any recordable injuries, and many major risk reduction projects had been initiated. A prioritizing system based on safety matters had been introduced, to resolve the problems of a backlog of maintenance orders. A management committee assessed the items waiting to be repaired according to their effect on safety, environment, or production. If one of these three factors was involved, the item was given priority over all other items.
Moreover, several internal, external, and corporate audits showed and confirmed the positive picture indicating that the safety management system at the gas plant was performing above average. Nevertheless, despite Longford's excellent safety record on September 25th, 1998 the tragic accident occurred.

This sketch briefly addresses the problem that many companies in the chemical process industry are currently dealing with regarding safety. In spite of the various kinds of safety measures and indicators used, major catastrophes still occur. In this example, all the indicators and measures implemented showed an excellent safety performance compared to other companies. So why did this accident still occur in spite of all the outstanding indicators? Were there no signs indicating that an accident was on its way? What was wrong with the safety measures and indicators that they didn't predict the accident?

In literature these problems can be recognised, Hale (Hale et al., 1998) indicates that finding adequate performance indicators is the fundamental difficulty of all safety science research. Pidgeon (Pidgeon et al., 2000) concluded that all the difficult questions, surrounding attempts to translate findings from accidents into proper theoretical frameworks to inform safety management up-front, are yet to be resolved. However, Hale (Hale et al., 1998) indicated that the field of safety management research is still young and especially needs empirical evidence that links the organization to safety performance. To take these observations and conclusions in current literature and practice into account, the focus of this thesis will lie on developing effective safety performance indicators in organizations handling hazardous substances. Applying the knowledge from existing literature into practice will develop these indicators. The scientific foundations for this thesis will therefore not only be retrieved by using scientific literature but also by empirical evidence in the form of accident analyses (case histories) and multiple case studies.

Before elaborating on the insights on safety indicators derived during the past years by research in the field of safety science, some basic concepts generally used in this field are clarified to prevent possible misinterpretation.

1.2 Safety concepts defined

Before scientifically sound research can be performed on a subject, clear definitions must be set. Although, this may seem a logical step, Osborn (Osborn et al., 1988) highlighted that this has been a stumbling block for research in safety science since its inception. Definitions of concepts like accidents, incidents, near misses, risk, and safety, are known in the field of safety science, but interpreted differently in various situations. Unclear and ambiguous definitions lead to misinterpretations and confusion and must be avoided. Therefore, some general concepts used in safety science and the definitions used in this thesis are discussed in this Section. In the remainder of this thesis specific concepts will be defined where appropriate and can also be found in a list of acronyms and definitions presented in the beginning of this thesis.

1.2.1 Safety and risk

Stating a definition of safety is often overlooked in safety research, and the concept of safety is not as obvious as it may seem, often being associated merely with the absence of risk. Literature contains many different definitions of risk (see for different examples of definitions Adams (Adams, 1995) Lees (Lees, 1996), IEC 61508 (IEC 61508, 2000)). The IEC (IEC 61508, 2000), defines risk as a combination of the probability of an occurrence of harm and the severity of this harm. Harm is

subsequently defined as physical injury or damage to the health of people either directly, or indirectly as a result of damage to property or to the environment. Determination of risk can be made by questioning three factors; event, likelihood and consequences:

What can go wrong? (event)
What is the probability of occurrence? (likelihood)
What are the consequences? (consequences)

However, all three questions are subjective to those who are asked to give an answer to the questions. Risk is thus relative to the observer and also has to do with both likelihood and consequences, Kaplan (Kaplan, 1981). There are multiple and varied understandings of risk and the concept that each individual chooses to adopt is subject to various value judgements and interpretations. No single definition of risk can claim to be universal. Risk means different things to different people and may be better understood as 'risk perception'. Therefore, risk is not defined in one dimension. Unambiguously defining which combinations of likelihood and consequences of an event have a higher risk than the other combinations of both dimensions, is not possible. Therefore, a standard of acceptable risk is not exclusively determined by the current state of the art in technology, but also by the desires and aspirations of the individual and of society, Pasman (Pasman et al., 2003). In this thesis, risk is taken to includes two dimensions that of likelihood and consequences, and is expressed as: risk (event) = (likelihood, consequences), see Chapter 3. However, in Chapter 5 risk has to be expressed in only one dimension. To overcome this dilemma, the definitions from current literature are considered and applied.

Safety may be defined as the absence of risk and can also be expressed as the inverse of risk, i.e. the lower the risk the higher the safety. Based on this relationship, it is justified to use either one. Moreover, safety is context specific, for example: In the street safety means; walking around without being assaulted by people. Whilst in traffic safety means: driving your car without being involved in a car accident.

In this research, the main focus is safety in a chemical company handling hazardous substances. The risks of accidents or other events during processes involving hazardous substances (flammable, toxic, or explosive) or activities where extreme conditions are used (like high/low pressures or high/low temperatures), are subject of this research. Process safety is the absence of risk from events with these hazardous substances and activities with extreme conditions. Non-process safety or process risk is often measured by accidents, incidents and near misses and this concept will be discussed in the following sub-Section.

1.2.2 Accidents, incidents and near misses

The concept of accident and incident are commonly used in safety research, but because various definitions of these concepts exist it is important to state them here. Accident and incident are both defined as unexpected sudden sequences of events with undesired outcomes, inflicting damage to people, property and/or the environment. The short duration of the onset distinguishes accidents and incidents (sudden events) from 'health' and industrial diseases like asbestosis, etc.

Like risk, accidents and incidents are context specific concepts, which are subjective, and strongly depend on people's perceptions. The difference between incidents and accidents is that accidents are the outcome of an incident or series of incidents having 'high' consequences. Therefore, incidents can develop into an accident according to van der Schaaf (Schaaf van der, 1991), who also recognizes an intermediate state as a near miss. He defines a near miss as a situation in which an ongoing sequence of events is prevented from developing further into an event with 'high' consequences. He combined the concepts of near miss, incident, and accident, as depicted in Figure 1, van der Schaaf (Schaaf van der, 1992). Incidents are in this respect the combination of near misses and accidents. Figure 1 shows that an organization may prevent dangerous situations from developing into an accident by various measures and tools (defences). If these defences are not adequate, the situation develops into an event with 'low' perceived consequences (incident). From here on it is often the operator who may adequately recover the situation, which means the incident, becomes a near miss. However, if no adequate recovery takes place, the incident will be able to develop into an event with 'high' perceived consequences (accident).

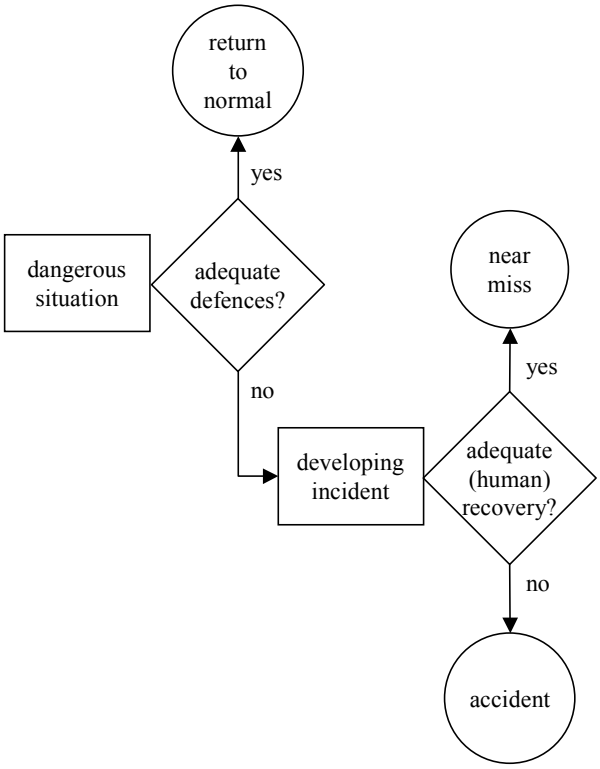


Figure 1 *A model for incidents, accidents, and near misses, van der Schaaf (Schaaf van der, 1992)*

Having set the fundamental concepts in safety research (i.e. safety, risk, accident, incident, near miss), the history and current status of the field of safety measurement will be discussed.

1.3 Safety scope and environment during the past

Having set the fundamental definitions in the field of safety research, this Section discusses how the determination of safety indicators developed over time, and why it is still possible for accidents to happen in the chemical process industry.

The first sub-Section deals with: the history of indicating safety, how the scope of research evolved, and how research into safety provides new insights and continuous improvement in indicating the safety performance of an organization. The last sub-Section discusses the influence of the changing environment on the way safety is indicated nowadays.

1.3.1 History and change of scope

Since industrialization, and the first boiler explosions in the early 1900s, authorities have put obligations on the management of the companies to prevent accidents from inflicting damage and especially injuries to people. The number of accidents were measured and the mandatory technical inspections from the authorities gave an indication of how well safety was controlled. However, until 1930 the policies were only aimed at improving the physical conditions of the technical installations. In this first engineering era, as Reason (Reason, 1991) calls it, the focus was for a reduction in the number of accidents only by technical safeguards. With the first scientific studies of accidents beginning in the 20th century, the unsafe acts of people were also considered, particularly in the mid-1960s, Hale (Hale et al., 1998). This second age was the human error era, as Reason (Reason, 1991) calls it. In addition to the technical inspections, psychologists tried to explain the human errors made. In an overview, Wagenaar (Wagenaar, 1983) clearly shows the predominance of human failure (80-100%) in accident research.

However, the focus was still restricted to the impact of the disaster and to the problems of rescue, relief and recovery. There was no emphasis on events prior to an accident, Turner (Turner, 1978). All the knowledge, tools, and techniques of events existing prior to an accident were built on a set of principles that were first derived from H.W. Heinrich's classic text of 1931, as stated by Peterson (Peterson, 1996). Perhaps the most important of these principles, which dominated until the 1980s, is the domino theory of accident causation. This principle implies that accidents result from a sequence of events and suggests that removal of one single event in this sequence of events will prevent an accident from occurring. In addition to the domino theory Heinrich (Heinrich, 1931) constructed a descriptive iceberg model, as can be seen in Figure 2, which is taken from van der Schaaf (Schaaf van der, 1992).

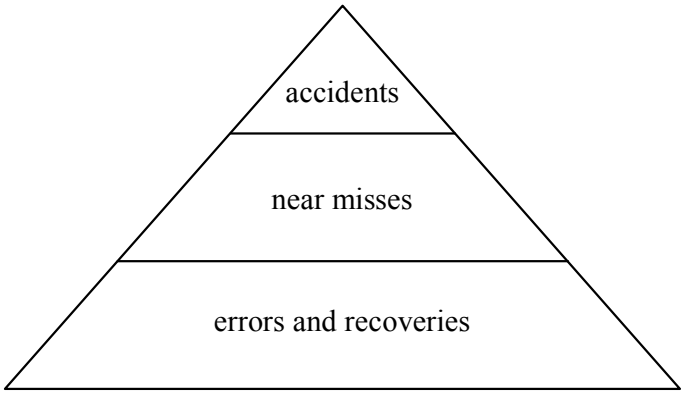


Figure 2 *A descriptive iceberg model as taken from van der Schaaf (Schaaf van der, 1992)*

Heinrich (Heinrich, 1931), discusses the relevance of the iceberg model as providing some evidence of similarity of cause, frequency and severity. However, the ratio relationship between huge numbers of errors and recoveries and almost never happening accidents, does not prove that there is a causal relationship between errors and accidents. Wright (Wright et al., 2003) showed that Heinrich and others in literature, had entwined two models, i.e. the ratio model and the common cause model. What the literature and practice had assumed was that accidents propagate from errors and recoveries (bottom) via near misses (middle) to accidents (top), which is never really proven. As Wright observes, the common cause model has come to imply a ratio relationship of consequences (and not of causes). Only recently the first evidence for the assumption made has been found, by research showing that similar patterns of root causes exist for near misses and accidents, e.g. at the British Railway, Wright (Wright, 2002). Despite this serious misunderstanding in literature and practice, the entwined common cause/iceberg model is still one of the most important assumptions in safety thinking today.

Accident numbers decreased in the human error era and the indicators for safety performance changed gradually from measuring the number of accidents to measuring the absence of injuries, damage, sickness, environmental pollution, etc. Although still in use it is recognised that these safety indicators have their shortcomings, Körvers (Körvers et al., 2001a):

- Correlation; safety investments (indicators), intended to produce safety improvements are usually well known but they are hard to correlate directly with any of these improvements.
- Representativeness; the perception of a good safety performance, does not guarantee a good safety process.
- Power of discernment; when the likelihood of accidents in an operation is already extremely low, the absence of an indicator of extremely unlikely accident is not a guarantee for a low risk.
- Availability; most indicators measure the consequences of an event, which means they are available too late to prevent similar consequences from occurring.

Further alternatives were researched. Based on the iceberg model, data on incidents, near misses, errors and recoveries, etc, were collected. A limitation in doing so was found to be an inability to interpret from the mass of data which errors and recoveries lead to actual accidents. The chemical process industry has never taken visibility into account. According to Hale (Hale et al., 2000), the chemical process industry misinterpreted Heinrich's iceberg model by putting large efforts into tackling small injuries, such as twisted ankles or scratches. These 'slips and trips' are not related to the safety of the primary operational process. Nevertheless, the chemical process industry still thinks that the accident frequency may be reduced by tackling these unsafe acts, according to the iceberg model.

During this human error era thorough investigations of a series of dramatic accidents (Bhopal, Chernobyl, Herald of Free Enterprise), shifted attention more towards the events prior to the accidents and led to the conclusion that the causes concerned more than only technical and human factors. Turner (Turner, 1978), was one of the first to look beyond technical and human factors and concentrated on the sociological and

organizational factors contributing to an accident. After Perrow published '*Normal Accidents*' in 1984 (Perrow, 1984), safety science began to conceive that accidents were processes and not sudden cataclysmic events, Vaughan (Vaughan, 1996). Heinrich's domino theory was disputed and replaced with the multiple causation theory, which states that accidents are caused by a number of events that combine in time. Many events and the accident itself are all symptoms of something wrong in the management system, Peterson (Peterson, 1996). In this third era, the socio-technical era according to Reason (Reason, 1991), it was recognised that safety problems emerge from the yet little understood interactions between technical, human, social and organizational aspects of a company in combination with a changing environment. This will be discussed more fully in the next sub-Section. As a result, research into safety management began in which safety was no longer measured (only) by the number of accidents, incidents, trips and slips, or technical inspections, but also by the outcomes of audits. These audits used checklists, questionnaires, interviews, etc. to identify the completeness and effectiveness of the Safety Management System (SMS). This SMS, is the system of structures, responsibilities, and procedures, with the appropriate resources and technological solutions available, Seveso-II directive (Seveso-II directive, 1996). The completeness refers to the availability of 'all' 'critical safety elements' inside the system, e.g. training, incident reporting, maintenance, etc. However, it is still unknown what 'all' these critical safety elements are. There are some agreements on national and international level, e.g. U.S OSHA Process Safety Management Standard (OSHA-1910.119, 1996) European Seveso-II directive (Seveso II directive, 1996). The effectiveness of the SMS is measured by audits and inspections, which determine by means of questionnaires and interviews how well the 'generic Shewart cycle', later named 'Deming cycle', Deming (Deming, 1986) is implemented for all critical safety elements.

Stimulated by the environment, many methods were developed to measure safety or the lack of it and identify process risks inside the chemical process industry, as shown by Tixier (Tixier et al., 2002). They studied 62 methods of identifying risks in industrial plants from which can be seen that many methods are available in different areas, e.g. technical, human, and organizational areas, but also in different phases of a technical installation's life-cycle. Nowadays, new standards have been applied, such as IEC 61508 (IEC 61508, 2000) where safety has to be taken into account in all phases of the technical life-cycle of the installation, i.e. designing, constructing, operating, maintaining, and decommissioning. So the scope of safety science has widened from the engineering domain via the human domain to the socio-technical domain, and it then broadened further to include all phases of the technical life-cycle of an installation.

A very important contribution in this socio-technical era is made by Reason (Reason, 1990). He made a distinction between active failures, and latent conditions. The active failures are in general failures made by those at the sharp end of the accident causation (e.g. technical and human failures). Effects are felt almost immediately. Latent conditions are removed in time and space from the sharp end of the accident causation (e.g. organizational and technical failures) creating conditions for active failures to be made. A strict boundary between both concepts cannot be made and in reality can be seen as a sort of sliding transition. Here, the two concepts are separated

by only mentioning that the overlap in the boundaries represents the interface between the organization and the human involvement, which is sufficient in this research.
Reason (Reason, 1990) displays his thinking by showing the development of an accident from latent conditions to active failures, which both penetrate a series of defences and eventually lead to incidents, see Figure 3.

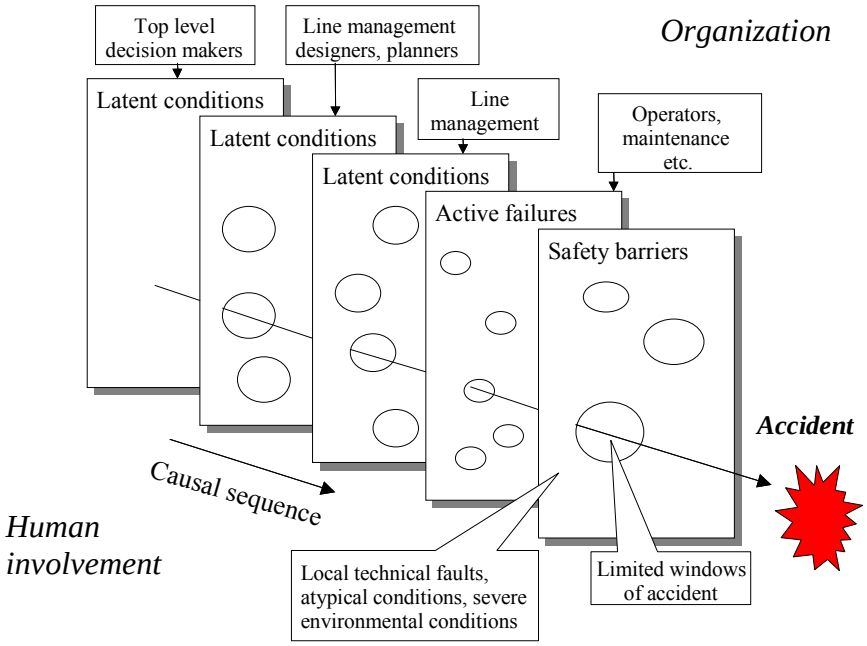


Figure 3 *Latent condition – active failure model of accident causation passing through a hole in the safety barriers, by Reason (Reason, 1990)*

Latent conditions, conditions created by management and technique lead to active failures at the sharp end or workplace. The latent conditions are for example conditions of the global safety style (top level decision making) of an organization (safety culture), but also conditions of different organizational functions which affect safety, i.e. poor maintenance procedures, inadequate training, design failures, etc. (line management, designers, planners). Examples of active failures are the errors, violations, and problems on the workplace. All latent conditions and active failures lead to holes in the organizational safety barriers. These safety barriers, defences, or safeguards are the barriers in a technological system that can arrest the accident/incident evolution so that the next event in the chain will not be realized, Svenson (Svenson, 2001). The function of these safety barriers is to protect people, environment, and assets from hazards. Mostly they do this very effectively, but there are always weaknesses created by the latent conditions and active failures, Reason (Reason et al., 2001). These safety barriers are often called the layers of protection. These layers consist of a variety of safeguards and are often displayed as onion skins layered around the hazard, preventing and mitigating it from causing damage to its environment. However, in reality these layers of protection are perforated with holes. These holes are not static because of external conditions (laws, market demands) and recoveries by operators, they are continually opening, closing, and shifting their location. The danger arises when holes momentarily line up, bringing the hazard in contact with the environment, people, or asset, resulting in incidents.

This concept is still dominant in thinking today and has become one of the fundamental principles in safety science. Hudson (Hudson et al., 1991) used this

thinking to develop TRIPOD, a method to measure 11 General Failure Types (GFTs) which are a selection of latent conditions. Groeneweg (Groeneweg, 1992) analysed hundreds of accident scenarios and validated the audit tool to transform questionnaires into 'Failure State Profiles' which graphically display a company's score on each of the 11 GFTs. These 'Failure State Profiles' are represented by bar graphs that show the extent to which each of these 11 GFTs contribute to future accidents.

Following the research which focused on failures, researchers looked at safety success. Organizations with small numbers of accidents, are considered High Reliability Organization's (HROs), such as the U.S. navy nuclear aircraft carriers, air traffic control systems and nuclear power plants. Studies into these organizations revealed three distinguishable attributes possessed by HROs as opposed to high risk organizations according to Roberts (Roberts et al., 2001):

- Continuously searching for deviations to resolve the generic causes responsible for these deviations,
- Designing their reward and incentive systems to recognize costs of failures as well as benefits of reliability,
- Communicating the organizational goals and showing everyone how they fit into the big picture to achieve these goals.

A measure of the reliability of other organizations can be assessed by identifying how these factors are addressed. With the HRO and other studies in safety management, research shifted into the less structural aspects of safety management. Perception issues and concepts like organizational culture directed research into the area of safety climate or safety culture and thus organizational learning, Pidgeon (Pidgeon et al., 2000). The safety culture, which is established by the internal and external environment of an organization, is the fourth era, the inter-organizational era, in which efforts are concentrated on improving the inter-organizational interactions, Wilpert (Wilpert, 2002). Rasmussen (Rasmussen, 1997) takes the external environment into account, in addition to the technical, human and organizational factors. Interactions between continuously changing internal and external factors shape the way safety is handled in an organization (safety culture).

Historically these four different eras (engineering, human error, socio-technical and inter-organizational) can be recognised in different application areas, i.e. nuclear, chemical, railroad, medical, etc. Moreover, it seems that new eras only evolve after serious accidents receive much public attention resulting in the development of another set of stimuli which leads to further decreases in accident rates. Figure 4 shows the changing scope of safety research in the chemical process industry during the past 50 years and expectation in the coming years, as adapted from Groeneweg (Groeneweg, 1992).

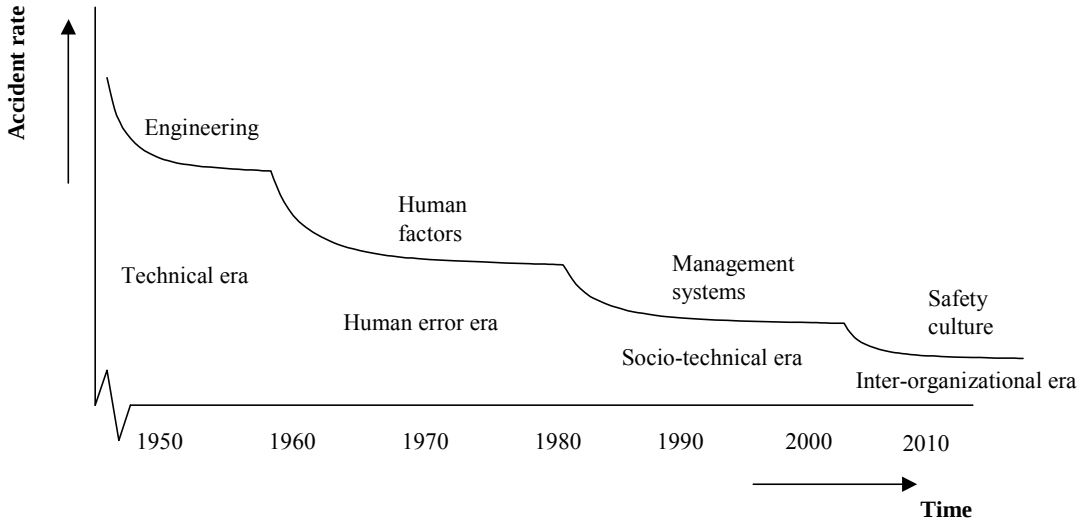


Figure 4 *The changing scope of safety research in chemical process industry, adapted from Groeneweg (Groeneweg, 1992).*

Figure 4 shows the focus in safety research during the last 50 years. Although this is an accepted figure in literature, for the sake of clarity, no actual data is used, see Groeneweg (Groeneweg, 1992), Visser (Visser, 1998), Wilpert (Wilpert, 2002). Above the line of decreasing accident rate, the focus area of that era is stated. The figure is taken from Groeneweg (Groeneweg, 1992), extended with the four eras identified by Reason (Reason, 1991) and Wilpert (Wilpert, 2002). Note that the consequences of the accidents are neither stated nor taken into account.

In the last shift towards the inter-organizational era, a better understanding of how accidents occurred in socio-technical systems and how the environment interacts with this socio-technical system became more important. Achieving a better understanding of the environment and its influence on the system enables more insight into how accidents evolve and consequently measures can be derived to prevent them. Besides the changing scope of safety science the environment also changes over time and influences the way safety is seen. This environmental change is discussed in the next sub-Section.

1.3.2 The influences of a changing environment

Today, companies must be capable of rapidly reorganising to survive in the strongly competitive market. Organizational change is generally seen as a pre-requisite for assuring competitive advantage and business survival in the global marketplace. Baram (Baram, 1998) defines four common types of organizational change, i.e. downsizing, outsourcing, forming strategic alliances, and deconstruction. By empirical studies and cited literature, Baram clearly shows the influences and the consequences of these changes on the causation process of accidents. For example the dispersion of hazardous chemical processes among contractors can lead to an increasing likelihood of process safety problems due to the lack of safety expertise of these contractors. Smaller companies who are less accountable are becoming increasingly more responsible for safety and corporate involvement is reduced to a minimum. Relevant safety information from sister companies is no longer communicated among the different companies. Moreover, this organizational change mentioned by Baram. Perrow (Perrow, 1984) highlights the increasing complexity of

techniques within organizations. This increase in complexity creates a lack of full understanding by operators and managers of possible interdependencies between system components. Important information is wrongly interpreted, not observed, or even ignored, providing the opportunity for an accident to occur. Kirwan (Kirwan, 2001), mentions the problem of accelerating technologies, and the market pressure on organizations to grab the benefits of new technology without knowing the 'downsides' of these technologies. To survive in modern world, companies have to adapt faster to their environment. However, measuring safety means not only taking the handling of hazardous substances into account, but also the actors inside the whole system; i.e. operators, line management through to top management.
Another factor is best described by Rosenthal (Rosenthal, 2000). He noticed that the as acceptance of disasters decreases discussions about safety and risks spreads into the domains of politicians, jurists, and journalists, where formerly these discussions were typically the domain of technicians and mathematicians. The public demands justification from both authorities and organizations by public inquiries, research, etc. An example is given by Tielemans (Tielemans, 1995). He states that people who were forced to separate their own garbage would not tolerate Shell's intention to dispose of their garbage (the Brent Spar) into the North Sea because of cost considerations. Technical discussions didn't help and were doomed to fail. The risk perception of the people is determined by their personal observations as viewed against their values and beliefs and differ from the technicians' explanation that risk can be seen 'objectively' as identical. This plurality of perception has led to many companies keeping their accidents inside their borders. For example in The Netherlands in 1999 the media brought a leakage of a hazardous substance to the attention of a local community which pressured the local authorities into conducting a major investigation. However, two years later another spill of the same hazardous substance at the same company was kept 'confidential' by the company and went unnoticed by the local community.
Brombacher (Brombacher et al., 2001), showed that the changes in the environment not only have an effect on safety in the chemical process industry, but may also affect the reliability of technical systems. In several areas similar changes or trends and their examples are shown, i.e. transportation, banking, chemical process industry, and consumer electronics. The five trends identified are:

- Increase in complexity of technical systems,
- Globalization and segmentation of business processes,
- Faster time to market,
- Higher expectations in functional correctness of the system,
- Increase in vulnerability of the system to external influences.

It seems that these changes in the external environment of companies influence the way safety is dealt with in high-risk organizations like the chemical process industry. However, another important change has been: the influence of the national and international authorities especially in the environment of high-risk organizations. Because investments in safety are still mainly driven by regulatory forces as discussed by Körvers (Körvers et al., 2001a), these changes have had a large impact on the way safety is controlled in the chemical process industry. As Hale (Hale et al., 1998) showed, the increasing technical complexity increased de-regulation as the technological changes were so complex that governments could not keep up with its knowledge, which mainly focused on prescriptive technical regulations. From the 1970s government authorities increasingly placed the central responsibility for

controlling safety on the company management. This led to an increased number of socio-technical models, and more recently cultural tools and methods, designed to show the authorities and ultimately the public all the effort put into safety. High-risk organizations demonstrate to authorities and the general public that safety is the number one priority and that considerable effort is being put into achieving a safer workplace and better environment. Responsible care programmes were established, and companies developed their own programmes and tools to indicate their safety performance. The European Union put a directive in place for all its member countries, which required major hazard installations (determined by the amount and type of hazardous substances present) to implement a Safety Management System (SMS). The United States' OSHA requires a similar system but puts it under a different name of Process Safety Management (PSM). The aim of these systems is to put in place safety measures and to control their continued and proper working. In this way companies assure the community that their risks are controlled.

The widening of the research scope showed that safety is not a simple 'technical' problem, but one of many different domains, Rasmussen (Rasmussen, 1997). Pressure from the external environment (authorities, public and market) requires ever more proof that companies within the chemical process industry are handling their hazardous substances safely. By comparing the average frequency of fatalities per 100.000 workers as an indicator for a safety average the manufacturing industry in the United Kingdom (including the chemical process industry) is shown to be four times as safe as the construction industry in the United Kingdom, see Table 1, HSE (HSE, 2003).

Table 1 Average frequency of fatalities per 100.000 workers in the United Kingdom (HSE, 2003)

	1995/1996	1996/1997	1997/1998	1998/1999	1999/2000	2000/2001	2001/2002	2002/2003
Manufacturing industry average	1	1.4	1.4	1.6	1	1.2	1.2	1.1
Construction industry average	5	5.6	4.6	3.8	4.7	5.9	4.4	4.0

The chemical process industry had to invest in safety (pressured by the external environment), without proper knowledge of whether the investments would result in a significant increase in safety performance. However, it is only after an accident has occurred that the performance of safety investments can be addressed and objectively justified. As shown by the example in Section 1.1, companies fulfil the required standards and even take additional measures to keep their installation working without inflicting damage to their environment. All indicators present in the example in Section 1.1 show excellent performance, Hopkins (Hopkins, 2000). The accident presented in Section 1.1, serves as a good example for the present day chemical process industry. The problem of accidents occurring despite the excellent safety performance shown by the safety indicators, leads to companies comparing safety tools and frequency of usage amongst each other. This results in companies implementing or adopting whatever safety tool a 'better company' uses, trying to achieve the same or 'better' results. Here 'better' is expressed by the number of lost

time injuries or recordable injuries divided by the number of hours worked, which is an indicator often criticised as discussed in the previous sub-Section and by many other authors (Hale et al., 2000, Groeneweg, 1998). Many other safety indicators are present, but will be more thoroughly discussed in Chapter 3. Moreover, the fact that safety tools are often developed to solve specific problems in specific situations is often overlooked by companies. Safety is becoming increasingly commercially attractive. Companies with a 'good' safety record may even sell their safety tools. Accidents keep occurring in spite of companies implementing all conceivable measures and are often seen as an act of God or resulting from human error, as in the example presented in Section 1.1. There the operators made some critical errors but they had been properly trained and therefore no excuses for their errors can be found, Hopkins (Hopkins, 2000). Hopkins showed how the technical, human and organizational factors together with the different elements from the external environment led to the accident. He explains how market pressure, downsizing and focusing on LTIs, had influenced the organization, leading to technical and human errors at the sharp end of the accident causation trajectory, and eventually to the accident. However, how the organization could have identified the factors influencing safety beforehand is not addressed.

From the research in the field of safety science, it appears that finding the right indicators for risks is still difficult. The visibility of errors (active failures) leading to an accident is very low, i.e. are the errors based on the same root causes (latent conditions) and would eliminating them actually avoid the accident? Measuring the absence of accidents and damage cannot be used as an indicator to prevent potential damage. By measuring elements in an organization, the questions are raised, which elements should be addressed and how should they be measured? How should a safety culture be established or defined within an organization, especially when external influences play an important role? How to find factors or signs indicating a possible risk in an organization is still a problem in safety research? Therefore, identifying 'pre-warning signs' which indicate that an accident might occur is the focus of this study. Many authors e.g. Reason (Reason, 1991), Tweeddale (Tweeddale, 1995) have referred to pre-warning signs as precursors, defined loosely as 'warning signs that accidents may happen'. Finding precursors which give an early indication that an accident may occur enables the chemical process industry to target their limited resources on the highest risks. Identifying these precursors, their causes and finding out why organizations don't use them will be the focus of this research. The scope of this focus will be discussed in more detail in the following Section.

1.4 The research scope and questions

Research in the field of safety increased over time, and has progressed in stages from looking only at the technical aspects of an installation at the design stage, to considering the interplay of technical, human and organizational aspects during the entire life-cycle of the installation. Moreover, influences from the external environment, such as the market, authorities and society, stimulated research and has had the important consequences for safety mentioned in the previous Section.

Finding indicators to 'measure' safety developed in the past followed broadly similar paths. However, in spite of applying these measures and indicators, in practice accidents still occur. Identifying possible risks before an accident occurs is of course the most favourable scenario. This in turn enables technical installations to be made inherently safe, by eliminating the unsafe use of hazardous substances or eliminating

the misuse of the installation under extreme conditions. The application of counter measures informed by risk analysis, decreases the risk to an 'as low as reasonably practical' level (ALARP). However, not all risks can be predicted and taken into account beforehand. The other extreme is waiting for an accident to occur and try to turn hindsight (accident analysis) into predictive pro-active knowledge. Tools like MORT, Johnson (Johnson, 1980) or TRIPOD-beta, Wagenaar (Wagenaar, 1994) categorize the causal factors of events to indicate where companies have to focus their safety efforts. However, this method is too late to avoid damage and companies are increasingly trying to prevent accidents occurring. Indicators during the operational phase of an installation are therefore necessary. Near misses are indicators that are analysed in the same way as accidents to categorize the causal factors and to indicate where companies have to focus their resources. Other researchers try to prevent accidents by assessing the quality of the SMS. These are audit-like methods, most of which are not scientifically based, Hale (Hale et al., 2000). Some researchers try to overcome this shortfall, by developing a more scientific approach, e.g. IRMA, Hale (Hale et al., 1999), or MIR based SLM-technique, Knegtering (Knegtering, 2002). Another approach tries to discover organizational safety performance indicators by generating the 'critical organizational elements' that influence safety. Some have done this by studying accidents, e.g. TRIPOD, Hudson (Hudson et. al., 1991). Whilst others try to establish the 'critical organizational elements' influencing safety by looking at the working practice, e.g. WPAM, Davoudian (Davoudian et al., 1994) or SAM, Murphy (Murphy et al., 1996). The weakness of these latter methods is that the link between the broad and vague organizational factors and safety is assumed and mainly based on expert opinions, Øien (Øien, 2001). Identifying precursors upon which companies can react is still a difficult problem in safety research, mainly because the events causing accidents differ in each case and are hard to predict. The important question from a theoretical as well as practical perspective is; which precursors and underlying causal factors indicate that an accident is on its way? This question is graphically shown in Figure 5, and derived from Reason's idea, see Figure 3. In respect to Figure 3, the precursors in Figure 5 are the results of 'active failures' in the operational process, the causal factors in Figure 5, are the latent conditions of Figure 3. Together the causal factors and precursors penetrate the safety barriers, which finally leads to an accident as Figure 3 and Figure 5 show.

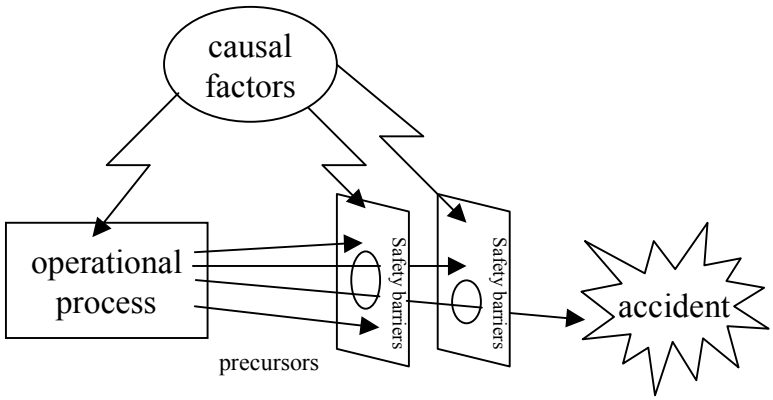


Figure 5 A graphical representation from the overall research question.

Providing companies with practical guidelines for assuring their safety, to replace or augment the present indicators which fail to signal a developing accident, justifies

further research. In this thesis an attempt is made to identify possible signs. This automatically leads to the first research question, formulated as;

Is it possible to identify precursors of accidents in an operational process?

If it is assumed that precursors can be identified in a scientific way, the next research question can be formulated. By using only precursors the elimination of all possible accidents is extremely unlikely. Retrieving precursors and acting upon them can be seen as a sort of 'fire fighting' approach. It is more important to devise pro-active measures to discover the underlying factors, causing the possible accidents. Subsequently companies can direct resources at these identified causal factors and possible accidents can actually be prevented. The next research question is therefore formulated as;

Is it possible to retrieve the causal factors of such precursors, which can explain accidents?

Assuming that both previous research questions can be scientifically founded, a better understanding of why accidents still occur despite all existing measures can be obtained. From both the previous questions the third research question can be derived, which is formulated as;

Why do accidents still occur despite the pre-warning presence of such precursors?

The most important question deals with the development of methods to identify those precursors which can reliably predict accidents and how the underlying causes of an accident may be retrieved to discover them;

How can the pro-active identification of accidents be improved, by using precursors?

Answering all four questions will help theory and practice in where to look for signs and derive causal factors for accidents, and show why accidents still occur in spite of all measures currently taken. It is inevitable that some accidents will occur, because not all accidents can be foreseen and prevented. The next Chapter will describe the underlying research process and will present the methodology of how all four research questions will be approached.

Chapter 2

RESEARCH METHODOLOGY

Based on the observed problems in the measurement of safety in the chemical process industry, as outlined in the previous Chapter, additional research into this area is needed to provide companies with better indicators of possible accidents. In this Chapter the research methodology used to gain a more complete understanding of this 'measurement problem', is presented. This Chapter starts by discussing the focus, type and methodology of the research process. Then the research strategy and methods will be discussed to present the design structure of the complete research.

2.1 Research process, type, and methodology

Success of a research project is largely achieved through dedication and a steady methodological approach to the work. Bickman (Bickman et al., 1998) divided research activities into two types; basic and applied research. The purpose of basic research is to expand knowledge; where the knowledge is an end in itself. The research described in this thesis is applied research whose purpose is to improve our understanding of the problem with the intent of contributing to the solution of that problem, Bickman (Bickman et al., 1998). Applied research is typically performed in an open environment and the result often consists of a design. Other differences between basic and applied research are in context and methods. Croom (Croom, 2001) cites several authors who proposed models for a systematic approach to the applied research process. Typically the research process consists of two major processes, i.e. planning and execution, Bickman (Bickman et al., 1998). The planning process consists of a definition phase and a research design phase. In the definition phase a broad area of study is defined and the research topic selected. In the research design phase; the approach, the way of collecting data, the way of interpreting the data and the validation of the data are selected. The execution process is the execution of the research design and reporting the results. When you collect data you are in fact beginning to analyse it. Moreover, when you begin analysing it you generate new ideas and thoughts which modify the process. These dynamic modifications cause the process to twist and turn like a kaleidoscope as different patterns emerge. Therefore these processes must not be seen as a clear-cut sequence, but rather as a series of repeated attempts to make sense of the data or as Bechhofer (Bechhofer, 1974) called them 'iterations' through various cycles of the above phases.
In this Chapter emphasis will be put on the planning process while the execution process will be addressed later. In the next sub-Sections; the focus of the research, the type of research, the research methodology, the research strategies and methods used will be presented.

2.1.1 Focus of the research

Today there is still a problem indicating 'safety' in high potential risk organizations such as the chemical process industry. Chapter 1 showed an example of how an accident could occur in the chemical process industry even though all safety measures

indicated that the safety performance was excellent. In recent years, the increased influence of the external environment has made increasing demands on the safety performance of high risk organizations. While market trends like outsourcing, globalisation, etc. have adversely influenced the probability of accidents in these high risk organizations, Baram (Baram, 1998). The developments described in Chapter 1, led to the problem of how to find reliable factors or signs indicating a possible risk in chemical process industry. This problem defined the four research questions. The framing of the research questions are very important in conducting sound and good research and there must always be a clear linking of the questions to concepts, Lewins (Lewins, 1992). Furthermore, the research questions should satisfy certain criteria. According to Punch (Punch, 1998) the research questions must be clear, specific, answerable, and interconnected. If the research questions do not satisfy all of these criteria, problems will occur during the research process. The constructed research questions are then posed, followed by a brief discussion to provide more detail. The research questions constructed in this research are:

Research question one:
Is it possible to identify precursors of accidents in an operational process?

Research question two:
Is it possible to retrieve the causal factors of such precursors, which can explain accidents?

Research question three:
Why do accidents still occur despite the pre-warning presence of such precursors?

Research question four:
How can the pro-active identification of accidents be improved, by using precursors?

In this thesis the definition of precursors is: clear, observable facts present in the operational process of an organization, before they appear less benignly in the trajectory leading to an accident. These precursors are present due to causal factors in the business process. However, these causal factors are not always clearly visible in the operational process.

The main purpose of this research is to design a protocol which provides companies in the chemical process industry with a better understanding of possible indicators of an accident, to enable them to further enhance their Safety Management Systems (SMS).

Many causes of accidents lie in the design of a process installation, HSE (HSE, 1995). However, the focus of this research will lie on the operational phase of the process installation where accidents always manifest themselves. It is in this operational phase that indicators are needed if in the design phase critical items have been overlooked which could pose a threat to: people, the installation, or the environment. To retrieve these indicators, knowledge of the accident causation has to be obtained. Then a way to identify the events preceding accidents has to be derived from this knowledge. Experience is the most costly form of knowledge in terms of injury and damage to people, installation, and environment, and waiting for accidents to occur is not an option. Therefore, actual accidents and reports of accident investigations are analysed. Literature on accident causation, and safety management is studied and lessons learnt

assimilated, together with conducting in-depth examination of existing safety performance indicators. Subsequently the causal factors in an organization are retrieved informed by literature from organizational science and safety management. Finally, the knowledge obtained leads to the design of concepts which will be tested and verified in practice, to obtain a standardized protocol. With this protocol companies in the chemical process industry should; obtain a better understanding of possible indicators of an accident, be able to reinforce their SMS, and increase their awareness of why accidents still occur in spite of the precursors present.

2.1.2 Type of research

To provide answers for the research questions posed in the previous Section, the next stage is to decide which philosophical position must be taken to provide insight into the subject of research, i.e. which research type must be chosen? Numerous authors on research methodology discuss various qualifications and methodologies of research types such as Meredith (Meredith et al., 1989), Gill (Gill et al., 1991), Croom (Croom, 2001). Croom divides these research types roughly into positivist and constructivist types. The positivist types emphasize observable facts derived from validated reliable measurements and provide results and conclusions which can be verified and generalized. The constructivist types depend upon the researcher as a participant, holding the view that actions and phenomena are present due to specific circumstances present at that moment.
This research attempts to identify clear, observable facts which are precursors of accidents. From these precursors possible causal factors which enable accidents to occur will be derived. The findings can be generalized by analysing several cases and eventually verified by some practical examples. This results in the philosophical positioning of this research as positivistic.

Other, often made distinction in types of research, are between; exploration, description, explanation, and testing, van der Zwaan (Zwaan van der, 1990). Exploration is conducted when theoretical knowledge in literature lacks information on which variables are important. Description types of research aim at the relevance of the variables. Explanation types of research aim at identifying the causal links between variables and phenomena. Finally, testing types of research aim at proving the hypotheses derived from the causal links. The research project discussed in this thesis is mainly explorative in nature. The emphasis is to design concepts and a protocol, which increases the understanding of the problem of how and why accidents continue to occur in companies in the chemical process industry. In this way a contribution to the solution of the problem will be made and consequently this research can be typified as applied positivistic exploratory research.

2.1.3 Research methodology

To conduct an applied positivistic exploratory research, an appropriate research methodology must be derived. De Leeuw (Leeuw de, 1996) distinguishes two primitive forms of research; the empirical cycle and the design cycle. The design cycle or in the Dutch applied research also called the regulative cycle, van Strien (Strien van, 1986), aims at effective intervention which results in a solution, that is implemented in the organization. This type of research is also called design-oriented research, van Aken (Aken van, 1994). The knowledge generated by the design cycle

concerns prescriptions relating to intervention in practice. For the purpose of causal knowledge production the empirical cycle is appropriate, de Groot (Groot de, 1994). The empirical cycle is applied to understand the way an exogenous reality co-exists or develops, without interfering in the existing reality. In this research a mixture of both the regulative cycle and the empirical cycle is used. First, because both theoretical research questions and practical problems are driving this research. Secondly, the objective is to apply the developed tool in a specific domain, the chemical process industry, to generate knowledge about cause-and-effect relations, which can be used to describe, predict and explain the problem.

To explain the research methodology used in this study, both the design cycle and the empirical cycle will be discussed. The design cycle typically consists of: analysis, synthesis, simulation (application), evaluation and decision. In the analytical phase the practical problem is analysed in context and properties for the product, e.g. tool, method, etc. to be designed are derived. In the synthesis phase a provisional design is created. In the simulation phase the behaviour of the design is tested before applying it into practice. Vosselman (Vosselman, 1996), argues that the properties of the design can only be judged properly after the design is applied in practice and not before. After the application phase, the evaluation of the design takes place by comparing the actual or observed properties of the design with the expected properties. The basic question to be answered at the end of this phase is: does the designed product work. Finally, the decision is made whether or not the design is suitable, or if a new or better design has to be developed. The latter can be done by re-analysing the practical problem or revising the provisional design from the same required properties as the previous design. The left scheme in Figure 6 shows a schematic view of the design cycle, as taken from de Haas (Haas de, 2000).

An empirical research process typically consists of the following five steps: observation, induction, deduction, testing, and evaluation. The first step is collecting facts from which to deduce a causal hypothesis. Then predictions are deduced from these hypotheses. These predictions are tested with new empirically observed facts to finally evaluate the degree of truthfulness of the induced hypotheses. ‘Iteration’ takes place by adding or deriving new facts from the observation phase or by inducing or refining hypotheses. The truthfulness is not fulfilled when one of the quality criteria for a sound research design, such as the internal validity, external validity, construct validity, or reliability, is not met. The right scheme in Figure 6 shows a schematic view of the empirical cycle, as taken from de Haas (Haas de, 2000).

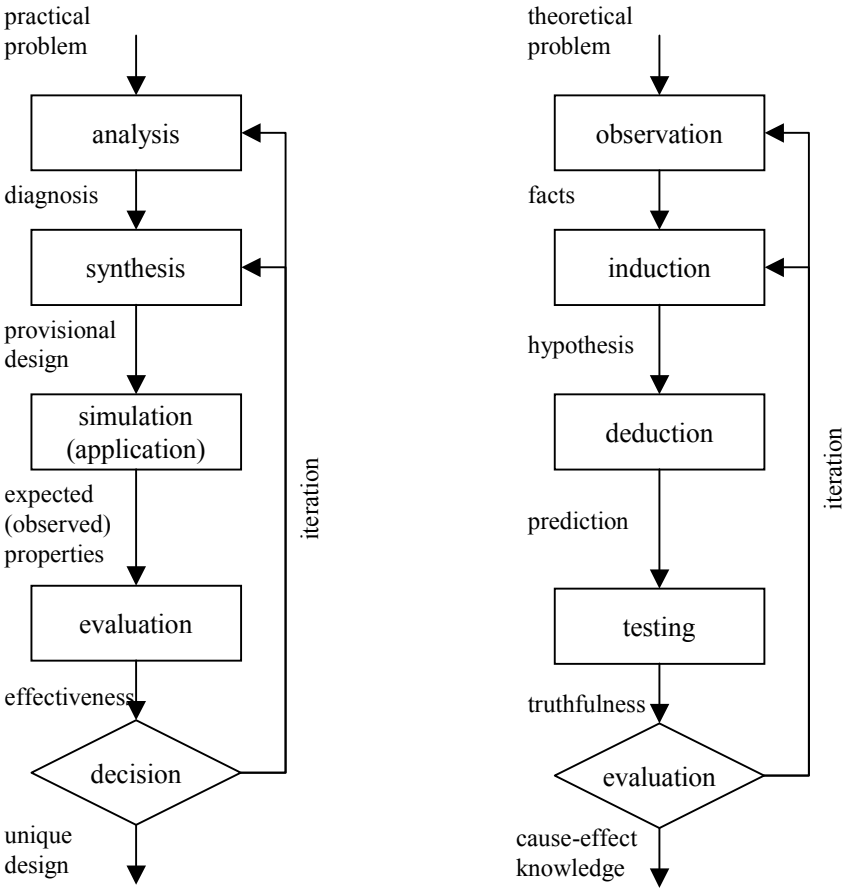


Figure 6 The design and empirical cycle (Haas de, 2000)

The theoretical and practical problem is analysed, and from the observations facts are gathered to deduce a hypothesis. Subsequently a provisional design is generated from the observed facts and from the analysed practical problems. This provisional design is evaluated in practice and the results are analysed to confirm or reject the hypothesis and develop or refine it. Finally, the enhanced design is re-applied in practice to derive the answers posed by the research questions. The result of the research is a newly developed method informed by cause-effect knowledge, see Figure 7.

The choice of the research questions, type, and methodology all have consequences for the chosen research methods, which will be discussed in the next sub-Section.

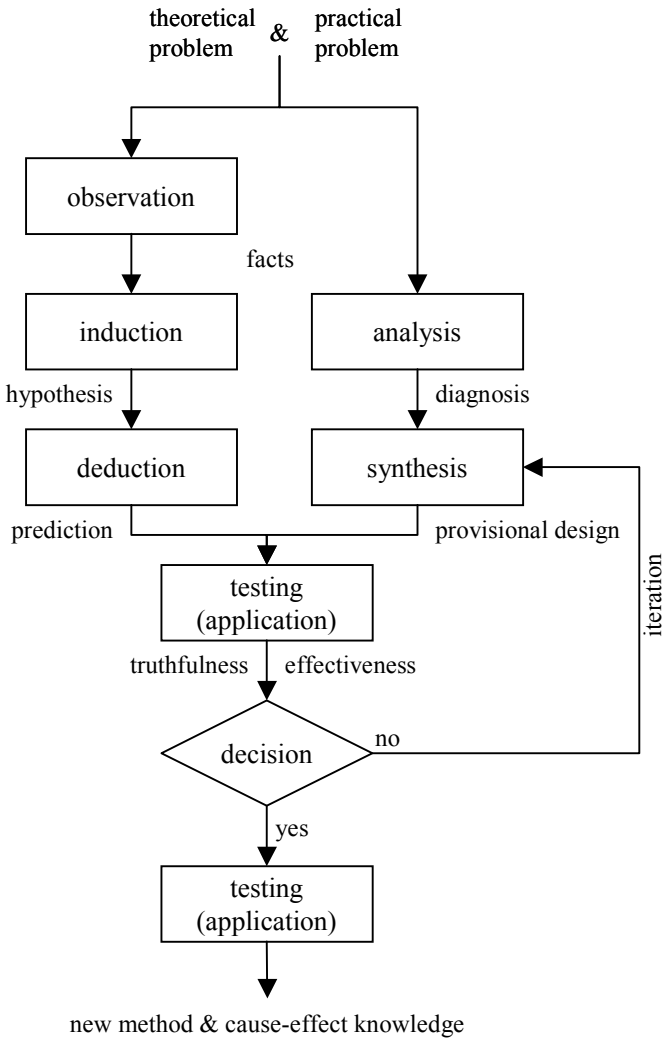


Figure 7 Research cycle applied in this study

2.1.4 Research strategies and methods

The choice of the most appropriate strategy for the research topic under investigation is one of the most important choices when designing research. Different methods of collecting and analysing empirical evidence have their own advantages and disadvantages. Yin (Yin, 1994) discusses three different conditions that distinguish which research strategy is most suitable. First, the type of research question posed has to be known. Secondly, the extent of control an investigator has over actual behavioural events has to be retrieved. Thirdly, the degree of focus on contemporary as opposed to historical events has to be established. This research aims at identifying indicators before an accident happens, which needs a research method that investigates a contemporary phenomenon within its real-life context where the boundaries between phenomenon and context are not clearly evident. Considering these three conditions only one strategy remains acceptable according to Yin (Yin, 1994) that is the case study. However, in respect to process safety, case histories of process safety related accidents are very important in gaining insight in the operational link leading to the accident. Because it is not always possible for the researcher to make direct observations and interviews he must retrieve the essence of

relevance reflected in the case histories, which is the aim of a strategy described by Strauss (Strauss et al., 1990) as grounded theory. This research will therefore consists of the two complementary strategies; grounded theory and case studies.

The grounded theory method aims at generating theory that describes patterns of behaviour, which are relevant and problematic for those involved. The researcher must constantly look for these patterns. Strauss (Strauss, 1987) mentions that the derived pattern of behaviour is the essence of what is going on in the data. In this research data will be allowed to emerge from the study area and the findings will be grounded in the specific context of each case history. Therefore, the theories that result from the findings will be grounded in actual case studies. The case histories are retrieved from the FACTS database, which is one of the largest accident databases in the world, which stores more than 18,000 files concerning accidents with hazardous materials. The database is maintained by the department of industrial safety, of the Netherlands Organization for Applied Scientific Research (TNO). The retrieval process will be discussed later in this Section and in more depth in Chapters 3 and 6.

Case study strategy is also used in this thesis. However, there is some debate about the ability to generalize from it and to cover these doubts, the case study strategy is applied in a structured way, as discussed by Yin (Yin, 1994). The research design applied in this thesis consist of an embedded multiple case study design. This means that there are multiple units of analysis and multiple case studies performed for collecting data. In this research, distinct sub-units in four different business processes will be studied. The first case study will be centred on a pesticide company in The Netherlands and can be seen as a first test of the hypothesis stated in Chapter 3 and the designed concepts and approach of Chapter 4. The other three case studies focus on multi-nationals with products such as: pharmaceuticals, coatings, and plastics. The selection of the cases will be based upon the five major issues stated by Bickman (Bickman et al., 1998); site selection, authorization, data collection process, accessibility, and other support, which will be discussed in detail in Chapters 5 and 7. The selection will be chosen in a way which enables all cases to be approached in a similar manner. Moreover, a similar mode of analysis allows a better judgement of the results of the designed method. Variety in the results is caused by the difference among the companies or the design. By keeping the variety among the companies as small as possible, the quality of the design can be better judged. If the results are similar, replication logic will take place. Replication logic is analogous to the logic used in multiple experiments according to Hersen (Hersen et al., 1976). Replication logic increases the extent to which findings can be generalized. Another factor increasing the extent to which findings can be generalized (external validity), is the availability of more than 18,000 case histories. From these case histories more than 100 cases will be analysed thoroughly.
The selection process of retrieving these case histories from the 18,000 is based on the availability of rich accident data located within the chemical process industry. A detailed discussion of the selection process can be found in Chapters 3 and 6.

Yin (Yin, 1994) discusses four criteria for judging the quality of the research design. After the external validity as already discussed, Yin defines the construct validity, the reliability, and the internal validity. The construct validity is the validity of the operational measures used for the research concepts. In this study construct validity will be addressed by the use of multiple sources for data collection. Case histories,

documentation, archival records, interviews, and observations provide findings converging in the same conclusion, which is called data triangulation, Patton (Patton, 1987). In this way the retrieved operational measures are validated. Reliability analysis shows that tasks performed to construct the research can be replicated by other researchers and will result in identical findings. Reliability of the case histories will be demonstrated by using a designed flow scheme, indicating how all findings retrieved from the accident database will be used. All findings collected during the four case studies will be put into separate case study databases, from which evidence will be retrieved when discussing the case studies in Chapter 5 and 7. Finally the last criterion is the internal validity, which validates whether certain relations actually exist or not. This internal validity will be demonstrated by applying pattern-matching logic. This pattern-matching is executed by comparing the empirically based pattern with the expected one, as discussed by Trochim (Trochim, 1989). If the results of the case studies differ from the results expected according to the previous research of case studies and literature knowledge, findings can be confirmed or rejected.
Furthermore, by applying grounded theory to the case histories in combination with four case studies, the overall validity of the theoretical concept is strengthened. The next Section will discuss the overall research design and places the context of this research in the research cycle as depicted in Figure 7.

2.2 Research design

In the previous Section the main characteristics and justification for using research type, strategy, methodology and methods were discussed. To finalize the research design, the research cycle constructed from both design and empirical research cycles will be placed in the context of this research by discussing the outline of this thesis. Deriving this final research design is necessary to see how the criteria for quality of research (according to Yin) will be achieved. Figure 8 shows the research design used in this study. Here the context of the research is positioned in the research cycle as applied in this study, which is already shown in Figure 7. The remainder of this Section will discuss the research design shown in Figure 8, as laid out in the Chapters of this thesis.

Chapter 1 provided a general research area, where the problem of measuring safety pro-actively was identified in literature and in practice. This was done by sketching a recent accident and discussing how safety was measured in the past and currently. Moreover, it highlighted that the pro-active measurement of safety is still a problem in the chemical process industry. The development of substantially more understanding of how to pro-actively indicate accidents in the chemical process industry, was finally derived as the scope of this study and will be discussed in the remaining Chapters of this thesis.

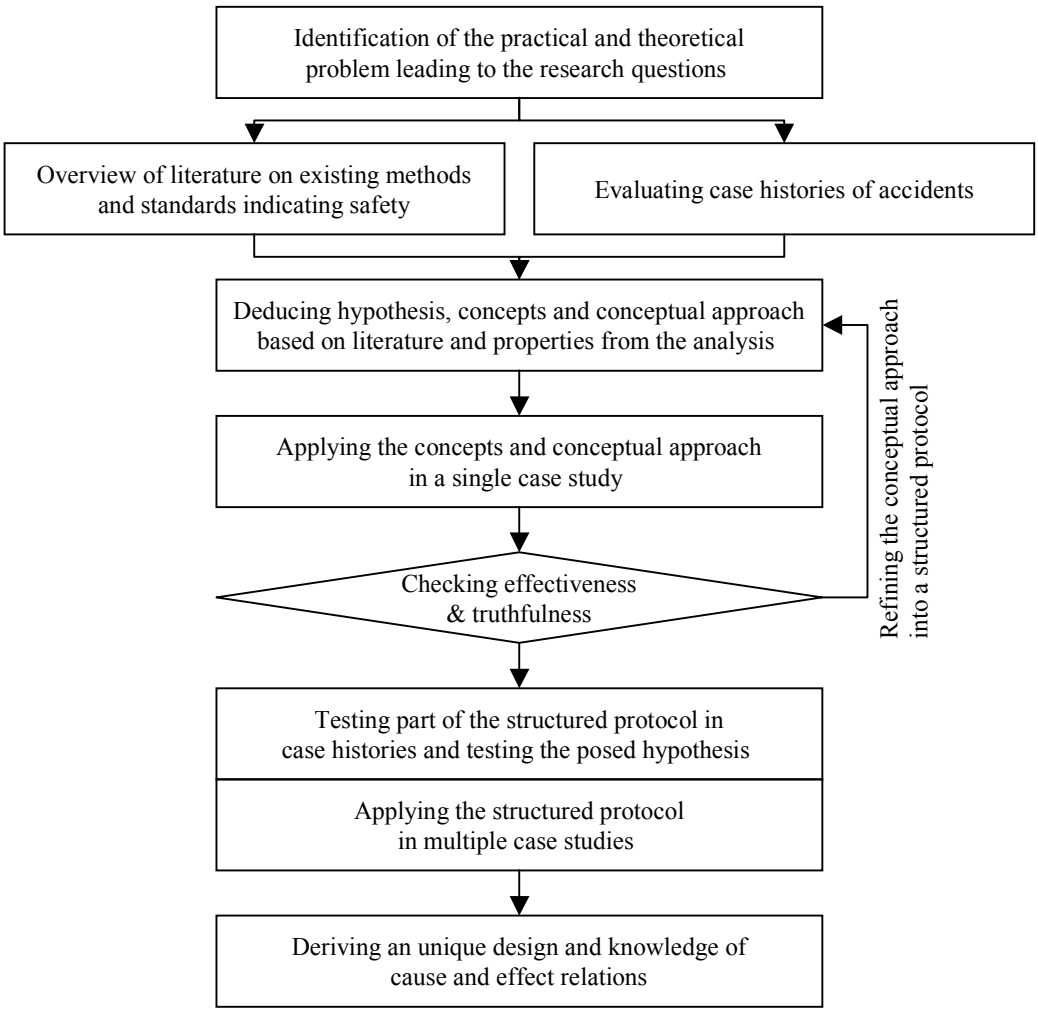


Figure 8 The research design

To analyse the problem posed in Chapter 1 an overview of current literature on tools, methods, and standards concerning safety indicators will be presented in Chapter 3. With this overview a better understanding of the signs currently used to indicate safety will be obtained. These signs will be compared with the signs present prior to recent accidents (1995-2002). From both literature and case histories a hypothesis will be derived that will be especially tested in Chapter 6. Moreover, in Chapter 4, the conclusions will be used to develop some generic concepts and a conceptual practical approach. The approach will consist of several steps and models derived from organizational science and safety literature.

In Chapter 5 the conceptual approach from the previous Chapter will be tested and evaluated and finally applied to a single case study in the Dutch chemical process industry. This exercise is performed to test the conceptual approach in practice. The findings of the case study will be evaluated and will lead to refinements in the conceptual approach. Finally a structured protocol will be derived and applied to the same case study to ascertain if the structured protocol is effective and suitable for practical use and leads to answering the research questions posed in Chapter 1.

In Chapter 6 the posed hypothesis of Chapter 3 will be tested and verified on case histories, concerning several well-documented accidents world-wide. Furthermore,

the structured protocol will be applied on a collection of well-documented recent case histories, concerning accidents in the Dutch chemical process industry. The analysis of the case histories will be performed according to the grounded theory strategy, discussed in the previous Section. Because the structured protocol uses a standardized flow scheme guiding the analysis, the results of the analysis are replicatable. Moreover, the data richness and number of case histories will increase the overall validity. By analysing the case histories in this way, the findings reported become scientifically sound and can stand criticism. Because case histories are used, certain steps of the protocol will be superfluous and unfortunately it will be not possible to perform some steps. Never-the-less, some valuable insights can still be retrieved from the case histories.

In Chapter 7 the derived structured protocol will be applied to multiple case studies in the Dutch chemical process industry. Three case studies will be conducted to derive the answers on the posed research questions and to confirm or reject the results from the case histories in the previous Chapter. The case studies will be carefully selected so that the outcomes of the analysis are predictable for all three cases. This replication strengthens the generalization and overall validation of all case studies and the research in general.

Finally in Chapter 8, all conclusions made during the research will be discussed in respect to the overall scope and research questions posed in this thesis. From this discussion general conclusions about the research performed in this thesis will be made. The research objective and research questions will be listed to check if the objective is achieved and if the questions can be answered completely and correctly. Finally, any additional questions arising from this research will suggest the scope of future research.

Chapter 3

AN ANALYSIS OF SAFETY INDICATORS AND ACCIDENTS

From Chapter 1 it appeared that all the existing safety management systems and tools cannot prevent accidents with hazardous substances in the chemical process industry. In this Chapter, the most commonly used safety indicators will be analysed to derive the set of deviations used for indicating. These deviations are then compared with deviations present in an accident trajectory prior to recent accidents. The differences between the two sets of deviations are then discussed to indicate why accidents still occur. These differences show shortcomings in current safety indicators and are used to set the criteria for a new safety indicator.

The contents of this Chapter is the basis for a paper by: Körvers P.M.W., Sonnemans P.J.M., Accidents a discrepancy between indicators and FACTS!, submitted for publication in Safety Science

3.1 Safety indicators

Despite numerous safety measures, accidents with hazardous substances still occur even though Safety Indicators (SIs) have been developed as pre-warning signs to focus companies' resources on risk areas. Moreover, SIs required by authorities enabled them to assess the safety performance of companies and focus their resources on companies which have problems controlling their risks, Modarres (Modarres et al., 1994).
The definition of risk from Chapter 1 is used to set up an analysis tool to find a possible link between SIs and recent accidents. The following sub-Section will therefore introduce this analysis tool before analysing current safety indicators and accidents.

3.1.1 The analysis tool

On the use of metrics for indicating safety, 'likelihood' and 'consequence' have a principal role and they form the two basic dimensions. When indicating risks, from historical facts and figures, simulations and knowledge, the likelihood and consequences can be established. The actual likelihood and consequence can never be derived exactly and they will always be based on perceptions of risks as discussed in Chapter 1. This perception of risks will in this Chapter be referred to as the 'perceived risks', which is the defined as the (perceived) likelihood and the perceived consequences of an event. The SIs attempt to indicate this perceived safety related risk in terms of the perceived likelihood and the perceived safety-related consequence of an event. For reasons of clarity the term 'risk' will refer to the '*perceived safety related risk'* and 'consequences' will refer to the '*perceived safety related consequences'* in the remainder of this Chapter. The 'consequences' are always based on people's perception of how great the damage to people, environment, or assets might be. The 'likelihood' of an event will sometimes be estimated (perceived).

However, sometimes the likelihood will be established by recording the actual occurrence of an event. Therefore, the likelihood is sometimes referred to as perceived likelihood when based on people's perception and sometimes as likelihood as based on observed frequencies. This risk can be shown graphically in a risk matrix, as depicted in Figure 9. Because the theoretical concept of risk and its two dimensions is difficult to translate into practice, both the likelihood and consequences of an event are classified as low to high. The risk can subsequently be derived by a point in Figure 9, having a likelihood (low or high), given on the vertical axis and consequences (high or low), given on the horizontal axis.

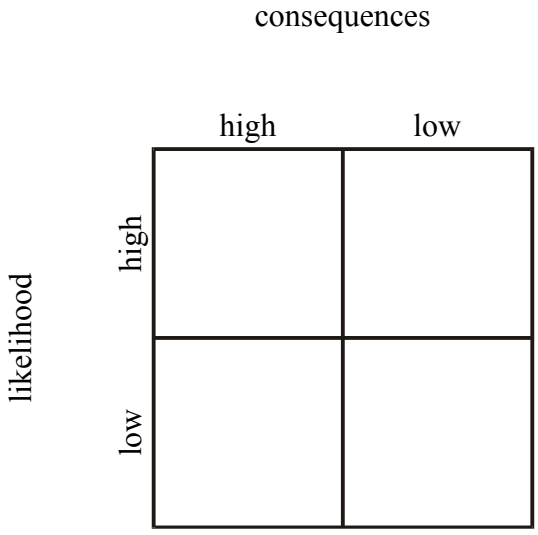


Figure 9 Risk matrix.

The risk matrix will be used to find a possible link between SIs and accidents which have occurred recently and attempt to establish why in spite of the presence of so many SIs accidents still occur in the chemical process industry. Therefore, in the next sub-Section, the most commonly used SIs are discussed and the data (events) they are constructed from are displayed in the risk matrix. Subsequently, this leads to the first risk coverage area, that of events SIs use to indicate safety.

3.1.2 Different categories of safety indicators

In this sub-Section a concise overview will be presented of safety indicators commonly used in current chemical process industry. Safety Indicators in this Chapter are restricted to the safety related risk indicators present in an organization. The SIs defined here are present in the chemical process industry in the form of operational data, and in the form of results from (safety) tools. In both cases the SIs aim to indicate the safety status, or risks, Marono (Marono et al., 1998). To retrieve the risk coverage area of commonly used SIs, both the tools, as well as the data they are based on have to be known. The relations between data, tools, and indicators are depicted graphically in Figure 10.

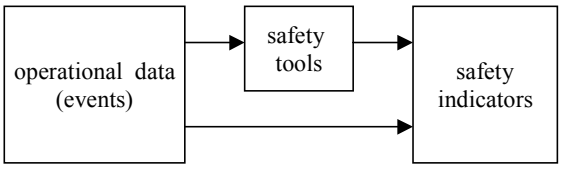


Figure 10 Relation between data, tools and indicators.

The number of SIs, present in today's chemical process industry is overwhelming as discussed by Tixier (Tixier et al., 2002). These indicators are categorized in several ways in literature, for example *pro-active* versus *reactive* indicators. Many of these categories are not unambiguous. Some authors, like Kletz (Kletz, 1998) define 'pro-active' as 'prior to the operational phase of an installation' while other authors, like Rasmussen et al. (Rasmussen et al., 2000), define 'pro-active' as 'prior to an accident.' In this thesis two categories of indicators are used, i.e. *pro-active* and *reactive* indicators. Here the definition of Rasmussen (Rasmussen et al., 2000) is adopted, who defined *pro-active* indicators as indicators 'before an accident' and *reactive* indicators as indicators 'after an accident.' Moreover, the pro-active indicators are divided into predictive and monitoring indicators. The monitoring indicators use actual events as a measure for the likelihood, while the predictive indicators predict the likelihood.
The reactive SIs are indicators which include the accidents themselves and statistics such as Lost Time Injuries (LTI), or Medical Treatment Cases (MTC) among others.

This thesis is focused on the pro-active SIs in order to derive pre-accident warning signs and reactive SIs will not be addressed. However, this does not mean that the reactive SIs have no use as pre-warning signs. On the contrary, they contribute to the enhancement of the pro-active SIs by means of the lessons learned from accidents.

The overview of pro-active SIs, the associated tools and data presented in this Chapter is not exhaustive but will serve as a fair representation of the variety of data, tools and indicators commonly used in the modern chemical process industry. The author has been unable to find literature with overviews of all known types of SIs, and therefore has created his own selection. In the following two sub-Sections the pro-active SIs, are divided into predictive and monitoring indicators together with their associated tools and data (events). From these indicators the risk coverage area will be derived.

3.1.3 Predictive safety indicators

A selection of predictive SIs, their tools and required data are listed in Table 2, and discussed in the remainder of this sub-Section.

Table 2 Predictive SIs.

indicator	**tool**	**data**
'known' safety risks	'handbooks,' 'procedures,' 'standards'	substance properties, process conditions, p&id (piping & instrumentation diagrams)
'new' safety risks	process hazard analyses	

Predictive SIs are mainly based on experiments and past accidents from which all kinds of 'safety' handbooks, procedures, standards, etc, are derived. The 'known' safety risks type of predictive SIs consists of data about substances, equipment,

process specifications, etc. which lead to safety rules. These safety rules subsequently prescribe certain (safety) measures. For example in the use and construction of pressurised vessels several design rules have to be taken into account, Fryer (Fryer et al., 1998).
The 'new' safety risk type of predictive SIs are constructed from 'process hazard analyses (PHAs),' e.g. Hazard And Operability (HAZOP) studies, Kletz (Kletz, 1974), Dow Fire & Explosion Index (F&EI), AIChE (AIChE, 1981), fault tree analysis, Watson (Watson, 1971), etc. These tools use data such as pipe & flow diagrams, properties of substances, equipment, and process specifications. The tools use this data to derive or calculate safety related risks, to adapt the design. The examples given here are based mainly on technical data. However, there are also tools for predictive SIs, using non-technical data. For example to derive safety related risks posed by the human factor, as discussed by Kirwan (Kirwan, 1998b). An example of preventive SIs addressing the organizational factors, are tools such as the Safety Culture HAZOP (SCHAZOP) developed by Kennedy (Kennedy et al., 1998).
Generally the predictive SIs try to identify the safety related risks before any operational activity has taken place. However, there is no guarantee that all risks will be indicated. Which is why in addition to predictive SIs, monitoring SIs exist, to indicate risks as precursors of accidents. These monitoring SIs are the subject of the next sub-Section.

3.1.4 Monitoring safety performance indicators

The monitoring SIs are similar to the preventive SIs. The author selected the monitoring SIs listed in Table 3, together with their associated tools and data to give a fair representation of those commonly used in today's chemical process industry.

Table 3 Monitoring SIs

indicator	**tools**	**data**
safety deviations	-	near misses, minor safety related deviations
safety measures check	inspections, observational programmes	presence and functioning of safety measures
organizational risk factors	audits, inspections	presence and functioning of organizational risk factors
safety attitude	safety climate, safety index	opinions of employees regarding safety inside the organization

The first type of monitoring SIs are constructed from actual safety related deviations from normal operation like small releases of hazardous substances, failures of safety related hardware, near misses, etc. This category of monitoring SIs are typified as the 'safety deviations' category.
The second type of monitoring SIs are constructed from tools such as (safety) inspections, and (safety) observational programmes. These tools are numerous, van Steen (van Steen, 1996) amongst others provides an overview of many different technical and human based inspections utilized by different companies in the chemical process industry. The aim of this type of tool is to check the presence and effectiveness of technical and human safety measures. This 'safe way of working' is compared with standards (technical and human) and expert opinion to indicate

possible deficiencies and opportunities for improvement. This second type of monitoring SIs is typified as 'safety measures check.'
The third type of monitoring SIs, are constructed from tools such as (safety) audits and (safety) inspections. Many different kinds of tools are in current use: TRIPOD, Hudson (Hudson et al., 1991), MORT, Johnson (Johnson, 1980), etc., for more tools see van Steen (van Steen, 1996) or Øien (Øien, 2001). The aim of these tools is to check if organizational risk factors are present and functioning effectively in the Safety Management System (SMS), e.g. does every operator obtain safety training, are equipment inspections carried out regularly and are safety procedures followed, etc. The SIs derived from these tools are ratings of these factors. The factors with the lowest rates are seen as the areas for improvement. The factors are derived from research into accidents, safety experts, or previous experiences. The European Union prescribes certain factors that should be present inside organizations identified as hazardous, Seveso II (Seveso II, 1996). This category of monitoring SIs is typified as the 'organizational risk factors' category.
The fourth and final type of monitoring SIs, are constructed from tools such as the culture climax or culture index. Sorensen (Sorensen 2002) and Guldenmund (Guldenmund, 2000), provide overviews of the tools used to derive this 'safety attitude' type of SIs as typified here. The aim of this type of SI is to capture people's beliefs, perceptions, and expectations regarding safety throughout the whole organization by means of questionnaires and interviews. This organizational element is recognised in literature, Sorensen (Sorensen, 2002) as very important for safety, and is therefore often discussed separately from other organizational risk elements.
In the next sub-Section the risk coverage area of these pro-active SIs (i.e. both the predictive and monitoring) will be constructed.

3.1.5 Risk coverage area of pro-active safety indicators

To derive the risk coverage area of the pro-active SIs, the likelihood and consequence of the events (data) that are collected to construct common pro-active SIs, have to be identified. The likelihood of the pro-active SIs data is based on the perceived frequency of events (the predictive SIs) and by the actual occurrence of events (monitoring SIs). If the frequency of the occurrence of an event is low (or high), the likelihood is low (or high). The consequences of the pro-active SIs are established by the perceived consequences regarding safety of the selected events in terms of high or low.

The predictive SIs select events (data) with a likelihood covering the range from low to high, while the consequences of these events are mainly high.
The 'safety' handbook, procedures, standards, etc. are based upon historical knowledge from real accidents (i.e. high consequences). The rules in these 'safety' handbooks, procedures, standards, only prescribe certain measures without considering the likelihood. The PHA tools analyse very unlikely scenario's that lead to serious accidents if they happen (high consequence). The PHA tools identify possible 'initiating events' (events enabling the occurrence of such a scenario) to eliminate the consequences, regardless of their likelihood.

The likelihood of events (data) for monitoring SIs also covers the range from low to high, while the consequences of these events are mainly high.

Events like leakages and injuries, all have high consequences. Inspections and behavioural programmes, are all based upon checklists, which in turn are based upon previous accidents, experience, and expert knowledge. Based on these sources of information, events are identified that have the highest potential of escalating into an accident. The identified events, and their causes are the elements for constructing the checklists. These checklists are mainly focused on events with high consequences. Organizational risk factors are derived in a similar manner.
A link between risks (likelihood and consequences) and the tools establishing the culture indicators cannot be identified from literature, Sorensen (Sorensen, 2002), so neither are included here.
These findings were obtained by discussing the different SIs with different experts from practice. Finally they are presented in the risk matrix at Figure 11 which shows the risk coverage area in terms of likelihood and consequences The data from this is used to construct pro-active SIs. Note that the results give an overview of the risk coverage area in qualitative terms in contrast to the risk coverage area of the events present in the accident trajectory described in the next Section.

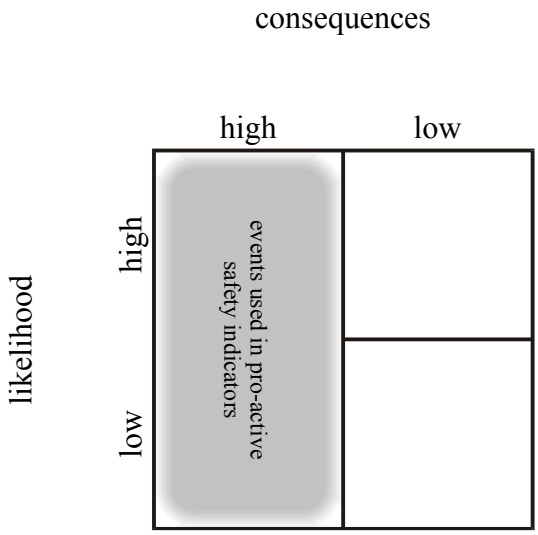


Figure 11 Risk coverage area of pro-active SI's.

From these results it can be concluded that the pro-active SI's mainly cover the 'high consequence' sector of the risk area.

In the next Section the risk coverage area of events present in recent accident trajectories will be identified.

3.2 Recent accidents

In this Section the risk coverage area of events preceding recent accidents is determined. To construct this risk coverage area a number of recent accidents (1995-2002) are discussed. The events present in recent accident trajectories are identified and their risk coverage area is determined.

3.2.1 Accidents database FACTS

When identifying the events present in recent accident trajectories, conditions regarding the availability of information must be considered. In this case, as with

many other reliability studies, the quality of information is an important 'figure of merit'. For this reason the database FACTS was accessed. FACTS is an accident database that is owned and maintained by the Netherlands organization for applied scientific research (TNO), department of industrial safety. The world-wide database contains information about more than 18.000 accidents with industrial processes where hazardous substances were involved. The database is frequently updated with information retrieved from investigations, scientific journals, technical reports, magazines and newspapers, and information from authorities, fire and police departments and companies.
The amount of detail on accidents recorded on the data base varies and the different levels of detail present, are indicated by a star (*) rating code. The higher the star (*) rating, the higher the richness of information present inside the database, as shown in Table 4 from the instruction manual of the FACTS database (FACTS, 2002).

Table 4 Detail levels of information in FACTS (FACTS, 2002).

Code	Explanation
*	Generally only one source available. Some facts and consequences are given. Reconstruction of the accident is barely possible.
**	Generally only one source available. Some facts and consequences are given. Approximate reconstruction of the accident is possible.
***	Generally always more than one public source or at least one confidential source available. A good description of the accident together with its immediate cause and the consequences. Reconstruction of the accident is possible.
****	A very good description of the accident, originating from internal as well as external documents. Always recommendations and lessons to be learned are available. The coding has been done in an extensive way and an extended abstract is available.
*****	A very complete description of the accident, originating from internal as well as external, independent qualified documents or public investigation reports available from renowned institutes or companies such as CSB, NTSB, OSHA, TNO, INERIS, DNV, etc. Many recommendations and lessons to be learned are available. The coding has been done in an extensive way and an extensive abstract is available.

The Facts database consists of the coded data and for most accidents an additional extended abstract, which briefly describes what actually happened. The coded data shows in more detail:

- a reference to the actual data,
- how detailed the information is,
- when and who added information to the database
- the country/place and date/time when the accident occurred,
- the activity, location and surroundings,
- the chain of events, leading to the accident
- detailed information about the hazardous substances and equipment involved,
- detailed information about the critical event (fire/explosion/release)
- detailed information about the consequences, damage to environment, assets and people and activities to mitigate these consequences
- lessons learned

The FACTS database does not show detailed accident analysis information, nor does it show in great detail which factors caused the accident. It mainly describes what happened and what were the consequences together with some general remarks about the causes.
The chain of events in the operational process, leading to the accident is briefly described in the Facts database. However, whether these events were present before the accident occurred is not indicated. So, to retrieve possible deviations and their

frequency, the underlying data has to be consulted. The 'underlying data,' used for this analysis includes all available information from whatever source.

From working and using the database in respect to this study, some general and more specific recommendations were derived:

- Increase the accessibility of FACTS by converting the database from a DOS to a Windows environment.
- Make the underlying data available if possible within the limitations of confidentiality.
- Show the (root)causes (technical, human, organizational) of the operational deviations leading to the accident. For example by classifying the (root)causes using the 7-stage protocol or other existing method.

Only the accidents rated with 5 stars (most complete information) are used for this research. In total 260 accidents were shown as 5-star accidents. From these 260 accidents, 91 occurred between 1995 and 2002. In these 91 accidents, 21 accidents involved transport by road, water, rail, or air. As those accidents did not impact on the chemical process industry they were excluded from the analysis. The 70 remaining accidents were distributed all over the world as can be seen from Figure 12. Please note that this figure does not represent the geographical distribution of all accidents in the world, it merely represents a sub selection of FACTS accidents.

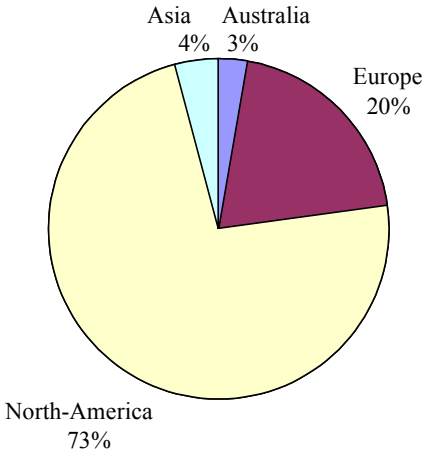


Figure 12 Geographical distribution of investigated accidents.

To provide some additional information regarding the 70 accidents, the activity or 'mode of operation' during which the accidents occurred is shown in Figure 13. From other accident research, for example Khan (Khan et al., 1999), generally similar ratios between modes of operation and maintenance/cleaning were found when an accident occurred. Khan (Khan et al., 1999) showed from analysis of accidents due to releases from pipe work and in-line equipment that the most dangerous modes of operation are 'normal operation (39%)' and 'maintenance (17%)'. The percentages are lower than presented here, because 19% of cases the mode of operation was unknown. They concluded that, on average less time is spent in 'maintenance' mode than in 'normal operation' mode of an installation implying that 'maintenance' is a very important mode of operation regarding safety.

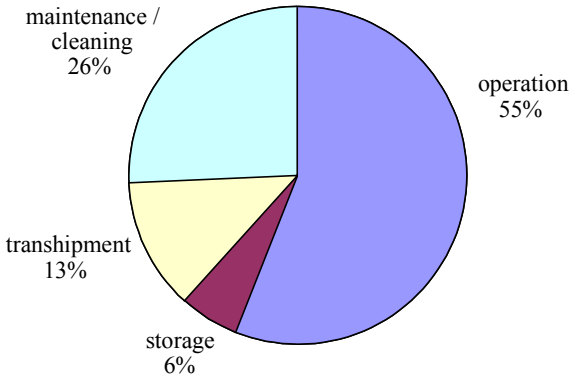


Figure 13 Site 'mode of operation' at the moment of accident for investigated accidents.

The next sub-Section will use this collection of accidents to identify the events present in recent accident trajectories.

3.2.2 Events in recent accident trajectories

From hindsight analyses of accidents by Heinrich (Heinrich, 1959), Turner (Turner, 1978), Leplat (Leplat, 1987), Reason (Reason, 1997), etc., it is known that failures or deviations in normal operations are present prior to, and are directly related with, an accident. From hindsight analysis as reported in FACTS, the failures or deviations as well as the accident trajectory or causal path, of 70 accidents are known. To derive the risk coverage area these deviations, are placed in the risk matrix. The only deviations taken into account are those which occur in the operational process and are part of the accident trajectory or causal path prior to the critical events as described in FACTS. So the 'latent' conditions lying behind these operational deviations as described by Reason (Reason, 1997) are not yet taken into account but will be discussed in the following Chapter.

Tweeddale (Tweeddale, 1995) identified two general sorts of deviations, i.e. 'hard' and 'soft' deviations. He identifies 'hard' deviations as malfunctioning equipment, and 'soft' deviations as faults in the system or procedures. In this thesis these definitions are slightly modified to cover all deviations identified in the operational process preceding and directly related with an accident. 'Hard' deviations are defined as the actual loss of containment or demonstrable loss of control, e.g. small leakages, overpressure, override of control systems, etc. 'Soft' deviations refer to indications of possible deviations, but cannot be demonstrated by actual facts, e.g. operator complaints, deficiencies of maintenance activities, or bad housekeeping activities, etc.

Using these definitions of deviations, 'hard' and 'soft' deviations were found in the causal path prior to the critical events of the 70 accidents. In total 158 'deviations' were derived from the operational process. These deviations consist of 48% hard and 52% soft deviations.

At first sight many more soft deviations were expected to be found compared to hard deviations, because from accident analysis it is known that in many cases, events triggering the accident are very often human errors, Reason (Reason, 1997). However, considering that soft deviations are often not explicitly reported or known, it makes sense that more hard deviations are present. Retrieving soft deviation information is

more problematical because it can only be achieved by interviewing the people involved and exposing the 'normal way of working' for a long time span prior to the accident. It is therefore assumed that in the daily operation more soft deviations can be identified than could be done by using FACTS.

In the next sub-Section the risk coverage area of the 158 deviations will be determined.

3.2.3 Risk coverage area of deviations prior to accidents

To derive the risk coverage of the identified deviations in recent accident trajectories, the likelihood and the consequences of these deviations must be identified. The definitions of the likelihood and consequences are identical to the definitions used for the construction of the risk coverage area of the pro-active SI's. The likelihood of the deviations is established by the actual occurrence of events. If events occur rarely or often, the likelihood is low or high respectively. The consequences of the deviations are established by the perceived consequences regarding safety of the selected deviation. If the deviation was known to have 'direct' consequences for safety, the deviation is classified as a 'high' consequence deviation. When the deviation had either no 'direct' consequences for safety, or merely in an 'indirect' way, the deviation is categorized as 'low.' Examples of deviations with 'high' consequences that are 'directly' related to safety are: damage to or the malfunctioning of high-risk equipment, leakage of hazardous substance, or injury to people, etc. Examples of 'low' consequence deviations ('indirect' safety related consequences) are: the malfunctioning of, or damage to non-critical equipment, problems with operational performance such as product quality problems or backlog of maintenance, etc.

The 158 deviations found are positioned in the risk matrix shown in Figure 14, where the grey area represents the risk coverage area. Note that the results are given in quantitative terms, i.e. in percentages, in contrast to the risk coverage area given in Figure 11. No further attention to the reliability of the results is paid due to the fact that access to the accident database is restricted and retrieving the appropriate information from the accident database to derive the risk coverage area is very time consuming. Moreover, the author repeated the analysis several times, with large time spans between the analyses, slightly adapting and eventually retrieving the results shown in Figure 14.

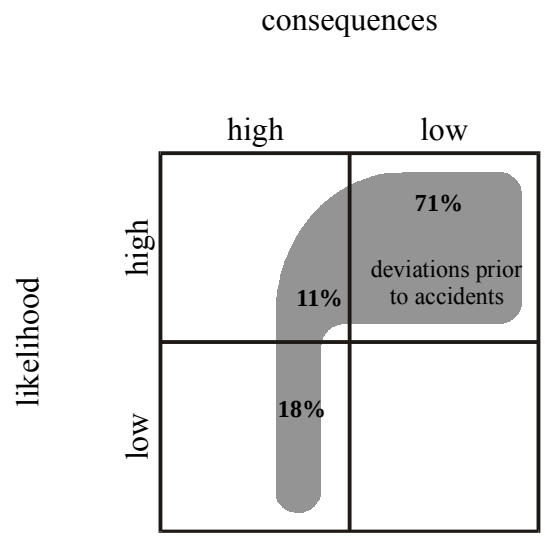


Figure 14 Risk coverage of deviations prior to accidents derived from FACTS.

Most deviations (82%) belong to the 'high likelihood' category, i.e. they are frequently re-occurring deviations. Most of these deviations (71 %) have 'low consequences' implying that they are signs indicating events that are not directly related to safety consequences.

In the next Section this risk coverage area will be compared with the one of the SIs.

3.3 Gaps between pro-active SIs and deviations prior to accidents

Both the risk coverage areas of the SIs and of the deviations prior to accidents, as discussed in the previous Section are depicted in Figure 15.

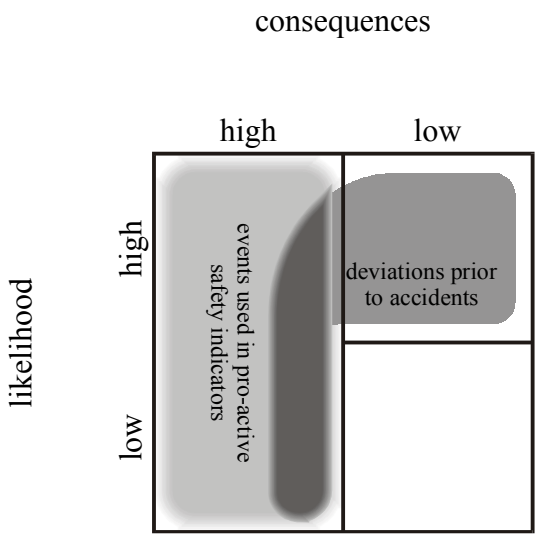


Figure 15 Risk coverage areas of SIs and of deviations prior to accidents.

From Figure 15 it can clearly be seen that there is a gap between the risks covered by the SIs and the risks that can be deduced from the deviations prior to accidents present in daily operations in the chemical process industry.
Deviations belonging to the category 'high' likelihood and 'low' consequence are rarely taken into account when constructing pro-active SIs, even though it is this

category of deviations that has been mainly responsible for causing recent accidents. Re-occurring deviations (high likelihood), which do not have a direct safety related impact (low consequence), are often the type of deviations that can be identified prior to an accident.
It appears that in constructing pro-active SIs, a specific class of data has not been retrieved from the operational business process in chemical process industry. This specific class of data is of re-occurring deviations in daily operations that do not have direct consequences for safety.
Examples of these re-occurring 'low consequences' deviations are: 'minor' damage of non-critical safety equipment, operator complaints, maintenance problems, quality problems, etc. Examples of 'high consequences' deviations (that are covered by the current pro-active SIs) are small leakages of hazardous substance, damages to or the malfunctioning of safety critical equipment, violation of safety guidelines and procedures, etc.
To clarify the difference between 'low consequence' and 'high consequence' deviations further, an example from FACTS (FACTS, 2002) is presented here.

In 1999 a pump exploded and 2000 litres of nitrous oxide spilt from a storage tank. The investigation report highlighted that the causal path of the explosion was: a valve which had been wrongly positioned by a repair firm; subsequently a wrong setting of this valve by the operator prevented the pump from cooling properly; the pump bearing overheated causing an explosive decomposition of N_2O vapours inside the pump. This resulted in 2000 litres of N_2O entering the sewer-wells. Moreover, emergency escape exits had been closed or blocked but fortunately the event did not result in any personal injury.
Before the accident, the bearing had overheated on a number of occasions and nearly always broke and had to be replaced. However, the recommendations of the report of the accident investigation were not aimed at preventing the re-occurring overheating issue, but amongst others on improving training procedures for the operators to spot the wrong valve settings and establishing procedures and rules to communicate with the repair firms. The company was fined because the sewer-wells were in a forbidden area, and the escape routes had not been checked and maintained periodically, resulting in the blocked and closed escape doors.
More than two years later a similar accident occurred in the same company, again the pump bearing overheated but on this occasion it was not the pump which exploded but a tanker refilling at a storage tank. The explosive decomposition had not been stopped by the cold transportation hose, as in 1999, which allowed it to enter the vehicle's tank and explode. The explosion caused injury to 11 people and severe damage to the immediate surroundings.

This example shows that the focus was put on deviations that have 'direct' safety related consequences ('high consequence' category), such as violation of safety procedures or shortfalls in safety training. However, the normal operation in which this ('indirect' safety related) overheating deviation occurred had not been identified as relevant ('low' consequence category). Finally this re-occurring deviation caused a 'similar' accident only this time with more severe consequences.
The severity of the latter event resulted in a more thorough accident analysis which finally identified the cooling problem as relevant and subsequently resolved it. Thus the 'indirect' safety related deviation that re-occurred was the overheating of the pump bearing. Although this information was not used in the construction of pro-

active SIs, it was clearly a sign for the serious accident that finally happened. The 'direct' safety related deviations are: the wrong setting of the valve, the escape doors being blocked, the presence of sewer-wells in a forbidden area, etc. These deviations were represented in SIs by means of safety instructions and regulations.

This example shows how 'low consequence' deviations are ignored and are not covered by the SIs in current chemical process industry. However, in practice not all 'low consequence' deviations are missed by the SIs as will be discussed in the next Section.

3.4 Discussion of the analysis

The risk coverage area of the pro-active SIs is determined in a straightforward way, without taking exceptions into account. These exceptions from practice and their influence on the results are discussed in this Section.

Some further explanation must be given here, because in practice some SIs encompass 'low consequence' deviations. For the 'known' risks type of predictive SIs it is obvious that they only cover 'high' consequence' deviations in the risk matrix. 'New' risks type of predictive SI's are developed to encompass 'indirect' safety related deviations (i.e. 'low consequence' deviations). Though, in practice these deviations are often excluded from the predictive SIs tools as Bayutt (Bayutt, 2003) shows; encompassing such 'indirect' safety related deviations is perceived as a waste of resources and attention is distracted from more important scenarios.

However, the current monitoring SIs are focused on the 'direct' safety related deviations. Consequently, frequent deviations with no immediate safety related consequence are not listed nor monitored.
Similar remarks can be made about accident reports, it was observed that the focus of the majority is on the 'direct' safety related deviations in the accident causation path, and almost no attention is given to the 'indirect' safety related deviations. 'Indirect' safety related deviations were mentioned but no attention was given to the fact that these deviations were in the causal path, re-occurring, and often present for a long time prior to the accident. Körvers (Körvers et al., 2002) gave some good examples by showing ten cases in which identical 'indirect' safety related deviations present prior to accidents repeatedly caused 'similar' accidents.
'Direct' safety related deviations were discussed thoroughly and extensively and special attention was concentrated on the safety procedures and rules which the company or its employees violated. It was only these violations that were discussed extensively and not that the 'indirect' safety related deviations which were common in the company. Rasmussen explains this fact by saying; ' ...there is a tendency to see what you expect to find…,' as was stated in Bourrier (Bourrier, 1998). Accident investigators are often safety experts and people from justice departments. Consequently they focus on safety procedures and activities that have been violated. So as Rasmussen (Rasmussen, 1997) stated; '…when rules, laws, and instructions, which are practically speaking never followed to the letter, are judged by these investigators, the focus will be on blaming people or companies…,' and not on the underlying causes of why these rules are always violated, as for example discussed by Clarke (Clarke, 1997) or Reason (Reason, 1997).

From the accident analysis it seems that accidents are often preceded by a high frequency of indirect safety related deviations. Note that from here on it is important to take hindsight-bias into account, when re-analysing from hindsight, which will be further explained in Chapter 6. Though this reasoning can be validated from accident analysis, this does not automatically mean that the opposite reasoning also applies, i.e. high frequent indirect safety related deviations signal accidents. Indicating which deviations will actually lead to an accident is impossible. As Reason (Reason, 1990) clearly states enormous amounts of 'active failures' resulting in enormous amounts of deviations are present, though the causes (the latent conditions) are limited and they have to be addressed. However, a distinction can be made of which deviations are more likely to evolve into an accident than others. This likely-to-evolve-into-an-accident class of deviations identified in this Chapter, will enable companies to: better indicate accidents, focus their limited resources and to retrieve the underlying causal factors.

From this analysis a hypothesis posed as follows can be derived: *Frequently re-occurring deviations, present in the operational process of an organization, can be identified in the causal path of an accident*. Subsequently, a prediction can be made, that the hypothesis will be valid in many cases. The final test of this hypothesis, confirming or disputing it, will be done in Chapter 6, where several accidents will be analysed on re-occurring deviations present in the accident trajectory.

In the next Section the implications of this analysis for developing a method which can serve as a pro-active safety risk indicator are shown.

3.5 Implications of the analysis

From the analysis performed it appeared that high frequency deviations that are perceived as indirectly safety related are often present in accident trajectories, although, they are not used by current pro-active safety indicators. This observation seems to be an important requirement for methods pro-actively indicating safety risks. Van der Schaaf (Schaaf van der et al., 2004) confirmed this observation, by showing that even in a High Reliability Organization (HRO) a near-miss reporting system failed to retrieve all safety relevant deviations, because operators do not report deviations which they perceive as only indirectly safety related. In the study performed by van der Schaaf, the frequency of the daily deviations was not taken into account. However, the study was based on small daily deviations and therefore all deviations automatically have a high frequency. Wagenaar (Wagenaar et al., 1997), retrieved further requirements a method indicating safety risks must have. First, the aim of a safety risk indicating method must be a reasoned listing of aspects in the operation that should and can be changed. This implies a methodological search for elements which reveal the (root)causes of possible accidents clearly and which is not exposed to personal subjectivity. These elements must be systematically present inside the operation and are not of any temporary significance. Furthermore, there must be a clear cause-effect relationship from operational risks to these systematic elements. Tixier (Tixier et al., 2002) argued that additionally the: feasibility of methods (often requiring specific training); risk hierarchisation of the results; link between human factors and risks, and the ability to include both the specificities of cases and to transpose the method to other cases, are very important but often missing. Suokas (Suokas et al., 1993) adds next to the above mentioned requirements, the

importance that methods indicating safety risks must have the ability to generate a general overview, show the link between risk reduction and operational benefits and uses limited resources.
Summarised, the important requirements for methods indicating safety risks are formulated as methods must:

- use *operational deviations*, which are *directly safety related*, but also high frequency deviations, which are *not directly safety related* as basis for the input,
- have the ability to *provide a general overview* of problems to compare them with other organizations,
- have the ability to *provide detailed cause-effect relationships* showing how problems arise and how they can be solved,
- be *feasible*, without requiring specific training,
- have a simple and clear structure or guidelines, increasing the *reliability* of the results and reducing the subjectivity,
- use *limited resources* in terms of time and money,
- be able to *rank the results*,
- provide a clear *link* between *risk reductions and a more effective normal way of working*; operational benefit.
- *include* linkage between *all (root)cause areas* (technical, human, and organizational interrelated).

Subsequently, three methods indicating safety risks will be evaluated on these nine criteria discussed above: whether indirect safety related operational deviations are used, general conclusions can be derived, detailed cause-effect relationships are available, the method is feasible, the results are reliable, only limited resources are needed, the results can be ranked, a clear link between risk reduction and operational benefit is present, and if all (root)cause areas are included.

The last requirement, i.e. if all (root)cause areas are included, was used to retrieve three pro-active methods indicating safety risks. All three methods address the entire socio-technical system (technical, human and organizational). These three methods are used to construct a new pro-active method of indicating safety risks, which includes the benefits and addresses the limitations of these three existing methods. The three methods evaluated are: MORT, Johnson (Johnson, 1980), TRIPOD, Hudson (Hudson et al., 1991), and PRISMA, van der Schaaf (Schaaf van der, 1992).

MORT:
The MORT analysis was developed for the U.S. Energy Research and Development Administration as a safety analysis method that would be compatible with complex, goal-oriented management systems. MORT is a diagram which arranges safety programme elements in an orderly and logical manner. It presents a schematic representation of a dynamic, idealized safety system model using a fault tree analysis methodology. Suokas (Suokas et al., 1993), discusses in detail the MORT method and its benefits and restrictions. The benefits regarding the requirements stated above are that the method gives a general view of the problems and also provides cause-effect relationships leading to developmental needs of an enterprise or an operating section. The restrictions regarding the requirements stated above are that the method does not identify immediate risks caused by mechanical faults or process disturbances.

Furthermore, suggestions for remedies often need further development. The method is time consuming and requires great expertise from the user, in order to reduce subjectivity. The method starts from production activities and links safety to it, but does nothing to increase the control of the normal way of working. According to Groeneweg (Groeneweg, 1998), the method does not make a selection on the basis of risk potential, effectiveness, or costs.

TRIPOD:
TRIPOD was developed by a research group from the Universities of Leiden and Manchester in a project sponsored by Shell International Petroleum Maatschappij. From close observations of various organizational activities, a limited set of 11 general failure types (GFTs) was derived. A GFT can be derived by using one of the 130 interchangeable checklists. When all GFTs are derived and globally rated failure state profiles can be constructed which identify the GFTs which have the highest number of contributions to an accident. The benefits regarding the requirements stated above are that the method gives a general view of the problems (in terms of failure profiles) and ranks these results. Furthermore, high reliability in practice is achieved by using straightforward checklists, which limits the resources needed. The restrictions of the foregoing requirements are that the method does not use actual operational deviations and no causal relationship between deviations/problems and (root)causes can be established, which makes it impossible to derive specific remedies. Correspondingly, due to the lack of detailed cause-effect relationships, a link to the normal way of working is not made visible. Finally, special training to apply the method in practice is needed.

PRISMA:
PRISMA is a pro-active method indicating safety risks developed by van der Schaaf (Schaaf van der, 1992). The organizational area was extended by van Vuuren (Vuuren van, 1998). In this method causal factors are derived from incidents in the operational process, via a fault tree technique. These causal factors are classified in three major areas, i.e. technical, human, organizational, which exists in a total of 20 causal factors. After analysing sufficient incidents to produce a stable 'PRISMA-profile', the causal factor having the highest contribution is identified as the target for improvements. Finally, generic solutions for these causal factors are available in a so-called Classification/Action Matrix, van der Schaaf (Schaaf van der, 1992). The benefits regarding the requirements stated above are that a general ranked conclusion is retrieved by showing an overview of which causal factors contributed most to the incident. The fault tree provides detailed cause-effect relationships, showing how problems arise and can be solved. The method requires little specific training and is very straightforward and reduces subjectivity. The limitations regarding the requirements stated above are that the method starts out collecting only perceived safety related incidents for analysis. Even though over time, a much wider range of reported incidents are collected, e.g. equipment failures, quality related issues, etc., companies often do not use this potential and only focus on collecting the perceived safety related incidents, Kanse (Kanse, 2004). Moreover, analysing safety related incidents takes time and can therefore not always be directly related to the normal way of working.

An evaluation of the three pro-active methods indicating safety risks discussed so far is shown in Table 5.

Table 5 Evaluation of different methods indicating safety risks.

	usage of indirect safety related operational deviations	general conclusions	detailed cause-effect relationship	feasibility	reliability	limited resources	rank results	clear link between risk reduction and operational benefit
MORT	-	+	+	-	-	-	+/-	+/-
TRIPOD	-	+	-	-	+	+	+	-
PRISMA	+/-	+	+	+	+	+/-	+	+/-

From this analysis it appears that a huge discrepancy exists between deviations prior to accidents, that can be found in 'normal operation' and the pro-active safety indicators and methods in current use. The re-occurring indirect safety related deviations that are the dominant class of events causing accidents are therefore defined as the precursors for accidents, as stated in Chapter 1. Furthermore, from Table 5 it can be concluded that a clear link between risk reduction and the normal way of working is not explicitly present in one of the three methods. Finally, the feasibility of methods (except PRISMA) needs some attention; additional expert knowledge is often necessary to apply the method. The focus of the method indicating safety risks developed in this thesis will lie especially on these three criteria.

Therefore, Chapter 4 will give a detailed definition of these precursors and a way to identify them in practice. Moreover, causes for the occurrence of these precursors will be identified to retrieve a better understanding of why accidents still occur, and this will be closely linked to the normal way of working. From these concepts a model will be developed which can approach practice in a straightforward pro-active way, without the need to possess any expert knowledge and which provides 'clear' directions for improvements in identifying safety related risks.

Chapter 4

SAFETY BY CONTROL

In order to find the organizational causes of precursors of accidents in the operational process, as identified in the previous Chapter, a model of this operational process has to be derived. In this Chapter an operational control model will be derived for analysing precursors. Next, the concepts 'precursors,' 'operational process,' and 'control' will be defined and explained. Moreover, the link between the operational control model and safety will be explained. Finally, a preliminary approach for applying these concepts in practice will be presented.

4.1 Precursors

In the previous Chapter it was shown that most accidents are preceded by deviations in the operational process, e.g. Heinrich (Heinrich, 1959), Turner (Turner, 1978), Leplat (Leplat, 1987), Reason (Reason, 1997), etc. Additionally, it was shown that a specific class of deviations is present which is not covered by current pro-active safety indicators. These deviations are characterised by a high likelihood and low perceived safety related consequences and were defined as precursors and re-occur in the operational process of the organization prior to an accident. In order to find these deviations in a real life operation and to eventually find their underlying causes, the concepts of re-occurring deviation and operational process have to be explained in more detail. The various definitions and concepts derived in this Chapter are necessary to understand the next Chapters, which shows how they are applied in practice.

4.1.1 Organization and operational process

To define an operational process, the concept organization, in which this operational process can be found, has to be explained. To understand the concept organization, some history of how to obtain more understanding of a complex concept as organization has to be discussed. The natural scientific method of studying a complex problem is to divide the problem into as many parts as necessary to reduce its complexity and solve the individual parts, from which subsequently the complex problem can be solved. This approach, which is called reductionism, has no success when analysing organizations, as is stated by Checkland (Checkland, 1991). The relationships between the individual parts are more important in solving the problem than the parts themselves. Examples of problems when analysing organizations are amongst others, the identification of relevant elements and the establishment of a problem-boundary, etc. The most important problems are the people because they are at the centre of an organization including different beliefs and purposes, different evaluations of problems, self-fulfilling prophecies, etc. According to Checkland (Checkland, 1991), systems thinking was the reaction to the failure of the natural science to solve complex real-life problems in organizations. The systems approach thinking uses holism rather than reductionism and uses models instead of experiments to understand a complex problem. Therefore, the systems approach is used in this thesis in order to better understand an organization.

In ‘t Veld (Veld in ‘t, 1999) represented an organization as a system, being a collection of elements, relationships between the elements themselves and relationships between the elements and the environment. An organization exists because it fulfils a specified function in its environment. To create this function by means of a system, processes are required. A definition of a process, which is adopted from Davenport (Davenport et al., 1990), is a set of logically related transformations to achieve a specified function or output. This specified output is often described more explicitly as the product that is created by the process. Furthermore, one has to consider that organizations aren’t just aimed at a specific output or goal, but strive for survival by responding to their environment, as stated by von Bertalanffy (Bertalanffy von, 1968). The specified output of a system can change according to the needs of the environment, which he called an open system. An open system depends upon its environment and both system and environment are in a state of mutual influence and interdependence. In contrast a closed system is self-containing and ignores the influence of its environment.

To define a system, a clear ‘system border’ has to be present between system and environment. However, this ‘system border’ depends on the scope of the researcher, in ‘t Veld (Veld in ‘t, 1999). A system’s view of an organization is shown in Figure 16. This system’s view of an organization will be used in the remainder of this thesis.

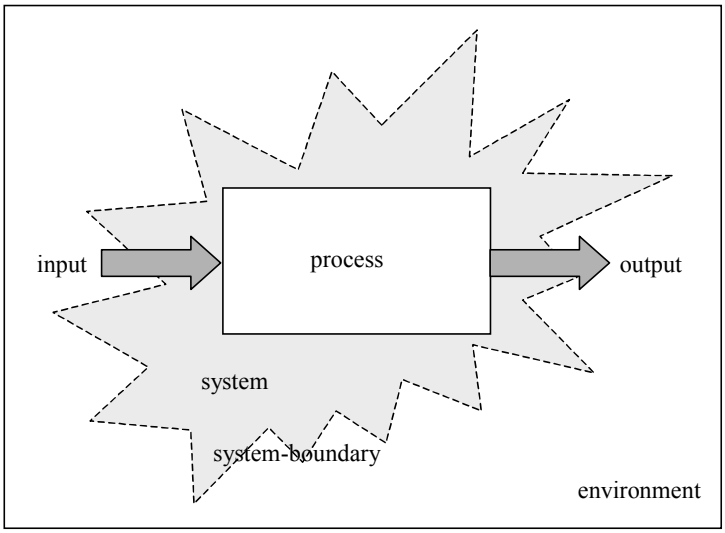


Figure 16 An organization in a system’s view

In an organization, represented as a system, multiple processes are present. The process responsible for realising the primary output or function needed to satisfy the environment is called the *primary process*. This function can be manifested physically as goods, or in a none-physical way as services.
To achieve the transformations inside a process, to create the primary output or product, resources are necessary. *Resource* is the term for all the means required to produce a product. Falster (Falster, 1997) distinguishes two types of resources: *durable* and *non-durable*. Durability determines if resources are part of the system. Durable resources (machines, tools, humans) are part of the system, they can be re-used. Non-durable resources (raw material, partly manufactures items) leave the system after transformation and by definition cannot be re-used. A special class of durable resource is human.

The process responsible for taking care of the resources is called the *secondary process*. Examples are maintenance or internal transportation, and the personnel department, material purchase, etc. Finally there is a *tertiary process* present in an organization, that directs and co-ordinates the primary and secondary processes, and their relationship with each other and the environment.

The *operational process* consists of the primary process and the secondary process directly interacting with the primary process, e.g. maintenance, internal transportation, etc. The precursors, identified in the previous Chapter, were re-occurring deviations in this operational process. When working with hazardous substances or performing transformations under special conditions (e.g. high pressure or extreme temperatures) unintended deviations can occur, and harm towards humans, environment or assets can be the result. These unintended deviations are the events triggering conditions that may result in an accident. A deviation can be distinguished in practice if the ongoing operational process or intermediate states in the operational processes deviate from a reference. These references in an organization are the organizational values and norms, which are the organizational objectives, settings or constraints for performance. The next sub-Section will elaborate further on establishing these organizational values and norms to further clarify the concept of a deviation.

4.1.2 Organizational values and norms

Argyris (Argyris et al., 1996) refers to an organization as individuals who can decide and act on behalf of a collectivity. In order to achieve this boundaries have to determine when an individual is authorised to act. By establishing rule-governed ways of deciding, delegating, and setting boundaries, the so-called theory of action is created according to Argyris. This theory of action is present in two ways; in the way of an 'espoused theory' and in the way of a 'theory-in-use.' The 'espoused theory' is the theory of action which is able to explicitly justify the followed pattern of activities. The theory-in-use is the theory of action which is implicitly present in a pattern of activities. This theory-in-use is the actual way individuals act in an organization, which may not always match the organizational 'espoused theory.' For example an organization's documents of policy statements, organizational flow charts, work orders, etc. contain elements of 'espoused theory of action,' which sometimes differ from the actual activity patterns, i.e. the 'theory in use'. Summarising, the espoused theory in an organization will not always be read or followed to the letter and consequently the organizational theory-in-use may or may not match the organizational espoused theory.

The fact that organizational values and norms are not simply a set of rules and procedures is shown by introducing the espoused theory and the theory-in-use and this has to be taken into account in the remainder of this thesis. A possible graphical representation to take organizational values and norms into account is given in Figure 17, which is derived from SADT (Structured Analysis and Design Techniques), SofTech (SofTech, 1976).

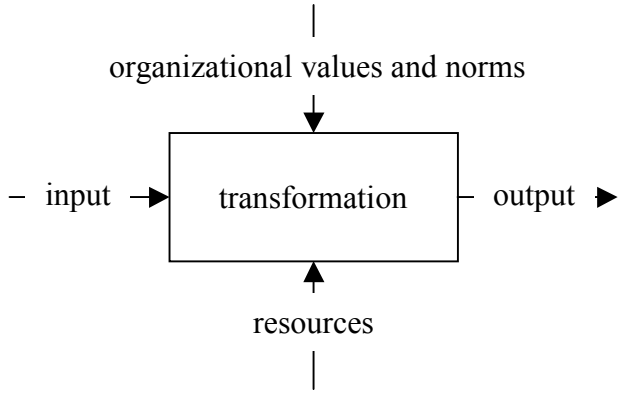


Figure 17 General representation of an organization derived from SofTech (SofTech, 1976).

Please note that the process from Figure 16 is replaced by a transformation. The process or transformation represents where input and resources are consumed by transforming them into the output, under the constraints of the organizational values and norms. The upper arrow represents the organizational values and norms. The lower arrow represents the durable resources, divided into human and non-human resources such as machines, etc. The arrows depicted left and right of the transformation are the non-durable resources.

Having a set of organizational values and norms, a deviation in the operational process can now be defined. In this thesis a definition of a deviation in the operational process, *is the transformation and its input, output or resource that deviates from the individual's expectations that are rooted in his or her image of the transformation's theory-in-use,* Koornneef (Koornneef, 2000). However, a *deviation, is also obtained when a transformation and its input, output or resource deviates from the transformation's espoused theory*.

Please note that one theory-in-use might differ from other theories in use of the same transformation, because different individuals will hold different images of the prevailing theory-in-use, so they will judge specific situations in a distinct matter.
Having set a definition of a deviation, the concept of a re-occurring deviation will be further explained in the following sub-Section.

4.1.3 Re-occurring deviations

In the end of the previous Chapter, a precursor was defined as a re-occurring deviation in the operational process. The concept of a deviation in an operational process was stated in the previous sub-Section. However, the concept of a re-occurring deviation will be explained in this sub-Section.

Theoretically, a re-occurring deviation means at least one re-occurrence of an identical deviation i.e. the conditions and the deviations themselves must be the same. Consider the following example: a safety valve becomes clogged during the mixing of product A. Whilst another safety valve also becomes clogged during the filtration of product B. Are the deviations (clogged safety valves) identical? In both situations there is a clogged safety valve. However, the conditions differ (different transformations, products, operators, etc.). The theoretical answer is no because a

deviation is only considered to be re-occurring when identical values and norms, identical resources, identical input and identical output are present, and a second identical deviation in the input, output, or resource of the transformation occurs (see Figure 17). Theoretically, identical means that the deviations must be the same in every detail (on the lowest possible aggregation level). However, in practice by influences from the external and internal environment, none of such identical conditions and identical deviations exists. Determining an identical deviation in every detail is almost impossible. Identical often stops at a certain level of detail. For example: a pump was said to have broken down three times, while actually the first time the bearing broke, the second time the seal leaked and the third time the shaft broke. On the aggregation level of the broken pump all three deviations appear to be identical. However, on a more detailed level all three deviations are quite different.

In practice, only a limited level of detail is considered. Moreover, when looking at the re-occurring deviations identified in accident trajectories in the previous Chapter, they were signs of something wrong. The vast majority concerned re-occurring deviations on a high aggregation level, re-occurring under many different conditions. So it must be noted that when identifying re-occurring deviations, a 'too tight' definition of 'identical', results in problems in identifying re-occurring deviations, e.g. identical deviations do not exist if every detail has to be considered.

Considering both theoretical and practical criteria, a definition for a *re-occurring deviation* is formulated in this thesis: *subsequent deviations with equal value to the first deviation, occurring in an equal input, output, or resource, on the lowest aggregation level as recorded in a company*. An example to clarify this definition is depicted in Figure 18.

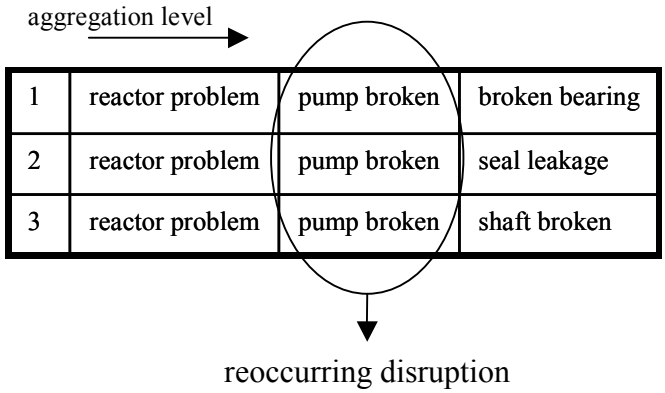


Figure 18 An example of identifying a re-occurring deviation.

Figure 18 shows a list of three deviations, at different aggregation levels. At the highest aggregation level (lowest detail), all deviations are equal, on the lowest aggregation level (most detailed level), all three deviations differ. Thus a re-occurring deviation is identified on the lowest aggregation level as present and where all three deviations are superficially equal.

A re-occurring deviation can be defined as: multiple deviations from the transformation's theory-in-use, or espoused theory, equal to each other on the lowest aggregation level as recorded inside a company, all occurring in the same input, output, or resource of the transformation.

In this thesis a more precise definition of a *precursor* is given, namely a re-occurring deviation in the operational process with the potential to cause an accident. Please note that the existence of a precursor does not imply that an accident will occur. As already mentioned in the previous Chapter and by other authors like Hale (Hale et al., 2000), some deviations appear only once and immediately result in a catastrophe, while others appear frequently but can only escalate into an accident with great difficulty. Although the presence of a precursor doesn't always imply the occurrence of an accident the analysis of recent accidents in the previous Chapter showed that accidents are often preceded by such precursors. When applying this definition of a precursor to the results of analysing the 70 accidents it appeared that in five cases no precursors could be identified from the information available in the FACTS database. In four of these five cases the accident was caused from outside the company: shooting with a rifle at a pipeline, drunken people driving into a pipeline, an arson attack on a storage depot of a chemical company and an earthquake at a chemical company. The remaining accident was so complex that the actual causes could not be uncovered, all possibilities known to experts were ruled out and the actual causation path of the accident so far remains unknown. From these examples it can be seen that accidents without a precursor in the accident trajectory are scarce and often caused by a direct relation with the external environment, such as arson attacks by criminals. These accidents did not happen because of deviations inside the operational process. It can be concluded that by defining a precursor as a re-occurring deviation in the operational process, a category of accidents is excluded from this study, i.e. the accidents that occur without any precursor in the accident trajectory.

In the previous Chapter hindsight was used to find the 'precursors' leading to the particular accidents. The accident trajectory was retrieved after the accident had occurred. To discover the accident trajectory prior to an accident is extremely difficult. This requires that all 'precursors' are taken into account, because as the actual accident trajectory is not known beforehand, nothing can be left out. Taking all precursors into account is, however, impossible, therefore the next sub-Section will elaborate further on taking 'all' precursors into account. In an operational process, all kinds of deviations can be found e.g. deviations within maintenance, quality, safety, etc.

4.1.4 Aspect and sub-systems

To find the precursors in an organization, further insights into the different types of relations in an organization are necessary. A process can be divided into smaller parts, called sub-processes. In this way, the complexity of the system can be reduced. The smallest distinguishable parts, or entities as in 't Veld (Veld in 't, 1999) called them, are tasks or activities. An activity or task is the smallest part of a process that requires resources. The boundaries of a task are indicated by a change in these resources. This division of a system into smaller parts of increasing detail, is a division into sub-systems. A sub-system is a sub-collection of elements (processes or activities) inside the system in which all original relations between these elements are preserved, de Leeuw (Leeuw de, 1986). The elements inside a sub-system are all of identical aggregation or detail level, see Figure 19.

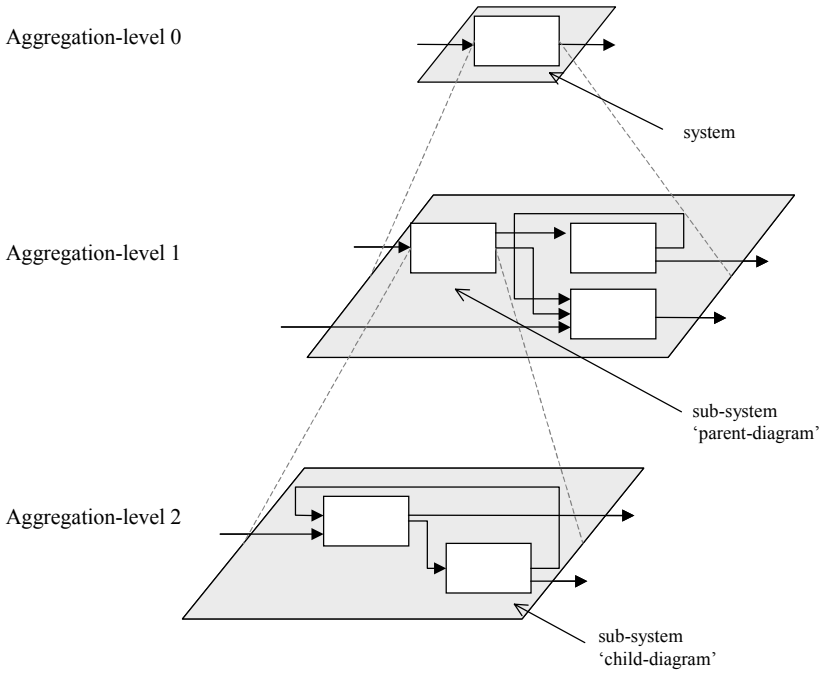


Figure 19 Dividing a system into sub-systems according to SADT, SofTech (SofTech, 1976).

The depicted method of dividing a system into sub-systems is taken from SADT, SofTech (SofTech, 1976). A level of identical detail is called an aggregation level in SADT. The highest aggregation level or least detail level is numbered 0, with each lower level the number ascends and the level of detail increases. SADT seeks to conquer the complexity of large systems in two ways: partitioning and hierarchical organization. The system, that is the collection of entities and their interrelations according to Cutts (Cutts, 1991), is seen as a black box. The user only needs to know the characteristics of the black box on a certain aggregation level but not how the system carries out its function in detail (i.e. on lower aggregation levels). In moving down the aggregation levels a more detailed insight is obtained, while moving up the aggregation levels gives a deeper understanding of the sub-systems' contribution or significance to the system, according to Mesarovic (Mesarovic et al., 1970). This process of 'system decomposition' can be repeated for successive aggregation levels until the level of activities or tasks is reached. De Marco (Marco de, 1979) describes the necessary consistency between different aggregation levels, which he describes as 'balancing.' This 'balancing' means that the 'parent' sub-system and its interfaces provide a context which completely bounds the 'children' sub-systems as can be seen in Figure 19.

Apart from dividing a system in different aggregation levels, or sub-systems, another division of a system can be created. A division into different aspects inside a system. As defined by de Leeuw (Leeuw de, 1986), an aspect-system is a collection of relationships between certain elements inside a system. An aspect-system is also called a partial system, which is actually derived from mathematics; i.e. in partial differentiation, the relationships between certain elements are assumed to be a constant factor, as is the case in an aspect-system.

In a system a single aspect can be seen in different sub-systems and vice versa in a single sub-system different aspect can be recognised. In Figure 20 in ‘t Veld (Veld in ‘t, 1999) shows how sub-systems and aspect-systems can be depicted in relation to each other.

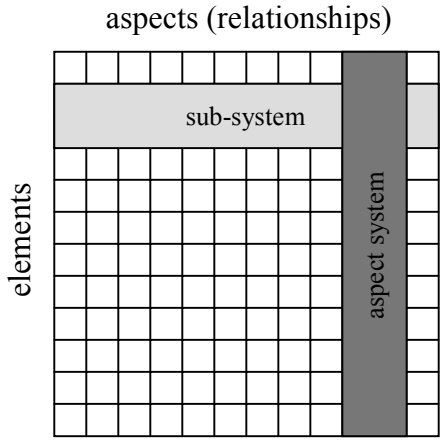


Figure 20 Sub- and aspect systems, in ‘t Veld (Veld in ‘t, 1999).

Figure 20 shows how an aspect-system is constructed from different elements all related by the same relationship and a sub-system constructed from different relationships all related by the same element.
In this research the focus is on the operational process, which is a sub-system in an organization, i.e. one element of the organization, with all relationships in the element preserved. Furthermore, in this sub-system different aspects are present. In this thesis the focus is on specific relationships between the element(s). Safety is one of these aspects.

Many authors (e.g. Visser (Visser, 1998), Kirwan (Kirwan, 1998a)) claim that safety is not a clear cut, separable part of the operational process. Many safety activities are interrelated with other activities from other areas within the operational process. So it is not possible for safety staff to operate at a distance from other aspects of the operational process, because detailed knowledge is required of different aspects of the operational process in order to fully understand safety, Seppala (Seppala, 1998). Studying the safety system as a separate aspect of the operational process will miss the important precursors, because precursors from other areas will not be taken into account and these may have a very important impact on safety. Therefore the focus of this thesis will be on the precursors in different aspects of the operational process, which were often missing in existing methods indicating safety risks. However, merely identifying these precursors is not sufficient, the organizational processes responsible for these precursors have also to be identified. This means that the co-ordination and control of the process must be addressed; the tertiary process. The way safety is integrated into these control processes provides more understanding why the current chemical process industry still experiences major accidents. As Hale (Hale et al., 1997) states, focus should be on certain elements in the operational process without losing the links with the system controlling this process. This controlling process provides a better understanding of the system-related mechanisms leading to precursors, which together with the socio-technical forces, Rasmussen (Rasmussen, 1997) sometimes escalate into accidents. To derive a model that links the precursors to their controlling processes, the concept of ‘control’ must first be addressed.

4.2 Precursors as a sign of ineffective control

The previous Section mentioned that safety is linked to the control concept and this is also known from literature: *risk management is a control function of maintaining a particular hazardous, productive process within the boundaries of safe operation,* Rasmussen (Rasmussen, 1997). If something is out of the boundaries of safe operation, an unsafe situation exists, which might escalate into an incident or accident. As Reason mentioned (Reason, 1991), these unsafe situations are themselves 'tokens' of failures in the management system. The SMS, as discussed in Chapter 1, has to execute a control function which ensures that unsafe acts are prevented or immediately alleviated if they occur. According to Reason (Reason, 1997) and Groeneweg (Groeneweg, 1998) this can be done by controlling the controllable failure 'types' in an organization and not the 'tokens'. However, as van der Schaaf (Schaaf van der, 1991) wrote as a response to Reason (Reason, 1991); …*with backtracking of 'tokens,' 'function types,' or even further 'source types' can be identified*. In fact many methods start by identifying 'tokens' to discover the dominant latent conditions, in order to identify the areas, to which resources have to be directed in order to improve the safety performance of the organization. Backtracking 'tokens' is fact determines where, why, and how control was ineffective. The answers to these questions enable organizations to identify their latent conditions and to react accordingly. However, to identify where, why, and how control is ineffective, the concept of control has to be defined. In the following sub-Section the origins and current understanding of the control concept will be given.

4.2.1 Control concept

Wiener (Wiener, 1948) and von Bertalanffy (Bertalanffy von, 1968) were the first to write about an open-system maintaining itself in a continuous inflow and outflow, in a so-called 'steady state.' Such a system needs regulation if the interacting parts of the system are not to give rise to chaos and disorder. An effective means of regulation is through feedback whereby information about the output of the system is compared with some predetermined goal. The margin of error becomes the basis for adjustments to the system in order to approach the goal more closely. In this way a system can be controlled or steered.

In the previous sub-Section the theory-in-action, defined by Argyris (Argyris et al., 1996), sets the targets according to which a deviation is resolved. In his control paradigm De Leeuw (Leeuw de, 1986) calls this theory-in-action 'the controlling process,' and he displays the task or transformation process as 'the controlled process,' as can be seen in Figure 21.

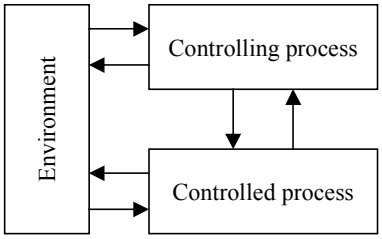


Figure 21 Control paradigm of de Leeuw (Leeuw de, 1986).

In this paradigm both processes, i.e. the controlled process and the controlling process, are influenced by their external and internal environment as Wiener (Wiener,

1948) and von Bertalanffy (Bertalanffy von, 1968) mentioned. Ashby (Ashby, 1956) added his 'law of requisite variety' which says that the variety in a system must be at least as large as the environmental variety if the system is expected to be able to regulate itself.
The next sub-Section will explain exactly what is meant by a controlling process, how it functions and what it represents.

4.2.2 An organizational control model

De Sitter (Sitter de, 1987), in 't Veld (Veld in 't, 1999), Argyris (Argyris et al., 1996), van Amelsvoort (Amelsvoort van, 1989), Keuning (Keuning et al., 1991) all developed models to represent a controlling process. Comparing these models, they mostly have four elements in common, i.e. steering, observation, judgement, intervention. These four elements comprise the theory-in-action or the controlling process, which is depicted in Figure 22 taken from van Amelsvoort (Amelsvoort van, 1989).

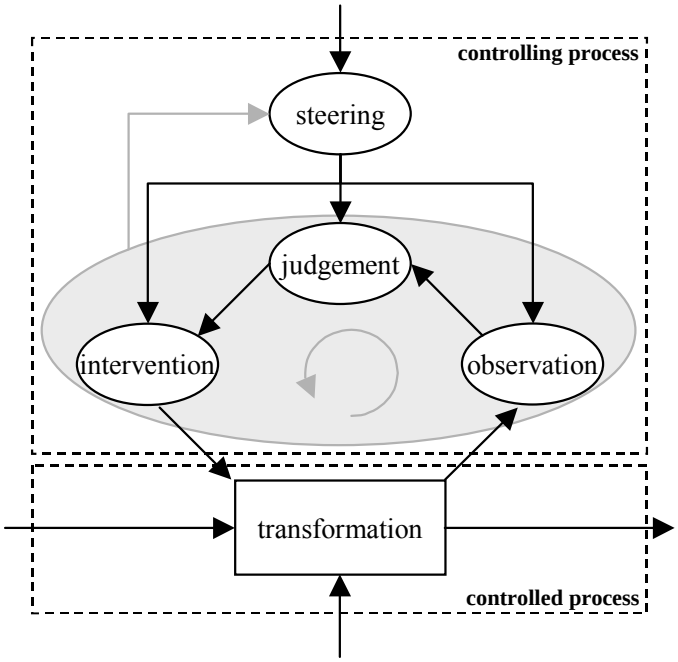


Figure 22 The controlling process, van Amelsvoort (Amelsvoort van, 1989).

Figure 22 is identical to Figure 17, except that the organizational values and norms are replaced by the more detailed controlling process. The steering element in the controlling process contains the organizational values and norms within which the controlled process (i.e. the transformation) must function and produce its output. The steering element sets the boundaries for the other elements of the controlling process; e.g. observation, judgement, intervention elements.
The purpose of the observation element is to monitor whether the transformation is performed according to the transformation's theory-in-use and espoused theory. In case of any deviation, relevant information will be transferred to the judgement element. Please note that the observation element actually measures any deviation of the inputs, resources and output of the transformation. The judgement element determines if an observed deviation is 'serious' according to the organizational values and norms present as espoused theory and theory-in-use. Subsequently, the judgement element decides whether or not to intervene and transfers this information to the

intervention element. The intervention element finally intervenes in the inputs, resources or output of the transformation to set the transformation and the output according to the organizational values and norms obtained from the steering element. In this model, the observation, judgement and intervention elements are also able to intervene in the steering element, questioning and eventually adapting the organizational values and norms that set the boundaries for the controlled process and in this way the boundaries for themselves.

4.2.3 Methods of control

Regulating the system according to its environment is the core function of control, van Amelsvoort (Amelsvoort van, 1989). This means that the system must adapt according to its environment. As discussed in Chapter 1, the external environment changes continuously and consequently the system must adapt to its environment in order to regulate itself, complying with Ashby's (Ashby, 1956) law of requisite variety. Kuipers (Kuipers et al., 1990) states that the regulation capacity has to be proportional to the regulation required to control the deviations present inside the environment. According to in 't Veld (Veld in 't, 1999) and de Sitter (Sitter de, 1987) there are two ways in which the system may adapt to its environment, that is: 'regulation of the transformation' and by 'adjusting the steering activity.'

Regulation of the transformation means, execution of the elements of observation, judgement, and intervention according to the transformation's theory-in-action or espoused theory. In literature two fundamental methods for regulation can be distinguished, which are called feedback control and feed forward control, de Leeuw (Leeuw de, 1986). Feedback control observes a deviation during or after the actual transformation. In case of a deviation, a judgement and intervention is performed at the inputs, outputs or resources of the transformation process after the observation and judgement activity has taken place. Feed forward control observes the inputs and resources of the transformation process prior to the actual transformation itself. In case of a deviation of the inputs or resources, a judgement and intervention is made at the inputs or resources of the transformation, before the actual transformation is performed.

Bateson (Bateson, 1972) defines the regulation of the transformation as '*single-loop learning,*' or '*single control loop*.' The organizational values and norms are kept unchanged. The underlying strategies and assumptions of action (observing, judging, intervening) may, however, change to correct the observed deviation and to reach the desired outcome set by the organizational values and norms.

The second way of adjusting to an external or internal environment (the elements in the system) is by adjusting the steering element. This can be done in two ways, by directly adjusting the steering element from outside the system (the external environment), or adjusting the steering element by triggers from the transformation's theory-in-use or espoused theory (the internal environment). The latter way of adjusting the steering element is called '*double-loop learning*,' or '*double control loop*,' Argyris (Argyris et al., 1996). Double-loop learning means that an extra loop is present in addition to the single-loop. This extra loop is present to question the organizational values and norms, which are the assumptions and the strategies underlying the theory-in-use and espoused theory.

4.2.4 Management and control

In practice the espoused theory will not always match the theory-in-use, as discussed in sub-Section 4.1.2. However, a perfect overlap of both theories means that observation, judgement, and intervention can be straightforward and problem-free. Landau (Landau et al., 1979) refers to this as 'control'. In other words, there is a fully rationalized plan of procedures that must be followed strictly because it is an accepted way of ensuring the organizational goals, and that the process is under control. However, if the environment changes (external or internal), the procedures are no longer adequate and the activities which need to be performed become uncertain and subject to a wide range of potential deviations. Still the organizational goals must be reached and requires what Landau (Landau et al., 1979) refers to as 'management'. Control relies on pre-defined rules and knowledge, while management is the way of dealing with a deviation without sufficient information. Both Landau's concepts of 'control' and 'management' are present in the control concept in this thesis. Note that in addition to substituting control, management can also supplement control; in a new situation where many procedures are present a lot of management is required.

4.2.5 Information and control

Apart from the elements and the working of the control concept, the arrows connecting the different elements in the controlling process are equally or even more important. The only difference in types of arrows, made so far, is between durable, non-durable, human and non-human resources. However, information is a special kind of non-human resource, and may be durable or non-durable and it is present, especially in the controlling process. In the remainder of this thesis there will be a distinction between information and other resources. Both resources and information can be durable and non-durable. However, the difference between information and other resources is that information or knowledge (i.e. used information) is intangible, while resources are tangible. The connections between the different elements inside the controlling process are made by information flows. These information flows constitute an information process. According to Falster (Falster, 1997) the information process is responsible for collecting and disseminating information, processing information and storing data to support the controlling process. Together with the resources (human and non-human (=infrastructure)) this information process constitutes the controlling process. Figure 23 shows a transformation and its controlling process in detail.

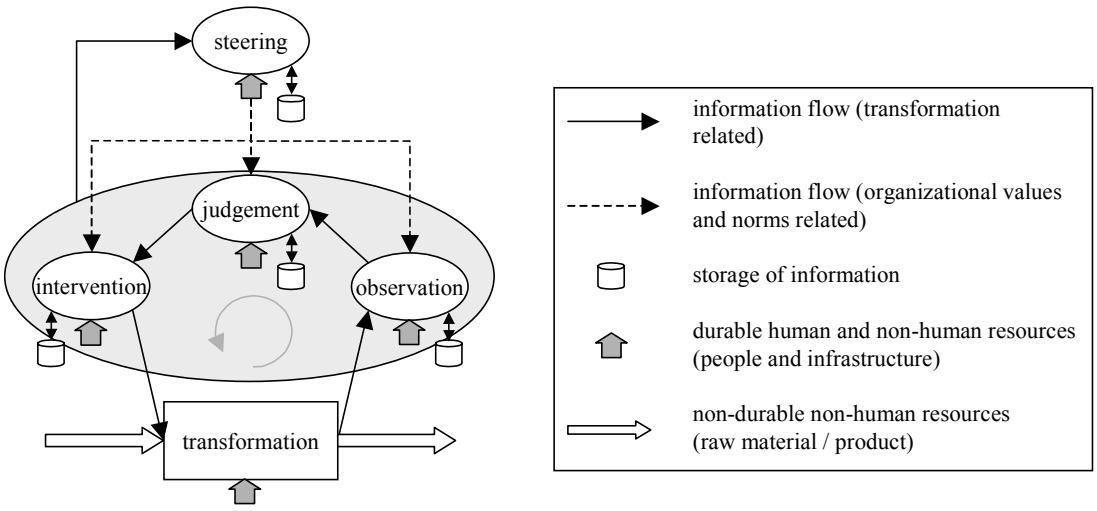


Figure 23 A transformation and its controlling process in detail.

The transformation uses durable human resources and infrastructure to transform the non-durable non human resources on the left (raw material) into the non-durable non-human resources on the right (product). All under constraints from the controlling process, which emanate from the observation, judgement, intervention and steering elements. All control elements receive information relating to the transformation process. This information is processed by means of the durable human resources and infrastructure, making use of the stored historical information. This processing takes place under constraints from the information flow related to the organizational values and norms, which are processed by the steering element.

A complete control model has now been derived, subsequently the link of the control model with the previous concepts of precursor and finally safety, has to be explained. The following Section will therefore discuss an approach of how to use all concepts in practice.

4.3 Developing an approach relating control and safety

In Chapter 1 Reason's latent condition – active failure model of accident causation passing through holes in the safety barriers (Reason, 1997) was shown (see Figure 3 in Chapter 1). This Chapter illustrates that active failures in this model can be represented by precursors. The latent conditions subsequently manifest through ineffective control processes enabling the failures and the precursors to occur. Both, active failures and latent conditions are responsible for creating the holes in the safety barriers which are between the hazards in an organization and an actual accident. In this way precursors, control and safety are linked because these holes in the safety barriers enable an accident to occur. However, how both latent conditions and active failures create these holes has still not been addressed and has to be explained to relate the previous concepts directly to safety. This will be done in the following sub-Section.

4.3.1 How holes in the safety barriers are created

An organization consciously failing to control a situation, knowing that a precursor has occurred which can escalate into an accident, is not realistic. Most often, an accident occurs without the organization having any inkling that an accident could occur. From the organization's perspective everything had been proceeding according to plan. Dekker (Dekker, 2002) illustrates how an unfolding sequence of events leads to an accident. He graphically represents this sequence of events as a tunnel which meanders its way to an accident. Figure 24 shows the tunnel and two different perspectives on the pathway to an accident, i.e. outside and inside.

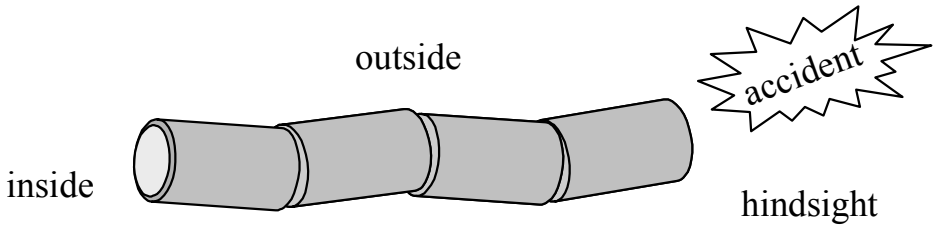


Figure 24 *Different perspectives on a sequence of events leading to an accident, Dekker (Dekker, 2002).*

From the outside and in hindsight the entire sequence of events (the outcome and the dangers involved) can be seen. From inside the tunnel, which is the point of view in the unfolding situation, the outcome is not known. The direction of the sequence of events was based on the circumstances inside the unfolding situation. To understand why an accident could occur, the inside perspective must be discovered.
To reconstruct the unfolding situation from inside a tunnel, Dekker (Dekker, 2002) proposes five steps:

1. Retrieve the sequence of events
2. Establish the boundaries of every event
3. Retrieve the information available during each event
4. Find the knowledge objectives, point of view and limited resources available at that time
5. Reconstruct the unfolding situation

In this study the perspective of unfolding events, leading to an ineffective control, is obtained. The considerations which made sense at the moment of occurrence, but led to an ineffective control, are retrieved by collecting the answers to the five steps from Dekker. To derive the answers to the five steps from Dekker, Figure 23 is used. Steps 1 and 2 can be seen as the ineffective control element in Figure 23. An event from the tunnel (as depicted in Figure 24) can be seen as an ineffective control element.
So, the event and boundary of the event (steps 1 and 2 from Dekker) correspond with one of the ineffective control elements, i.e. observation, judgement, intervention, or steering. Steps 3 and 4 from Dekker, i.e. retrieving and finding information, knowledge objectives, point of view and limited resources during that event, correspond with the resources and information flows interacting with the control element. These resources and information flows are graphically depicted by the arrows interacting with a control element as seen in Figure 25. Step 5 from Dekker, reconstructing the unfolding mindset, is obtained by identifying all interacting information flows and resources of the ineffective element, which explains the unfolding situation leading to the ineffective control element.

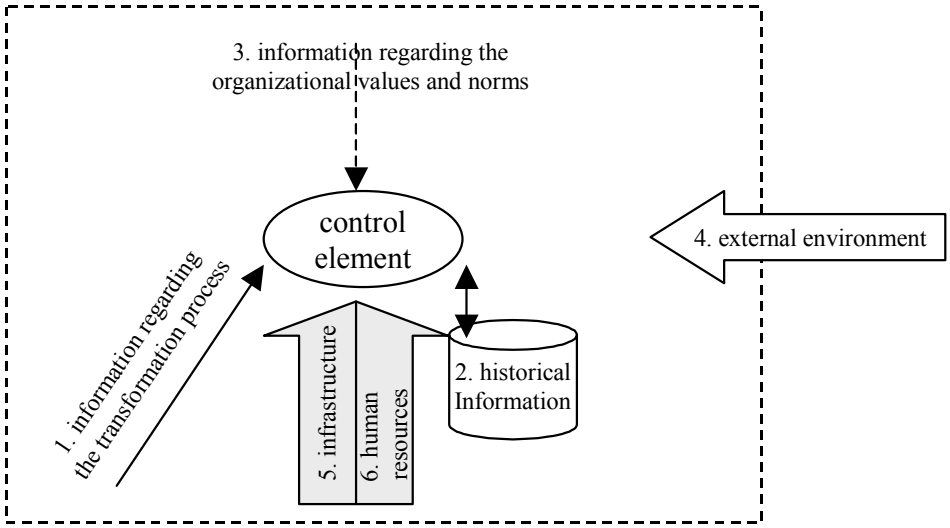


Figure 25 Information flows and resources explaining the unfolding situation.

These information flows and resources create Dekker's unfolding situation and are the latent conditions leading to an ineffective control process that can be a link in the chain of events leading to an accident. From literature various numbers of latent conditions are present, e.g. Hudson (Hudson et al., 1991) identified 11 types of latent conditions, Jacob (Jacob et al., 1994) identified 20 different types of specifically organization related latent conditions, Weil (Weil et al., 1999) identified 6 types of specific organizational related latent conditions, Boreham (Boreham et al., 2000) identified 3 types of latent conditions, while Busby (Busby et al., 2003) identified 8 types of latent conditions. Most of these different types of latent conditions need clarification because they are non-specific and too encompassing to benefit an organization. Moreover, often in order to understand them the specific context within which these conditions occur must be known. However, if they are too specific they can only be used company specific. Therefore, in this thesis, the context of the control model is used to introduce a new taxonomy for the latent conditions. A taxonomy that is context specific (control model) but not too specific that they cannot be used in different organizations, as Dekker suggests (Dekker, 2002) by 'unfolding the situation' and thereby identifying the causal conditions. In this way latent conditions are typified in terms that have a specific meaning in the context of the control model introduced earlier and can be used in different organizations.

A condition contributes to the unfolding situation if it is not present or dominant. From the control model these conditions are indicated as arrows entering the control element, see Figure 25. Thus the latent conditions are specific and context related (ineffective control element), but on the other hand general enough that they can be used in different organizations. The six types of latent conditions are, the numbers are corresponding with the numbers seen in Figure 25:

1. transformation, i.e. the use and presence of information relating to the corresponding transformation process,
2. history, i.e. the use and presence of historical information concerning the previously deviations in the corresponding transformation process,
3. organizational values and norms, i.e. the presence of constraints of time, cost, quality, risks, etc.,

4. external environment, i.e. the use and presence of information from outside the organization (new technologies, regulations, etc.),
5. infrastructure, i.e. the design of the installation and equipment,
6. human, i.e. availability of the 'right' people.

The 'transformation,' 'history,' 'organizational values and norms,' and 'external environment' types of latent conditions are all latent conditions concerning information flows. The 'infrastructure' and 'human' types of latent conditions both concern resources.

When these latent conditions create an unfolding situation, the safety barriers present in an organization can be seriously affected. Svenson (Svenson, 2001) identifies three functional categories of safety barriers, e.g. 'technical,' 'human,' 'organizational.' These safety barriers can be activated by different safety barrier systems, such as the closure of a valve automatically by a computer or manually by an operator. Moreover, a safety barrier system can (simultaneously) operate more than one safety barrier, like an operator who can close a valve, connect a hose, or a computer which closes down a machine and alerts an operator, etc.
A 'technical' safety barrier represents technical equipment, whose function it is to arrest the accident/incident evolution so that the next event in the chain will not be realised. The 'human' safety barrier is the 'suitable' people, whose function it is to intervene and arrest the accident/incident evolution so that the next event in the chain will not be realised. The 'organizational' safety barrier is the procedures, rules, guidelines, etc. present, which function to arrest the accident/incident evolution so that the next event in the chain will not be realised. In this thesis the latent conditions and precursors in an unfolding situation are considered to have three possible effects on the safety barriers: negative, positive or none at all.

- negative, where a safety barrier is ineffective and does not prevent the development towards an accident/incident (a hole in a safety barrier). Where the safety barrier is missing because it was never there or has been removed or not applied.
- positive, where new barriers are initiated that intervene and take over the function of the ineffective or missing barriers.
- none at all, where the barrier works correctly and prevents the progression to an accident/incident.

If the safety barriers are ineffective or missing, the precursor present can pass through a hole in a safety barrier and if a sequence of safety barriers are ineffective or missing, eventually an accident can occur. To explain the foregoing, an example is given:

In the book 'The Challenger Launch Decision', Vaughan (Vaughan, 1996) documents how an organization decided to launch one Space Shuttle after another, even though the O-rings in the solid rocket boosters showed recurring signs of heat damage. Despite the re-occurring damage, the O-rings were considered to be 'acceptable.' The underlying causes of the failed judgement was the lack of proper process (transformation) information and an increased time pressure (information regarding the organizational values and norms). These influences led eventually to a decreasing failure norm for the O-rings, and finally resulted in the explosion of the Challenger Space Shuttle.

From this example it appears that the capability of an organization to control deviations in the operational process and thereby preventing them from escalating into accidents, indicates the robustness of an organizations commitment towards preventing accidents. The working of all control processes in an organization could therefore be used as a performance indicator to represent the safety of an organization. Furthermore, the cause-effect relationships as presented in this sub-Section provide appropriate specific preventive measures, which can significantly enhance the effectiveness of the organization's normal way of working. Companies can respond accordingly to the identified accident scenario's, by interrupting the cause-effect relationships, as shown by the letters A to C in Figure 26, which is essentially identical to Reason's (Reason, 1997) model as shown in Figure 3.

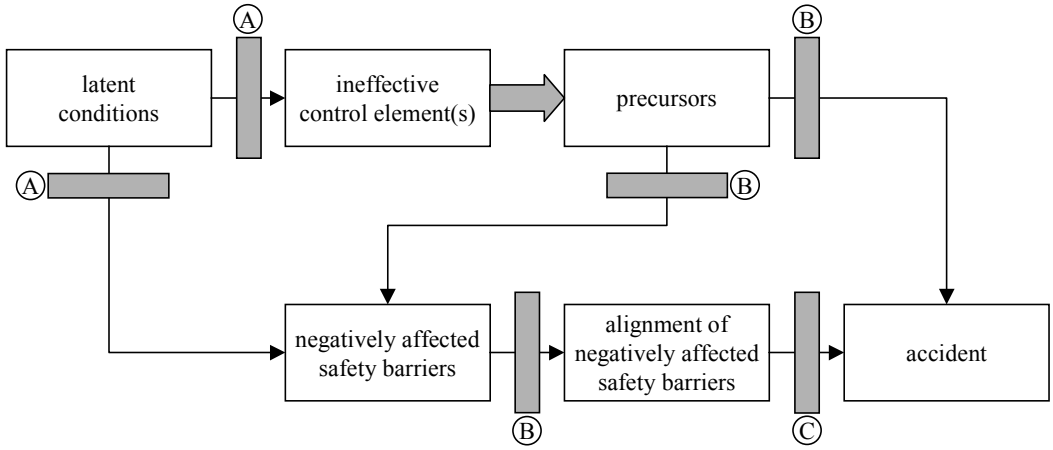


Figure 26 Line of reasoning and possible intervention possibilities.

The letters A to C in Figure 26 represent the possible interventions a company can make, to arrest the development of an accident. The interventions react to the situation as shown prior to them. The thick arrow represents a cause effect relationship that is so direct, no intervention can be implemented preventing the effect from occurring if the cause is not removed. In Figure 26 one relation is present, between the initial ineffective control elements and the precursors, implying that if latent conditions are present, the initial ineffective control elements are automatically present to and will automatically result into precursors.

The order of the letters identifies the most effective intervention (removing the cause: A) till the least effective intervention (removing a sign: C). The possible intervention strategies are stated below:

A: Removal of the latent conditions initially causing the accident scenario. This is the most effective intervention. The intervention requires alterations in the organizational system, e.g. changing the retrieval and analyses process of data, redesigning equipment, enhancing the training programmes, etc.

B: Operators are able to recover deviations, meaning they react to deviations or ineffective safety barriers, alleviating the effects from these 'problems', Kanse (Kanse, 2004). This intervention is less effective than removing the latent conditions, although these recovery actions/strategies can be used to enhance the learning cycles in an organization.

C: By maintaining an overview of effective and ineffective safety barriers, accidents can be prevented by making sure that no alignment of ineffective safety barriers can take place. Therefore, the overview has to be known to all the actors inside an organization and has to be constantly updated, which requires enormous amounts of resources, e.g. time and money. This form of intervention can be seen as the least effective way of intervening.

In practice the presence of all three ways of intervening are needed. It is not possible to eliminate all latent conditions and there will always be conditions leading to possible ineffective safety barriers and ineffective control elements, which subsequently lead to precursors. Therefore, recovery is necessary, to intervene and arrest the precursors and ineffective safety barriers from evolving into a possible accident. Finally, because not all precursors can be effectively recovered, finally an overview of affected safety barriers is necessary to prevent an alignment of ineffective safety barriers and the presence of precursors that can escalate into an accident.

By explicitly showing the cause-effect relationships from precursor via control to the latent conditions, recommendations for all three ways of intervention principles can be made. The next sub-Section will therefore discuss an approach where the concepts discussed in this Chapter can be used to display the working and influence of a control process on the safety of an organization.

4.3.2 A practical approach using the concepts defined in this Chapter

From the concepts derived in this Chapter a practical approach is derived shown in Table 6. This table shows how to use the concepts for retrieving the working and influence of a control process on the safety of an organization and identifies pro-actively safety risks.

Table 6 A practical approach to identify pro-actively safety risks.

1	identify precursors
2	identify the ineffective control element in the control process
3	identify the conditions, i.e. resources and information flows, causing the control element(s) to be ineffective.
4	identify the influence of the conditions on degradation of the safety barriers and derive countermeasures as they occur in practice.

With the definition of a precursor given in this Chapter, precursors can be identified from practice (step 1). These precursors are the results of active failures and, by backtracking, they lead to the ineffective control element (step 2). Subsequently, the latent conditions, i.e. information flows and resources causing the ineffective control element(s) have to be identified (step 3). When identifying these information flows and resources, the unfolding situation leading to the ineffective control element(s) can be discovered. Furthermore, the influences of these 'latent' conditions on the degradation of the safety barriers have to be identified (step 4). Thus the influences of the control processes on safety can be retrieved and possible safety risks can be identified. Furthermore, possible countermeasures can be derived to prevent these risks from escalating into possible accidents.
The next Chapter will use this approach on a first case study in practice to identify how ineffective control affects safety and possible accidents originate.

Chapter 5

ESTABLISHMENT OF A PROTOCOL FOR ANALYSIS

The concepts derived in the previous Chapter are applied in practice by means of a case study, describing a pesticide company struggling with the question of how to improve the safety of their operational process further. The control model derived in the previous Chapter is used to analyse both the controlled process and controlling process with respect to its impact on process safety.
Using this case study, the concepts derived in the previous Chapter will be enhanced to retrieve a structured way of analysing which in turn will be developed to retrieve the operational control structure of the company and the way safety barriers (measures) are affected by the control process in daily use.

Section 5.1 is based on a paper by: Sonnemans P.J.M., Körvers P.M.W., Brombacher A.C., 2004. Effective Safety management – A case study in the chemical industry, Quality & Reliability Engineering International Vol. 20 (2), pp….

5.1 A case study

In this Section the concepts of a precursor, control process and safety, will be applied to a practical case. From this case study, further refinements and a structured way of approaching practice will be derived. To find a suitable case study, the selection criteria and their underlying rationalisations have to be given. In Chapter 2, Bickman (Bickman et al., 1998) stated that selection criteria should be based upon five major issues; site selection, data collection process, authorization, accessibility and other support. These five issues, the selection criteria and their advantages and disadvantages are stated below:

- The site selection is largely determined by the risks present in the company and hence the importance of safety issues in the company. A batch industry company handling hazardous substances is a company with a high risk which means that safety is an important issue. The risks are determined by the type, amount and conditions of the substances and the complexity of the company, as discussed by Perrow (Perrow, 1984). Hazardous substances are a first selection criterion. The complexity is determined by the type of industry, batch or continuous. In a batch process, as opposed to a continuous process, the number of changes in the chemical and control process is much higher. These changes often decrease the full understanding of the working of the system, which according to Perrow increases the complexity and the risks. The batch industry is a second criterion.

- The data collection process is determined by the availability of data and also the accessibility, authorization and other support as will be discussed later on. The size of a company to a large extent determines the way of working. Large companies are more formalised and have more data available. Small companies have a less formal way of working and often have less data available, which makes it very difficult to collect and to analyse data. A large

company (multinational) is a third criterion. However, the aim is to test the concepts in practice and this requires both an overview and insight into how the analysis concepts work in practice. Therefore, the criterion of a large company is replaced in this first case, by a small company.

- Authorization, accessibility and other support is determined by the relationship with the company and its culture. The relations with the company have to be such that access to the relevant data is sufficiently authorized and fully supported by the company's management. The fourth criterion is sufficient authorization to obtain relevant data. The accessibility and other support are mainly influenced by the cultures of researcher and company employees. For example, cultural differences can influence the correct understanding of data or people. The final criterion is therefore a company located in The Netherlands.

In addition to these selection criteria, the limitations of the author's contacts and the willingness of companies to participate, narrowed the search for a suitable case down to a small Dutch company (< 30 people). This company produces in batches, falls under the Dutch Seveso-II directive (BRZO, 1999) and authorized access to the relevant data. The selected company had experienced some serious accidents recently, in spite of using many technical safety systems. Thus the management was aware of the necessity to enhance both safety and the reliability of the operational process.

In the following sub-Sections the practical approach derived in the previous Chapter will be applied on this case study. Therefore, the precursors present inside the operational process are identified. Then, the control of the operational process will be modelled and analysed to find the ineffective control elements. Furthermore, the 'latent conditions' causing the ineffective control will be retrieved and their impact on the existing safety barriers will be identified. Finally, improvement opportunities for the company will be indicated, together with some recommendations and enhancements for the applied concepts and the proposed practical approach.

5.1.1 The pesticide company and its precursors

The case study concerns a small company producing pesticides in The Netherlands. For reasons of confidentiality, the name or detailed information of the company cannot be revealed, but they are known to the author.
The company produces particular pesticides for industrial clients as well as for the consumer market. The company is licensed to produce and export these pesticides as they satisfy the safety, health and environmental requirements of many governments world-wide. The company produces pesticides in several compositions on a produce-to-order basis in small batches. Each order has a specific composition and once an order has been accepted it has to be delivered within a specified time limit or a financial penalty is incurred.
The company is divided in several organizational units: Sales, Customer Service Department, Purchasing, Production, Storage and Quality laboratory. Despite the fact that these units are all involved in the operational process, they do not reflect the actual process flow, instead they represent the way in which the company has organised its human resources into groups.

The operational process of the pesticide company is described in terms of different transformations or sub-processes. The operational process consists of six different sub-processes. These sub-processes are named: synthesis, extrusion, mixing, packaging, packaging lines, technical support and quality laboratory. Furthermore, there are three storage points: storage of hazardous substances (haz. sub. storage), storage of packaging material (pack. storage) and storage of end-products (product storage). The entire operational process flow is depicted in Figure 27.

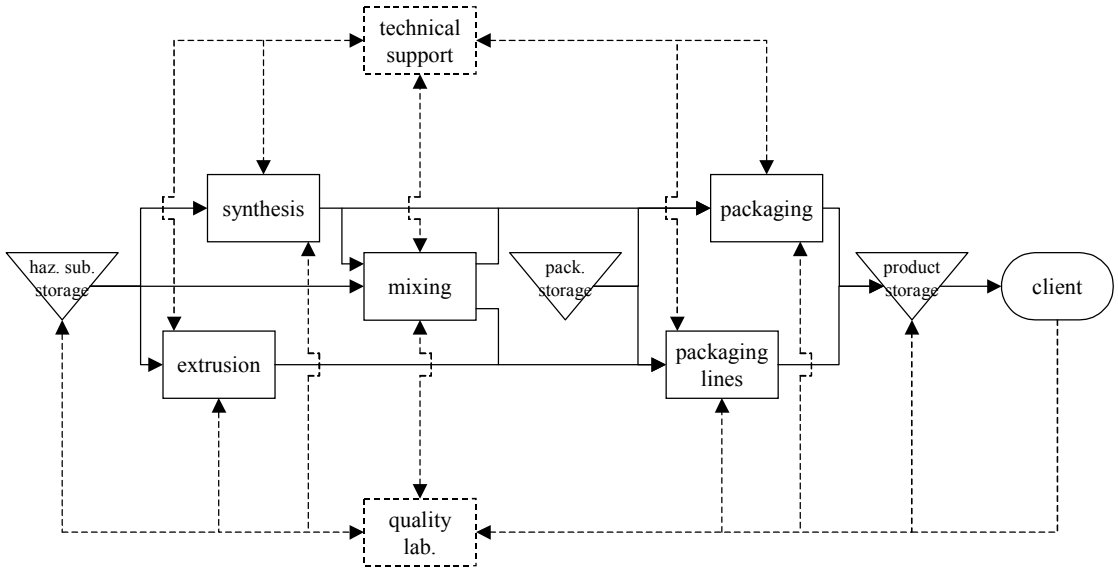


Figure 27 The operational process of the pesticide company.

The solid lines and rectangles in Figure 27 represent the process flows and the sub-processes of the primary process. The broken lines and rectangles and the solid triangles represent the sub-processes and flows from that part of the secondary process which interacts directly with the primary process. The primary process and the parts of the secondary process together constitute the operational process as shown in Figure 27.

Before modelling and analysing these sub-processes in terms of the control model, the company's problems, their perceived solutions and the precursors used are stated.

Recently, the pesticide company experienced two accidents. The first accident was a small fire of a mixture of liquid pressurised gas and liquid pesticide, which resulted in some material damage. The second accident was an instantaneous release of pesticide powder, which resulted in a number of operators requiring treatment for respiratory problems in a local hospital. Management recognised that safety problems had to be addressed. Additionally, a major concern for the company was the high financial penalties which resulted from late deliveries. Both the safety and the reliability of the operational process had to be improved. The management thought that operator errors were the cause of almost all the problems in the process.

In addition to these problems, several re-occurring deviations (precursors) were present in the operational process. To identify these precursors, deviation data had to be collected and analysed. However, only planning schedules and product quality data were available. Therefore, additional data was obtained mainly by interviews.

From analysing the planning schedules of the last 6 months it was concluded that 35% of all scheduled jobs were completed on time, 50% were overdue and 15% were removed from the planning schedules. The 15% of scheduled jobs which were removed from the planning schedules, were removed for a variety of reasons. Some were removed because they had been produced previously and others were removed because the sales manager required different products to be produced first, etc. The planning schedules of overdue jobs were analysed and this revealed that 50% of the overdue scheduled jobs were caused by equipment failure, 20% were caused by shortage of material and the other 30% of cases the causes were unknown. In spite of the low percentage of jobs finished as scheduled, the company manages to deliver 80% of their products in time. The company manages to deliver the products in time by structurally working overtime to avoid penalty costs.

From the analysis of the planning schedules, the data from product quality and several cross functional interviews, a list of precursors in a time period of six months could be derived. In Table 7, ten precursors identified in the pesticide company are given.

Table 7 An example of precursors.

1	shortage of packaging material on the packaging lines
2	coagulating of substances while mixing
3	no correct connection between tank and packaging lines
4	packaging machines not empty while performing maintenance
5	storages overfilled
6	malfunctioning of the machines of the packaging lines
7	clogged extrusion machine
8	shortage of materials while packaging
9	leakages and fumes filling packages from synthesis
10	product purity problems while extruding

While identifying the precursors with help from the definition given in the previous Chapter, some problems appeared while applying the definition on the obtained data. Events were identified in which several similar deviations occurred at the same time. From the analysis of the planning schedules, it appeared that the same deviations occurred simultaneously on the packaging lines and in the packaging. The question which arose was; whether a lapse of time is necessary between a re-occurring deviation? Meaning, if a second deviation of the same nature occurs simultaneously with the first deviation, does the re-occurring deviation fall into the classification precursor? Precursors are a sign of ineffective control, but if a second deviation of the same nature occurs simultaneously with the first deviation, is the company actually able to learn from the first deviation, and be able to control it effectively? Subsequently, another question related to the last question arose; how many deviations must actually re-occur, before the single or the double control loops can undisputedly be qualified as being ineffective? Is there a minimal number of re-occurring deviations that must occur to qualify both control loops, i.e. single and double as discussed in the previous Chapter, as ineffective?
Furthermore, the numbers of identified precursors were so large, that not all precursors could be analysed. The problem was how to arrange the precursors in such a way, that the most relevant precursors regarding safety would be analysed? Many precursors concerned product quality or planning problems, which could not, in any way, affect safety.

These problems of how to deal with the implications of applying the precursor concept stated in the previous Chapter in practice, will be further addressed in Section 5.2. The following sub-Section uses the identified precursors to model the control processes in the operational process. Subsequently, the ineffective elements of the control processes will be identified.

5.1.2 The modelling and analysis of control

Real-life operational practice will not always correspond neatly with the theoretical control model derived in the previous Chapter, which is characterized by a completely closed control loop. Never-the-less, to better understand any malfunction of an operational process, it is worthwhile to map that process on the theoretical control model and to identify the ineffective control elements (observation, judgement, intervention, steering) in practice. By identifying ineffective control elements, one will get a clear picture why precursors exist. In this sub-Section the different control models and their ineffective elements are identified.

All sub-processes experiencing an identified precursor will be mapped on the theoretical control process. An example of the mapping is given in Figure 28 for the precursor 'shortage of packaging material on the packaging lines,' identified in the packaging lines sub-process.

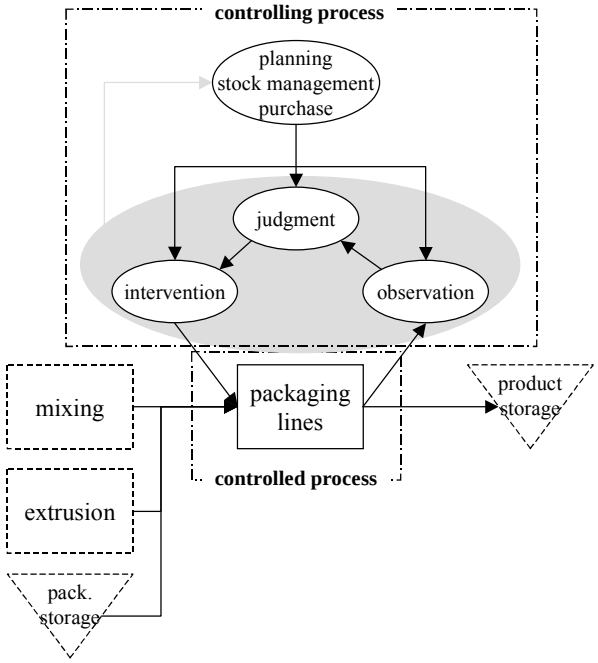


Figure 28 Packaging lines sub-process.

Figure 28 will be explained by discussing the controlled process, the precursor and the controlling process, successively. The dashed rectangles in Figure 28 represent the interacting sub-processes of the selected controlled process, i.e. the packaging lines. The arrows represent the flows between the packaging lines sub-process and interacting sub-processes and control elements.
The packaging lines receive substances from the mixing and/or extrusion processes. From the pack. storage, packaging material is provided to the packaging lines. The packaging lines insert the received substances into the provided packaging material

and produce the end-products, which are finally sent to the product storage. The packaging lines sub-process, as discussed above is a practical example of a controlled process as defined in the previous Chapter.
An identified deviation, often re-occurring (precursor), is the shortage of packaging material on the packaging lines sub-process. The packaging lines are running at full capacity when suddenly a shortage of packaging material causes them to stop. This precursor (stoppage) is observed by the packaging lines operators and passed to the production manager, who decides if the production batch, which is running on the packaging lines has to: be stopped and removed; wait for new or other packaging material or stopped and wasted, etc. The intervention he decides on will then be executed. All activities are performed according the norms provided by the steering element, which in this case contains the planning schedules from the planning department (planning), an inventory of packaging material from stock management (stock) and a timeframe for new or other packaging material from the purchasing department (purchase). This is a practical example of a controlling process, as defined in the previous Chapter.
The ineffective control element will subsequently be derived, from the working of the control process. The observation, judgement and intervention are all performed according to the identified norms of the steering element. Though, the deviations are observed, judged and mitigated according the norms, the deviation still re-occurs. It is therefore concluded that the steering element is ineffective and enables the precursor to occur.

All ten precursors from Table 7 were further analysed and the accompanying ineffective control elements retrieved. For reasons of conciseness the analysis of other controlling processes are not described here, but the ineffective control elements were retrieved in a similar way. The results of all ten precursors are stated in Table 8.

Table 8 The identified precursors and their ineffective control elements.

No.	**precursor**	**sub-process**	**ineffective control element**
1	shortage of packaging material on the packaging lines	packaging lines	steering
2	coagulating of substances while mixing	mixing	judgement
3	no correct connection between tank and packaging lines	quality lab.	steering
4	packaging machines not empty while performing maintenance	packaging lines	steering
5	storage overfilled	product storage	observation
6	malfunctioning of the machines of the packaging lines	technical support	steering
7	clogged extrusion machine	extrusion	steering
8	shortage of substance while packaging	packaging	steering
9	leakages and fumes filling packages from synthesis	packaging	steering
10	product purity problems while extruding	extrusion	observation

The first two columns of Table 8 show the ten precursors as identified in Table 7. The third column shows the sub-process where the precursors are identified and the fourth column shows the identified ineffective control elements of the accompanying controlling process.

From the identification of the ineffective control elements in the operational process, it can be seen that in seven out of the ten identified precursors the 'steering' element was ineffective. Moreover, in two out of the ten the 'observation' element was ineffective and in one out of the ten the 'judgement' element was ineffective.

The next sub-Section will discuss how the latent conditions, that cause the identified ineffective control elements, affect the current safety barriers in the pesticide company.

5.1.3 Latent conditions and their effect on safety

In this sub-Section the ineffective control elements are further analysed to retrieve the conditions causing their ineffectiveness. By checking all six types of conditions for their contribution to the ineffectiveness, the causal conditions can be identified. These causal conditions are the latent conditions. Subsequently, these latent conditions are used to explain why certain safety barriers are affected in the pesticide company.

To find the latent conditions, of the ineffective control elements, the information flows and resources interacting with the ineffective control elements must be identified. The information flows interacting with the ineffective control element were present in four different types, information regarding the transformation process, information from past deviations in the transformation process, information regarding the organizational values and norms, and information from the external environment. The resources interacting with the ineffective control element are present in two different types, human resources and infrastructure. The existing situation of an identified ineffective control element was reconstructed by means of the six types of latent conditions. The condition(s) causing the ineffectiveness are identified as the latent conditions causing the ineffectiveness and which enable the precursor. Table 9 shows which latent conditions caused the ineffective control elements which in turn enable the precursors.

Table 9 The latent conditions of the ineffective control elements.

No.	sub-process	ineffective control element	information flows				resources	
			transformation	history	organizational values and norms	external environment	infrastructure	human
1	packaging lines	steering	…	…	…	…	…	…
2	mixing	judgement	lacking	lacking	time	-	-	knowledge
3	quality lab.	steering	…	…	…	…	…	…
4	technical support	steering	…	…	…	…	…	…
5	product storage	observation	-	lacking	time	-	lacking	-
6	packaging lines	steering	…	…	…	…	…	…
7	extrusion	steering	…	…	…	…	…	…

8	packaging	steering	…	…	…	…	…	…
9	packaging	steering	…	…	…	…	…	…
10	extrusion	observation	lacking	lacking	time	-	-	knowledge

The first, second and third column of Table 9, show the ten sub-processes and ineffective control elements as identified in Table 8. The fourth, fifth, sixth and seventh columns, together called 'information flows,' show which types of latent conditions, i.e. information regarding the transformation process, historical information, information regarding the organizational values and norms, and information from the external environment, leads to the ineffective control element. For example for the second sub-process mixing, where the judgement control element was ineffective, amongst other things it lacked both information regarding the mixing process, and historical information about the deviations in the mixing process. This lack of information together with the time pressures contributed to the ineffective judgement, enabling the coagulating of substances to re-occur.
Furthermore, the eighth and ninth columns of Table 9, together called 'resources,' show the other types of latent conditions, i.e. infrastructure and human resources. For the ineffective judgement element of the mixing process, in addition to the 'information flows' relating to latent conditions the lack of knowledge of the human resources involved, contributed to the ineffective judgement.

The analysis of the collected data, identified that the ineffective judgement element of the mixing sub-process was caused by a combination of the lack of information from the mixing process, the lack of historical information about coagulating substances while mixing, time constraints and operator knowledge.
It appeared that substances coagulating while mixing was a re-occurring problem. This precursor was resolved by an operator adding other substances which dissolved the coagulating substance. However, the judgement was ineffective because the deviation re-occurred because operators didn't have the right training to know which substances under which condition coagulate and the incidents of coagulating substances were not recorded because of time constraints. The combination of all these conditions led to an ineffective judgement, enabling the coagulating of substances to re-occur.

Likewise, the latent conditions from the ineffective observation of the product storage sub-process and the ineffective observation of the extrusion sub-process, the No.5 and No. 10 respectively from Table 9 can be derived. However, from the seven remaining ineffective steering elements no latent conditions could be obtained, which is displayed as the '…' in Table 9. The steering element itself was so complex that no latent conditions could be unambiguously retrieved. Therefore, some additional research had to be performed, so that latent conditions could be retrieved for an ineffective steering element. This problem will be further addressed in Section 5.2.

Once both latent conditions and precursors are identified in the company's control process and operational process, the effects on the company's safety barriers can be retrieved. Therefore, the safety barriers present around the transformation process will be identified, i.e. technical, human, and organizational safety barriers. Subsequently, the identified types of latent conditions are used to check if they affect the identified safety barriers either positively, negatively, or not at all (as discussed in the previous Chapter). How safety barriers are affected is illustrated by the example of the re-

occurring coagulation of substances during mixing. The coagulation severely increases the power the engine has to provide to mix until the engine blocks. Because, the operators reset the engine and pour a dissolving substance into the coagulated substance, the engine is again severely stressed. If the blocking mechanism fails, which will happen if repeated attempts are made, the friction inside the engine will become so high that it may catch fire. As discussed previously, the re-occurrence of coagulating substances caused by latent conditions affect the engine's blocking mechanism (technical function category of safety barrier), until it 'fails.'

The ineffective observation element of the extrusion sub-process enables the re-occurring product purity problem, which had no effect on any safety barrier present. It appears that the focus of the analysis so far should be more on safety relevant precursors and processes, to avoid results that do not affect any safety barrier. This problem will also be discussed further in Section 5.2.

5.1.4 Results and discussion of the case study

From the precursors and ineffective control elements identified and analysed in the pesticide company it was shown that the improvement of production depends especially on the steering element. The steering element was identified as ineffective seven times out of ten. An ineffective steering element points to a failure of the management and other interconnected sub-processes, such as planning, purchasing, etc. and not to the operators in the primary process as claimed by the management.
To identify precisely how ineffective control elements affect safety, refinements of the ineffective steering element inside the control model concept are necessary. Moreover, the analysis must be formulated to retrieve a clear cut way of analysing, which increases the research's overall validity and reliability, which in turn increases generalizability and the scientific value of the research. The results retrieved from the analysis so far, are not so unambiguous, as to enable other researchers to repeat the analysis and obtain the same results. Therefore, all steps of the analysis must be formulated and executed in such as manner as to retrieve unambiguous final results, which show how and why the control processes in the company affect safety.

For the company in the case study, it can be concluded so far that improvement efforts should be focused on reducing time pressure and obtaining information on previous deviations in product storage and in the mixing and extrusion processes. Further training should be provided for operators in the mixing and extruding processes and they should be given more information about the process itself. The reliability and safety issues discussed in sub-Section 5.1.1 could not be addressed, because the steering element could not be further analysed. However, after adequately addressing the identified limitations and applying the concepts from the previous Chapters again, these issues can be addressed properly, as stated in sub-Section 5.3.7.

5.1.5 Discussion of the problems identified during the analysis

From the case study it is observed that the concepts presented in the previous Chapter are able to display the controlling processes in an organization and to partly derive the way in which an ineffective control element affects safety in a company. However, during the case study some shortcomings of the proposed concepts emerged. The proposed concept were not able to;

- derive an unambiguous concept of a precursor capable of processing all deviation data.
- identify safety relevant precursors and control processes.
- derive latent conditions from the complex ineffective steering elements.
- derive an unambiguous method for analysis.

In the next Section the identified shortcomings of the proposed concepts will be addressed.

5.2 Concept refinements

From the results of the case study it is concluded that the concepts presented are suitable for displaying the control process of an operational process and to partly identify control improvement areas. However, modelling an operational process with respect to control loops and affected safety barriers requires some additional refinements to the proposed concepts:

- Extend the concepts of a precursor to achieve an unambiguous concept capable of processing all deviation data.
- Focusing the precursor analysis process to include only those precursors and control processes linked to safety
- Extend the control model concept, to reduce the steering element's complexity, enabling latent conditions to be derived from it.
- Derive a method for an unambiguous analysis.

All four issues will be addressed in the following sub-Sections, which will inform the basis for a structured protocol to approach practice.

5.2.1 Extend the concepts of a precursor

In the previous Chapter, a definition of a precursor was given. However, in practice whilst processing the deviation data some additional questions arose which impacted on this definition. These questions were:

1. If a second deviation of the same nature occurs simultaneously with the first deviation, does the re-occurring deviation fall into the classification precursor?
2. Is there a minimum number of re-occurring deviations that must occur to qualify both control loops, i.e. single and double as ineffective?

The purpose of retrieving precursors is to analyse them with the help of the control model derived in the previous Chapter. This control model establishes why re-occurrence has taken place first by checking the single loop control elements and second by checking the double loop control elements.
If a deviation is observed for the first time the control process must be able to learn from this mistake, so that different strategies of the existing theory in use can be applied to remove a deviation which re-occurs. If the same deviation does occur for a second time it indicates that the strategies didn't work, or were not implemented and that the underlying organizational values and norms must be adapted. When a deviation occurs for the third time (i.e. re-occurrence for a second time), it is a sign

that either the new values and norms are wrong, or that the new values and norms were not properly implemented.

The above explanation of how the control model works, encompasses both answers to extend the concept of a precursor enabling the processing of all data unambiguously. The answer to the first question is that if a second deviation occurs simultaneously with the first deviation, the organization is unable to learn from the first deviation and it cannot be classified as precursor. Therefore, a time lapse which gives an organization the opportunity to learn (to take action), is necessary between identical deviations occurring. In other words, a deviation occurring seven times, but simultaneously, will be seen as one event.
The answer to the second question is that it is only by two occurrences (i.e. re-occurrence for a first time), that the single loop can be questioned. The double loop can only be questioned after three occurrences (i.e. re-occurrence for a second time). Concluding, that only identical deviations occurring three or more times and separated with a time lapse sufficient for the organizations to learn, will be recognised as a precursor.

This leads to the precursor criteria:

- Occurrence of three or more individual deviations from the transformation's theory-in-use, or espoused theory
- These deviations must all occur in the same input, output, or resource of the transformation.
- These deviations must be equal to each other on the lowest aggregation level as recorded in a company
- These deviations must occur after each other, with a time lapse sufficient for the organization to learn (to take action).

Data retrieved from interviews and observations must comply with the same criteria, but such data cannot be verified easily. Therefore, cross-functional interviews and confirmation by different people in the organization are necessary.

Thus the precursor concept is extended in such a way that all deviation data can be processed to retrieve precursors unambiguously.

5.2.2 Focusing the precursor analysis process

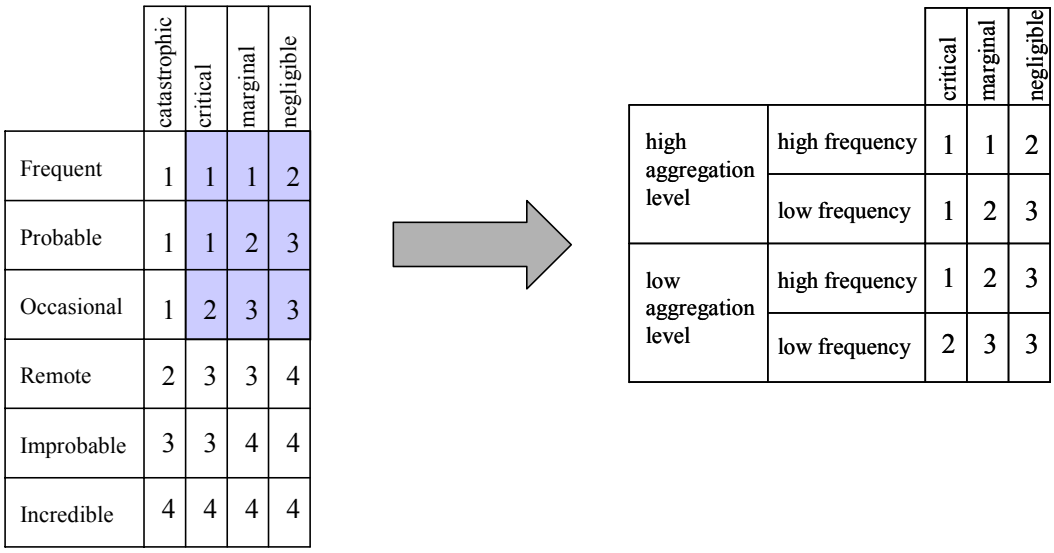
Findings from the case study revealed that modelling of operational control processes takes an enormous amount of time, while afterwards many precursors and their accompanying control processes are not that relevant from a safety perspective. From a traditional safety perspective only those processes which are directly related to the highest risks are analysed. This implies that a prioritisation of precursors has to be made before analysing the effectiveness of accompanying control processes.

To prioritize the identified precursors in respect to safety, the perceived risk(precursor)=(likelihood, consequences) will be established and is taken as the prioritization criterion. To determine this perceived risk, the 'likelihood' and 'consequences' must be established. The likelihood of the identified precursors is established by establishing a 'relative frequency' and an accompanying 'aggregation

level' of the identified precursors. The 'relative frequency' is established by the number of deviations process/equipment/operator experiences during a specified time period related to the average use of the process/equipment/operator. For example, a valve leaks ten times a year, while on average the valve is used once a week, so the 'relative frequency' is expressed as 10/52.
In practice several aggregation levels can be distinguished, as is explained in the previous Chapter. However, the different aggregation levels cannot be identified and compared without ambiguity so in this thesis only two aggregation levels, high and low are distinguished. A high aggregation level is distinguished if the precursor is identified on the highest aggregation level of the sub-processes, as defined in the operational process, i.e. if the re-occurring deviation occurs in all transformations of a sub-process. A low aggregation level is distinguished in all other cases. For example, a precursor at a high aggregation level is the leakage of all type Y valves and a precursor at a low aggregation level is the tripping out of a specific valve. Because the consequences of precursors on a high aggregation level have a 'greater impact' (involves several items), such precursors are prioritized above low aggregation level precursors. Subsequently, all high and low aggregation level precursors are sorted separately, according to their 'relative frequency.'

After the likelihood, the perceived consequences of the precursors have to be established in order to determine the perceived risk. To determine these consequences, expert opinions and past lessons are needed. From accident reports and several multi-disciplinary experts in the company, the precursors are listed according to their perceived consequences in terms of: 'critical,' 'marginal,' and 'negligible.' The consequences are established by deriving a scenario, perceived as highly likely, and determining the consequences if this scenario would occur.

Finally, both the properties, 'likelihood' and 'consequences,' determine the risk. However, to prioritize between different risks, the risk has to be expressed as a one-dimensional entity, as discussed in Chapter 1. To establish this one-dimensional risk, a standard risk matrix is used, as depicted on the left side in Figure 29, taken from the safety standard IEC 61508 (IEC 61508, 2000). From this standard risk matrix, the risk matrix used to prioritize the precursors is derived, as depicted on the right side in Figure 29.



Risk classification (IEC 61508, 2000) **Derived risk classification**

Figure 29 Risk classification and derived risk classification to prioritize precursors.

In Figure 29, the rows of both risk classification matrices show the established likelihood, while the columns show the perceived consequences. The result of both likelihood and perceived consequences is the perceived risk, which is indicated with a perceived risk class from 1 to 4 for the left risk matrix and from 1 to 3 for the right risk matrix. The interpretation of the different risk classes for the left matrix in Figure 29 is derived from the IEC 61508 (IEC 61508, 2000) and is stated as:

1. Intolerable risk.
2. Undesirable risk and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained.
3. Tolerable risk if the cost of risk reduction would exceed the improvement gained.
4. Negligible risk.

An interpretation of the different risk classes for the right matrix in Figure 29 is not made. The perceived risk is only derived for prioritizing the precursors so no interpretation is necessary. Class 1 risk means that the precursor present in this class will be analysed first, precursors in Class 2 risk, second, etc. The final decision, which precursors will be analysed further if there are more precursors belonging to the same class of perceived risk, is made by the multi-disciplinary group of experts, who established the perceived consequences.

By adding a step which prioritizes the precursors against their perceived risks (which is defined as the inverse of safety), the small group of analysed precursors and the accompanying control processes will have a higher probability of being relevant in respect to safety.

5.2.3 Extending the control model concept

Findings from the case study revealed that the ineffective steering element in the controlling process was too complex to retrieve the latent conditions which caused this ineffectiveness. From literature it is known that the controlling process or tertiary process, as discussed in Chapter 4, of which the steering element is a part, consists of different hierarchical levels. Insight in these hierarchical levels and their interactions will reduce the complexity of the steering element enabling the retrieval of the latent conditions causing the ineffectiveness.

Mintzberg (Mintzberg, 1983) states that different hierarchical levels are necessary in a control process. Here, the co-ordination of the organization takes place and because as Mintzberg states: 'not all decisions can be understood,' several hierarchical levels are necessary. Mintzberg, distinguishes two types of co-ordination and calls them 'horizontal' and 'vertical' coupling. Horizontal or lateral coupling, is the direct tuning between activities in one hierarchical level. Vertical coupling, is the indirect tuning by activities from different hierarchical levels. Both types of coupling determine the structure of the controlling process.
Parsons (Parsons, 1960) distinguishes three hierarchical levels in an organizational structure. He identified a 'technical,' a 'managerial' and an 'institutional' level in an organizational structure. The emphasis of the 'technical' level is on the primary product, by controlling the operational process. The 'institutional' level is principally involved with cultivating exchange relationships between the organization and the external environment, with maintaining legitimacy and with defining the organization's role in the external environment. The 'managerial' level provides the necessary linkages between the 'technical' level and 'institutional' level, and enables the vertical coupling. Moreover, the 'managerial' level also integrates the 'technical' level activities and enables the horizontal coupling. The 'managerial' level achieves this by acquiring resources from the external environment and by influencing the organization of the operational process.

Nowadays, these hierarchical levels are still used to explain the control structure in an organization. Van Mal (Mal van, 1999) uses the terms 'operational' control level, 'tactical' control level and 'strategic' control level, for the 'technical,' 'managerial' and 'institutional' level respectively. The terms used by van Mal will be used in the remainder of this thesis.

The three hierarchical levels are interconnected by information flowing from the strategic level via the tactical level to the operational level, and the other way around. From upper to the lower level, the information flow is related to the environment on the strategic level, which is the organizational values and norms. However, as Thompson (Thompson, 1967) identified, the tactical control level can allow the operational level to operate as a relatively closed system. The tactical level provides a buffer between the uncertain environment and stability of resources required for uninterrupted production on the operational level. In this way the influences from the external environment on the operational level will be reduced to a minimum. The information flow going from lower to upper level is related to the operational process or transformations. The top down flow provides the restrictions and conditions for the transformation, while the bottom up flow provides information about the status of inputs, outputs, and resources of the transformations. The horizontal information flows are between different control elements on one hierarchical control level.

From literature and the basic control model derived from the previous Chapter the different control levels and the complexity of the steering element was resolved by the author and is graphically represented in Figure 30.

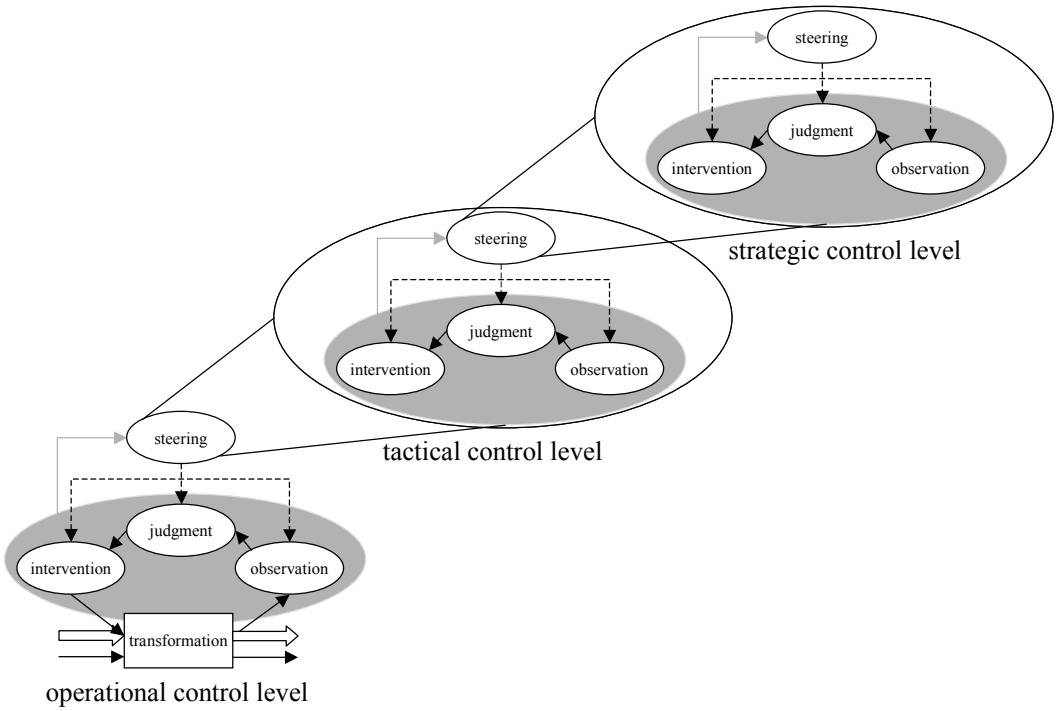


Figure 30 Complexity of the steering element reduced.

In Figure 30 the complexity of the steering element can be seen. The steering element on the operational control level consists of an identical control process, but on the next-higher tactical control level. Similarly, the steering element of the control process on the tactical control level consists of an identical control process on the next-higher strategic control level. Since the highest control level has no control process on a next-higher level, the strategic control level has its own steering element, which comprises the actual organizational values and norms, upon which all the other values and norms are based.

By reducing the complexity of the steering element the analysis process aims to retrieve an ineffective control element. However, the actual interrelations between the different hierarchical control levels must be known. No literature exists to accurately describe how the different hierarchical control levels are interrelated. Therefore, the author has established the relationships, as discussed by Körvers (Körvers et al., 2001b), see Figure 31.

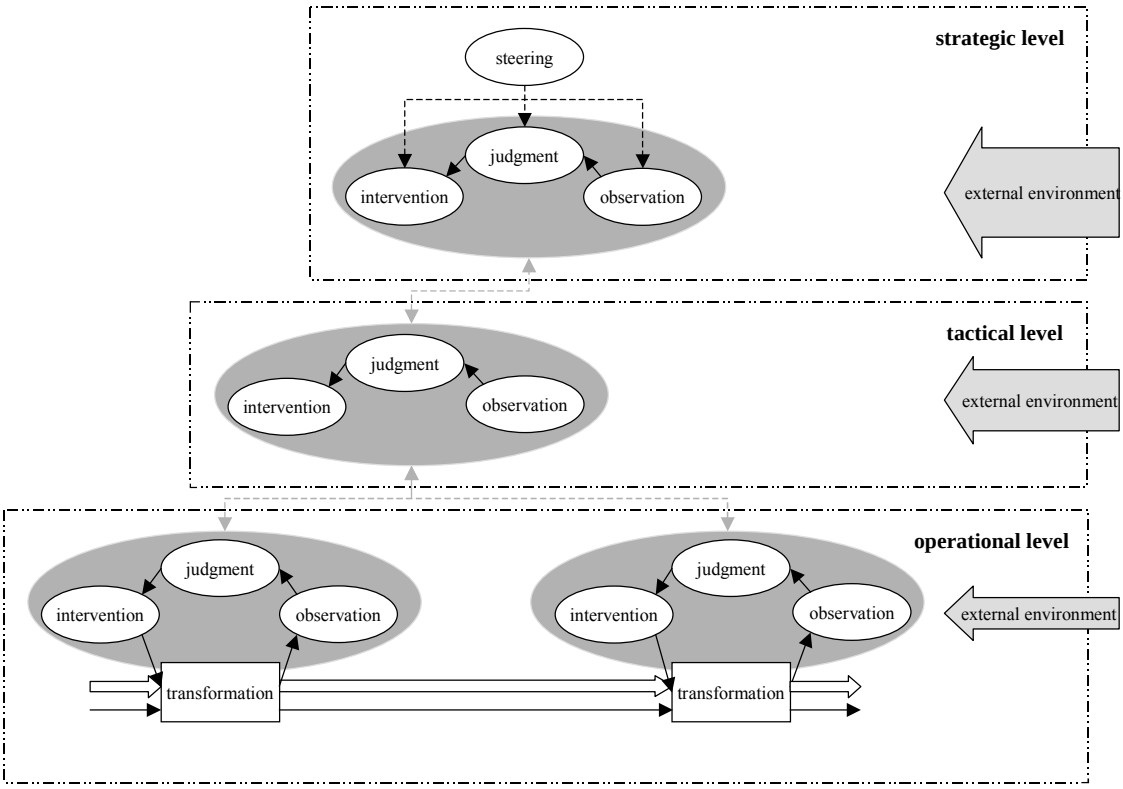


Figure 31 *A simplified model of how the hierarchical control processes are interconnected.*

Figure 31 is explained from the strategic control level to the operational control level. On the strategic control level, the steering element for the tactical control level is derived from the steering element and the control process, i.e. observation, judgement and intervention. The steering to the operational control level is provided by the steering and control process on the tactical control level. Eventually the steering of the operational control level, controls the whole operational process by means of the operational control elements.

Please note how the steering or the organizational values and norms on the next-higher level can also be questioned (second-loop learning) in Figure 31. Moreover, note that the external environment becomes increasingly important in the higher hierarchical control levels.

From the enhanced concepts a structured protocol will be derived, which is presented and discussed in the following Section.

5.3 A protocol for analysis

The final shortcoming of applying the concepts from the previous Chapter on a practical case, was the ambiguity of the method of analysis. Therefore, a more structured approach was developed by the author using the concepts from the previous Chapter and their additional refinements presented in the previous Section. The result is a protocol for analysis consisting of seven stages, which are stated in Table 10. These stages will be explained in detail in the succeeding sub-Sections. In these sub-Sections the purpose, the contents, and an example will be shown. The purpose shows the goals of the stage (‘What’), the contents shows how these goals are achieved

('How') and finally an example, based on the results of the previous case study, will clarify the stage.

Table 10 The proposed 7-stage protocol.

1.	**Select the research area**: Selecting the boundaries of the case and identify the primary and part of the secondary process (operational process), which together with the tertiary process constitutes the research area.
2.	**Identify precursors**: Identify individual re-occurring deviations in the operational processes (precursors) of the selected research area.
3.	**Prioritize precursors**: Prioritize the list of precursors according to their perceived risk classes.
4.	**Identify the ineffective control processes**: Identify the accompanying control processes and the initial ineffective control elements on the subsequent hierarchical control levels that let the prioritized precursors occur.
5.	**Identify the latent conditions**: Identify the conditions causing the control elements on the different hierarchical control levels to be ineffective.
6.	**Identify the affected safety barriers**: Identify if, how and where safety barriers are affected by the identified 'latent conditions' and 'active failures' (resulting in identified precursors).
7.	**Derive conclusions**: Formulate conclusions how safety is interrelated with the control structure in the selected research area.

5.3.1 Select the research area (Stage 1)

Purpose
The purpose of Stage 1 is to define the research area, to establish a clear boundary between factors which are to be included and excluded in the analysis.

Contents
The setting of a boundary around a research area, is achieved by selecting a part of the operational process against a selection criterion which is established by the researcher in accordance with the request of the company's management. Moreover, the tertiary process and the process controlling the selected operational processes are also identified.

Example
In the test case, the boundaries are set around the pesticide company, the operational process is already shown in Figure 27. The tertiary process will be discussed during Stage 4 of the protocol.

5.3.2 Identify precursors (Stage 2)

Purpose
Identify the precursors in the part of the operational process selected as the research area.

Contents
From different data sources deviations present in the operational process are collected according to the criteria that define a precursor. The raw data is then split up into tangible data, that is to say data directly available in the organization, e.g. data present in databases, reports, forms, etc. and intangible data, which is indirectly available in an organization, e.g. data retrieved by interviewing people.

The tangible data retrieved from databases, reports and forms in an organization are:
- (safety:) incidents, inspections, audits.
- (production:) product & process quality deviations, shift & batch problems.
- (logistic:) downtime of reactor, delays in production time.
- (maintenance:) number of resets, repairs & replacements of equipment.

The intangible data obtained by means of interviews are:
- deviations/problems experienced by operators/engineers/managers

From this data, the problems/deviations in the operational process are selected (this means collecting not only directly safety related data). Subsequently, precursors are derived from these individual problems and deviations, according to the precursor criteria. From the previous Chapter and the refinements in this Chapter, the following criteria were retrieved to identify a precursor:

- Occurrence of three or more individual deviations from the transformation's theory-in-use, or espoused theory
- These deviations must all occur in the same input, output, or resource of a transformation.
- These deviations must be equal to each other on the lowest aggregation level as recorded in a company
- These deviations must occur after each other, with sufficient time lapse to enable the organization to learn (to take action).

By using multiple sources for data collection, repeatedly confronting the data with multiple actors (operators, managers, engineers) in the operational process and updating the data, triangulation takes place to address the construct validity and to validate the retrieved data.
By collecting first the tangible data, confronting operators with this data, letting them add or remove some deviations (including the intangible data), until all actors (operators) agree, there is little to no bias from the researcher present in the final collection of precursors and the collection gives a fair and reliable representation of the daily re-occurring deviations in the operational process.

Example
From the analysis of all planning schedules during a time period of six months and interviews with various (chief)operators, one of the deviations present inside the

packaging sub-process (line No. Vg: 'Verpakken groot') appeared to be the shortage of substances while packaging. This deviation occurred eight times in a time period of 26 weeks, see Table 11, as retrieved from the planning schedules and was confirmed by interviews with various operators, see Table 12.

Table 11 Example identical deviations, from the planning schedules of 26 weeks.

date	**order No.**	**No. of products left**	**line No.**	**remarks**
Wednesday, wk 27	76004	100	Vg	product A short
Monday, wk 30	330033	60	Vg	drums halve filled
Monday, wk 40	83005	20	Vg	no more product left
Tuesday, wk 42	9003	80	Vg	product B short
Friday, wk 44	50065	50	Vg	product C short
Thursday, wk 48	86500	200	Vg	no more product left
Friday, wk 50	4500	80	Vg	product D short
Monday, wk 51	15000	200	Vg	product E short

Table 12 Example identical deviations as a result of the interviews.

chief operator 1	filling of the drums stops because of product shortages
operator 1	shortage of product causes tanks to be only partially filled
operator 2	due to scheduling faults product was short while filling barrels
operator 3	frequent filling problem, because products are short

All deviations were in the input of the packaging sub-process. Moreover, the deviations are all equal as shortage of substances while packaging, which is the lowest aggregation level as recorded in the company. Finally, all deviations occurred after each other, with an average time lapse of three weeks (as retrieved from the planning schedules), which is a time lapse large enough for the organization to take action. Therefore, it can be concluded that shortage of substances during the sub-process packaging is a precursor.

5.3.3 Prioritize precursors (Stage 3)

Purpose
Identifying the precursors with the highest perceived risks, to be more focused in finding safety relevant ineffective control elements.

Contents
First the aggregation level of each precursor is determined. The precursors are sorted according to their aggregation level (high aggregation level is prioritized above low aggregation level). Subsequently, the precursors are sorted according to their relative frequency, for each aggregation level. Thus all precursors are sorted according to the property 'likelihood.' Note, that with the precursors obtained only from interviews, the likelihood cannot be unambiguously obtained from data and is therefore estimated by a multi-disciplinary group of experts, which establish the consequences. Additionally to prioritize precursors according to their perceived risks, all precursors have to be sorted with respect to the property 'consequences.' This is achieved by

means of the available accident information and discussing the list of precursors with a multi-disciplinary group of experts from in the company.
To establish the individual risks of all precursors the properties 'likelihood' and 'perceived consequences' are combined in the derived risk matrix, as shown in Figure 29. If there are several precursors of the same class of perceived risk the final choice of which precursor will be analysed further is made by the multi-disciplinary group of experts which established the perceived consequences.

Please note that it is still possible that relevant 'safety precursors' will not be taken into account for further analysis, because the risks are 'perceived risks.' This implies that relevant precursors, actually leading to an accident, may not be taken into account for further analysis.

Example
To draw a comparison between the previous results and the results from applying this protocol, the ten precursors already presented in Table 7 are taken for further analysis. From the derived precursors in the previous stage, which are based on analysing deviations during six months, a prioritized list of precursors is derived. The derived risk matrix for all ten identified precursors is depicted in Figure 32. Note that no lower aggregation level precursors were present amongst the ten identified precursors.

		critical	**marginal**	**negligible**
high aggregation level	**high frequency**	packaging machines not empty when performing maintenance (15/26)	malfunctioning of the machines of the packaging lines (50/183)	product purity problems while extruding (20/52)
		leakages and fumes filling packages from synthesis (30/52)		shortage of packaging material on the packaging lines (100/183)
	low frequency	no correct connection between tank and packaging lines 30/183	clogged extrusion machine (8/52)	shortage of substance while packaging (8/183)
		coagulating of substances while mixing (5/183)	storages overfilled (25/183)	
low aggregation level	**high frequency**			
	low frequency			

Figure 32 Risk matrix to prioritize all ten identified precursors.

The risk matrix as shown in Figure 32, is derived from the previous Section. The ten precursors identified, are placed inside the risk matrix. The number below each precursor shows the relative frequency, e.g. in the first row, first column 15/26 means that during the specified time span of six months, on 15 occasions the packaging machines were not empty when performing maintenance activities on these machines, while maintenance activities are weekly (52/2=26) carried out on these machines.
From the risk matrix depicted in Figure 29, the risk classes of all identified precursors can be derived. With respect to Figure 32 this means that the precursors present in the three dark grey cells are classified first, the two grey cells are classified second and the light grey cell classified third.

5.3.4 Identify the ineffective control processes (Stage 4)

Purpose
Identify the corresponding control processes of the identified precursors and retrieve the initial ineffective control element that enables the deviation to re-occur.

Contents
In practice the processes controlling the identified and prioritized precursors are identified by taking the theoretical hierarchical control model, as shown in Figure 31, as a reference. The controlling processes identified in practice are linked to their theoretical counterparts to constitute the control processes of the identified precursors. When these control processes are identified, the ineffective control elements are identified by the flow scheme, depicted in Figure 33.

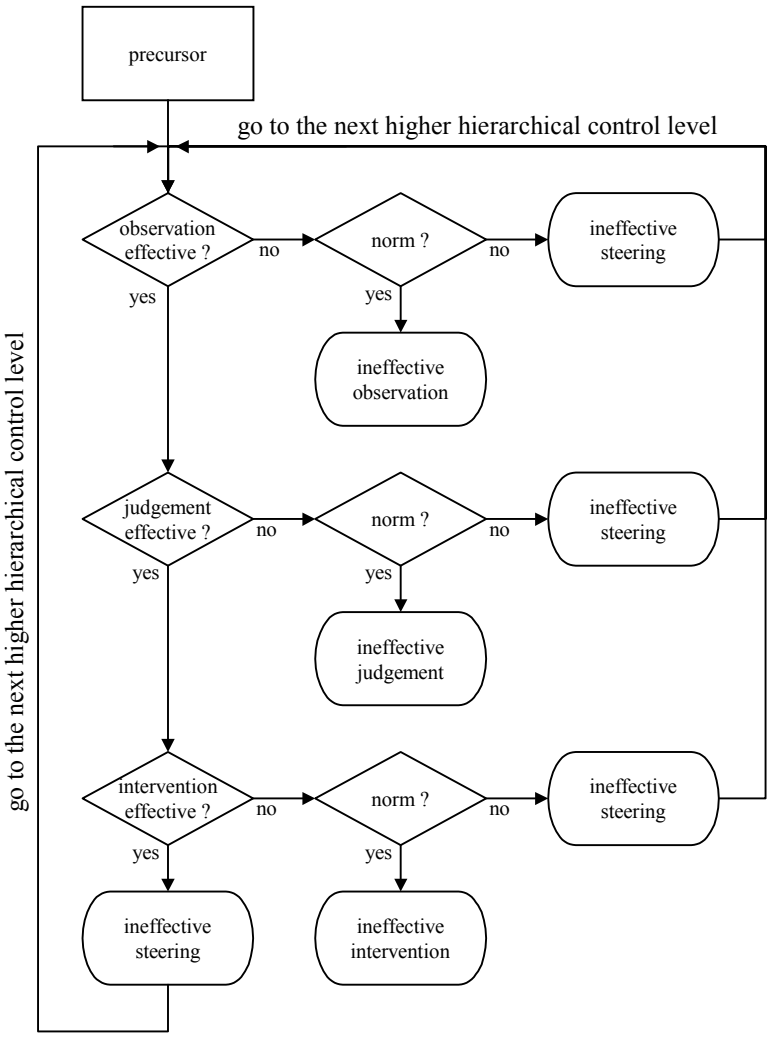


Figure 33 Flow scheme to identify the failing control element.

This flow scheme structurally checks whether or not a control element is working effectively. This flow scheme is used as a guideline on each successive hierarchical control level (operational, tactical, strategic), starting on the operational level.

The flow scheme works as follows, starting with an identified precursor the first diamond is reached. There, the effectiveness of the subsequent observation element is

checked (observation effective?). If the observation element is not effective, an additional condition is tested, concerning the organizational values and norms provided by the steering element (norm?). The process steering the observation is only considered to be ineffective when one or both of the following criteria are satisfied:

- is the control function executed according to the norm? and/or
- does a norm exist?

In all other cases the observation itself is considered to be ineffective (ineffective observation). The other control elements, i.e. judgement and intervention, are checked in a similar way, as can be seen in Figure 33.
If the flow scheme identifies a failing steering element, then the flow scheme continues onto the next-higher hierarchical control level by questioning the control loop on that next-higher level. However, if the steering element is tested on the tactical control level and higher, the first criterion, which has to be satisfied if the steering has to be considered ineffective, must be replaced by the following criterion.

- is the re-occurrence caused by restrictions from the next-higher level?

If this condition is not satisfied, the single loop control element is ineffective and not the double loop steering element. This will successively repeat itself, up to and including the highest, strategic control level. If a steering element is identified as ineffective on the strategic control level the analysis stops and doesn't continue. In this way the initial ineffective control element can be identified, and is considered to be the 'origin' of the fault that initially enabled the precursor to occur.

Please note, that the analysis discriminates between the ineffectiveness of any single loop control element and the ineffectiveness of the corresponding (double loop) steering element, where the steering element has the benefit of the doubt. If any single loop control element seems to be ineffective, the steering element is questioned (norm?). If all control elements perform according to the corresponding norms, then the steering element is said to be ineffective and the analysis continues by unfolding that steering element, i.e. by questioning the single loop on the next-higher control level.

Example
From Figure 32, the precursor 'packaging machines not empty when performing maintenance,' prioritized as belonging to the first risk class, is taken as an example, to identify the controlling process for this precursor in practice and to identify the initial ineffective control element.

The precursor was identified in the maintenance sub-process. In practice, the operators from technical support observed the presence of substances inside the packaging machines. Subsequently, they consulted the chief operator on how to remove the substances from the machines and perform the most suitable intervention. These actions correspond with the control elements on the operational control level. The actions were performed in order to resume production quickly, and adhere to planned schedules. Additionally, experience and training provided the operators with guidelines on how to perform the maintenance effectively. In practice the production manager, responsible for any preventive solutions was not aware of the existence of this precursor and consequently had no overview of these deviations even though the company's quality and safety standards required an overview of all deviations and

measures to handle them. These latter elements are part of the control process on the tactical control level. Subsequently, the initial ineffective control element can be derived using the flow scheme of Figure 33. The path, showing how the initial ineffective control element is retrieved, is depicted in Figure 34.

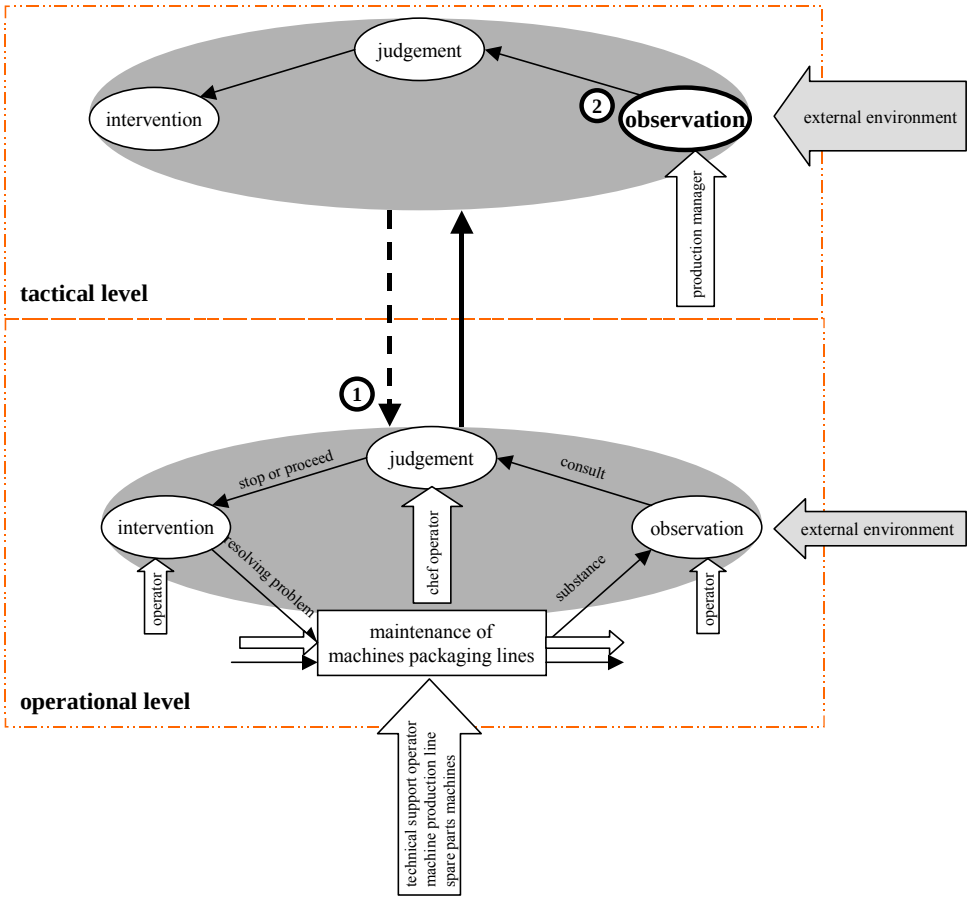


Figure 34 The path to the initial ineffective control element.

The precursor ‘packaging machines not empty when performing maintenance’ is effectively observed by operators from the technical support. Judging is performed according to the norms as is the subsequent intervention. This concludes, as can be derived from the flow scheme, that the steering element at the operational control level has to be ineffective (see number 1 in Figure 34). The ineffective steering on the operational control level was the absence of procedures to remove the substances from the packaging machines. Continuing on the tactical control level, it appears that this precursor was not known on tactical level. This implies that the observation element on the tactical control level is ineffective (see number 2 in Figure 34), while the steering element on the tactical control level stresses the overview and procedures for handling deviations. Finally, the ineffective observation element on the tactical control level enables the re-occurrence of full packaging machines when performing maintenance.

5.3.5 Identify the latent conditions (Stage 5)

Purpose
To identify the latent conditions which enable the initial ineffective control element.

Contents
The situation of an initial identified ineffective control element is reconstructed by checking the six types of latent conditions for their causal contribution to the ineffectiveness of the control element. A latent condition type contributes if it is missing, or dominantly present. These contributing types of latent conditions clarify the actions and assessments people made at the point in time causing the control element to be ineffective. These types of latent conditions are divided into information flows, i.e. transformation, history, organizational values and norms, external environment, and resources, i.e. infrastructure and human. Graphically, the six possible types of latent conditions, are displayed as the arrows interacting with a control element, as already shown in Figure 25.

Example
The ineffective observation element on the tactical control level, as identified in the previous stage, is analysed in more detail by retrieving the types of causal latent conditions, contributing to the ineffectiveness.
For the initial ineffective observation element, information about the transformation was not available on the tactical level. Moreover, no information was available of previous deviations. Finally, constraints for orders to be delivered in time were present, as fines were levied for each day of late delivery (information regarding the organizational values and norms). The types of causal latent conditions are information regarding, transformation, history and organizational values and norms. These three types of latent conditions cause the ineffectiveness of the observation element and enabled the re-occurrences of substances in the packaging machines when performing maintenance.

5.3.6 Identify the affected safety barriers (Stage 6)

Purpose
To identify how the ‘latent conditions’ and the precursors affect the safety barriers that are present in the organization.

Contents
Once the ‘latent conditions’ and the precursors are identified in the company’s control process and operational process, the effects on the company’s safety barriers can be retrieved. The safety barriers present around the transformation process will be identified, i.e. technical, human, and organizational functional categories of safety barriers. Subsequently, the identified types of latent conditions are tested to check if they affect the identified safety barriers. The safety barriers can be negatively, positively, or not at all affected by the identified types of latent conditions.

Example
The ineffective observation element on the tactical control level from the previous sub-Section is taken as an example. The safety barriers involved in the transformation,

are the safety procedures (organizational) and personal protective equipment (technical) which are legal and company requirements. However, the types of latent conditions identified in the previous sub-Section showed that there were no procedures in the operational process which prescribed how to react when there are (hazardous) substances inside equipment (packaging machines) under maintenance.
The 'latent conditions' and 'active failure' that result in precursors, affect the use of a legally required safety barrier, i.e. the safety procedures prescribing how to react when substances are present inside the packaging machines.

Please note that, not removing substances (pesticides amongst others) from equipment (here packaging machines) during maintenance can cause serious accidents, as known from FACTS (FACTS, 2002).

5.3.7 Derive conclusions (Stage 7)

Purpose
To indicate the weaknesses in the safety management systems.

Contents
The number of initial ineffective control elements on each hierarchical control level (=where) and the corresponding latent conditions leading to these ineffective control elements (=why) will be discussed. The results of the discussion will be reflected on the number of affected safety barriers (=consequences). Furthermore, the individual affected safety barriers will be combined, to find possible 'alignments' of affected safety barriers that enable accidents (=risks). Finally, the weaknesses of the current safety management system are indicated by the previous findings.

Example
As a result of analysing ten precursors, mostly the observation (3) and judgement (4) elements on the tactical control level enable the precursors to take place in the operational process. Additionally, the observation (2) and judgement (1) elements on the operational control level were identified as being ineffective. These ineffective control elements were caused by the following distribution of types of latent conditions: transformation (6), history (8), organizational values and norms (9), external environment (2), human (3), infrastructure (4). On the tactical control level the strict delivery times coupled with; the lack of safety considerations (organizational values and norms), the lack of historical information regarding previous deviations and the lack of information regarding the transformations, caused ineffectiveness and enabled precursors. Similar shortfalls were reflected on the operational control level which together with the lack of qualified people (human) caused ineffectiveness and enabled precursors. Finally, 12 safety barriers were identified as 'negatively' affected from nine cases (transformations and precursors). In one case (transformation and precursor); i.e. product purity problems while extruding, no affected safety barriers could be identified. Examples of negatively affected safety barriers are; the lack of procedures for handling hazardous substances, overriding shutdown system, ignoring safety checks, ignoring legally required storage prescriptions, etc.

By combining the affected safety barriers and their latent conditions, greater insight was gained into the two accidents which 'suddenly' occurred, mentioned in sub-Section 5.1.1.

The underlying causes why the first accident occurred, is briefly discussed below:
The re-occurring lack of packaging material on the packaging lines, was caused by an ineffective observation element on the tactical control level. The strict delivery times, the lack of historical information regarding previous deviations and the lack of information regarding the transformation process enabled this precursor, and subsequently over-rode a shutdown system. The function of the shutdown system was to stop the packaging lines, if there were no packages underneath the spraying nozzles, which filled the packages with hazardous substances. The operators switched to manually to stop the spray if they can see that a problem could occur. However, any abrupt stoppage of the supply of packaging material causes hazardous substances (pesticide and liquid pressurised gas) to be injected into the free space of the packaging hall. The machines of the packaging lines often malfunctioned and before starting maintenance or repairs the technical support operators usually had to remove the hazardous substances from inside the machine. The accident occurred when a machine, adjacent to the packaging machine under maintenance, sprayed hazardous substances into the packaging hall. The hazardous substance, which was a mixture of liquid pressurised gas and pesticides was injected into the packaging hall, were it was ignited by sparks from the machine under repair. Fortunately, the fire was extinguished quickly with only minimal damage.

The underlying causes of the second accident are briefly discussed below:
Due to the strict delivery times, no safety considerations (organizational values and norms) and the lack of historical information regarding previous deviations, causing ineffective observations on the tactical control level, a hose was repeatedly wrongly connected between a tank (this time containing toxic powder) and the packaging lines. Machines of the packaging lines malfunctioned repeatedly owing to an ineffective judgement on the tactical control level. The occurrence of these two events resulted in a spill of 100 kg of toxic powder and resulted in several operators suffering from severe breathing problems which required hospital treatment.

The SMS is lacking especially on tactical control level, where a number of safety directives are not followed effectively and the consequences of deviations are only analysed for time constraints. Improving the observation and judgement element on the tactical control level can be achieved by addressing the latent conditions.

In contrast to the perception of the company's management, the tertiary process, instead of the primary process executed by the operators was responsible for the unreliability problems and accidents that had occurred. Countermeasures were suggested and the company was advised to implement a deviation reporting system, which collects daily deviations, stores, analyses and monitors them. Moreover, the causes of these deviations must be adequately addressed to reduce the numbers of deviations in future. In order to achieve this, less pressure must be put on time constraints and time schedules must be fixed and not constantly changed during operation. Instead of time constraints, safety awareness must be increased, by giving operators additional training and stimulating reporting of deviations and 'problems.'

Using the 7-stage protocol, the previous accidents can be explained and causal weaknesses in the safety management system of the company can be identified, i.e. the identified latent conditions on the tactical and operational control levels. To test the working of the developed protocol further, in the next Chapter practice will be approached from hindsight to verify whether other accidents can also be explained. If this is a success, practice will be approached pro-actively.

The choice of the small company for the case study, gave the advantage of retrieving an overview of all processes quickly. However, on the debit side the company had the disadvantage of having a highly informal way of working. This informal way of working often created sudden changes in the control structure such as when the director decided that certain orders had to be produced first or must be stopped or equipment and personnel 'borrowed' from neighbours, etc. It is therefore preferred that in subsequent cases the developed protocol will be applied on more formal organizations, which implies larger organizations such as suggested in the selection criteria.

Chapter 6

ANALYSING RECENT ACCIDENTS WITH THE 7-STAGE PROTOCOL

In this Chapter further evidence is provided that precursors exist long before they escalate into an accident. It will be demonstrated that the existence of precursor information could have been used to foresee and even prevent recent accidents with hazardous substances. Moreover, a set of precursors retrieved from 17 recent accidents in the Dutch chemical process industry is used to validate the 7-stage protocol developed in the previous Chapter. In spite of the limited accident information it is shown that if a proper control action had been initiated, all of these 17 accidents could have been prevented.

Section 6.1 is based on a paper by: Körvers P.M.W., Sonnemans P.J.M., Beek van P.C., 2003. Are accidents always unforeseeable?, Proceedings of the annual Loss Prevention Symposium AIChE, New Orleans, pp. 483-492. The remainder of this Chapter is based on a paper by: Sonnemans P.J.M., Körvers P.M.W., Brombacher A.C., Beek van P.C., Reinders J.E.A., 2003. Accidents, often the result of an 'uncontrolled business process' – a study in the (Dutch) chemical industry, Quality & Reliability Engineering International 19(3), pp. 183-196.

6.1 Precursors and re-occurring accidents

In the previous Chapters it was shown that re-occurring deviations (precursors) are often present in the accident trajectory. Kletz (Kletz, 1993) predicted in 1993, that accidents were re-occurring and were doomed to repeat in years to come. To confirm that precursors are often present within accident trajectories, a study is performed to confirm Kletz's prediction about re-occurring accidents and secondly to find 'similar' precursors within these re-occurring accidents. By showing that 'identical accidents' are preceded by the same precursors, only the tip of the iceberg of accidents preceding by precursors is revealed. It is assumed that by showing the existence of 'identical accidents' preceded by the same precursors, in reality many more accidents re-occur which could have been prevented by learning from precursors in the past. Pasman (Pasman et al., 2002), shows an example of a re-occurring 'identical accident' with the same precursors present prior to the accidents. To retrieve other examples, from the accident database FACTS, 'identical accidents' were retrieved. Recent accidents (1997-2002) which have the highest level of information richness (indicated by 5-stars) are selected. From this collection of accidents, ten accidents were selected by the following criteria, re-occurrence of the accident, preceded by identical precursors, in the same company. In all ten cases several precursors were present prior to the accidents. However, from this set of precursors, one characteristic precursor was chosen per re-occurring accident, that is the precursor which was predominantly present. Predominant precursors are defined as the initial re-occurring events which are present in both accident trajectories examined. Subsequently, the complete accident database was searched for past 'identical accidents' with the same characteristic precursor in other companies. The definition of an identical accident is an accident occurring in the same technical environment, with the same substances

and/or equipment present. For example, the unloading of a specific hazardous substance into a storage tank. In all ten cases several identical accidents in other companies with the same characteristic precursors were found.

6.1.1 The search for identical accidents

The ten identified accidents are displayed in Table 13. In the first column of Table 13 the accident number is shown. In the second column of Table 13, the year in which the initial accident occurred is shown. The third column shows the country where the initial accident occurred. The fourth column shows the characteristic precursor identified and the fifth column gives a brief description of the accident. The sixth column shows the number of previous 'identical accidents' in other companies and the seventh column shows the time period in which these earlier accidents occurred. In the eighth column the different countries where these earlier accidents occurred can be found.

In this study only 'identical accidents' with the same characteristic precursor are considered. This means that many apparently similar accidents are not listed in Table 13 e.g. accidents in which the same precursor, occurred prior to different types of accidents and accidents that are identical but preceded by different precursors. However, by showing that several identical accidents preceded by the same characteristic precursor do exist, the best case situation is revealed, reality will be worse. The existence of these types of accidents shows that, even now, companies don't learn as well as they could. The statement of Kletz (Kletz, 1993) that accidents re-occur can indeed be confirmed by this study, showing only at best the tip of the iceberg. An example of such an 'identical accident', preceded by the same characteristic precursor, was discussed in Chapter 3 and will only be briefly repeated here.

In 2001 a tanker exploded in The Netherlands while filling a tank with nitrous oxide (N_2O), which caused severe damage to the immediate surroundings and slightly injured 11 peoples. The explosion was caused by the bearing of a pump overheating, which led to an explosive decomposition of the N_2O vapour in the tank. The pump had overheated on previous occasions when the bearing had broken down. In 1999 the same company experienced a similar accident. The overheated bearing of a pump caused an explosive decomposition of the N_2O vapour, however, this time not in the tank, but in the pump. The vapours of N_2O were stopped because the transportation hose was cold enough to stop the explosive decomposition of vapours from entering the tank. Therefore, the N_2O vapour decomposed in the pump and exploded there, which caused the liquid N_2O to flow out of the tank.

In search for similar accidents with the same re-occurring deviations prior to the accident, two cases were identified here. In both cases an explosion occurred during the unloading of a tanker when a pump overheated causing a decomposition of N_2O vapour, resulting in an explosion.

Table 13 The selected accidents and their 'identical' predecessors from FACTS.

nr.	year	country	'precursor'	description accident	number of 'identical accidents' in FACTS		
					numbers	years	countries
1	2001	The Netherlands	overheated pump	While filling a tank car with laughing gas the tank exploded	3	1979 -1999	USA, The Netherlands
2	2000	Great-Britain	odor complaints	Dissipation of natural gas in the ground, caused an explosion in a house	7	1973 - 1999	USA,Great-Britain
3	2000	USA	presence of explosive mixtures of paint and oxygen	During paint spraying in a badly ventilated area an explosion occurred	5	1979 -1998	USA,The Netherlands, Singapore,Great-Britain
4	2000	Germany	no labels and fixed places for small portions of hazardous substances	Because several chemical materials came together at a laboratory a toxic cloud emerged from the sink	3	1992 - 1999	USA,Switzerland Great-Britain
5	1997	USA	often failure of 'Clow model GMZ check valve'	Wrong functioning of a check valve, relieved an explosive gas cloud and exploded	4	1980 - 1994	USA,Saudi-Arabia
6	2001	USA	often wrong or false value on level measure device	During maintenance polymer waste ignited an caused an explosion of the tank	3	1965 - 1989	USA,The Netherlands
7	2001	USA	clogged relief valves	While removing a pipeline, gasoline was present and ignited	7	1970 - 2001	USA,Japan,Spain, The Netherlands
8	2002	USA	no precise coordinates for excavation work	During excavation activities a natural gas pipe got damaged causing the environment to be evacuated	5	1980 - 1999	USA,The Netherlands
9	2001	USA	Flickering flames when igniting furnace	Due to a wrong ventilation, an explosive mixture aroused in a furnace and exploded	6	1979 - 2001	USA,The Netherlands
10	2001	Switzerland	no verification of material and equipment of tank car	At transshipment of hazardous substances, wrong substances contacted and reacted	6	1986 - 2000	USA

It is a common observation that events in the past appear simple, comprehensible, and predictable in comparison to events in the future. The hindsight bias is the tendency for people with knowledge about the outcome to falsely believe that they could have predicted the reported outcome of an event, Christensen-Szalanski (Christensen-Szalanski et al., 1991). After learning of the occurrence of an event, people tend to exaggerate the extent to which they could have foreseen the likelihood of its occurrence. In this Chapter searching for precursors in accident databases is susceptible to this hindsight bias because the importance of precursors was highlighted in Chapter 3. To overcome this problem, in Section 6.1 the presence of precursors in the accident trajectories were rated independently and then confirmed or rejected by another rater. One rater was the author and the other rater was an experienced accident investigator. Both used the same accident information, which resulted into the precursors as listed in Table 13.

6.1.2 Results from the study

The conclusions resulting from this study are, that for all ten accidents characteristic precursors were present in 'identical accidents' that had happened before. Second, the value of detailed accident information is shown. If the companies had the information regarding identical accidents and preceding precursors available beforehand these accidents could have been prevented. From the lessons in the past, precursor and scenario's can be identified to initiate measures and prevent the accident. Therefore, it can be concluded that in many cases learning opportunities are present prior to an accident by looking for re-occurring deviations. Indications for possible accidents and accident mechanisms can often be found from the past. To classify an accident immediately as 'unforeseeable', as companies often do, to avoid legal fines or negative publicity, cannot always be justified.

The results from the study into 'identical accidents' show that precursors often do exist prior to accidents. The existence of precursors prior to accidents creates the opportunity to derive indicators for accidents. To actually obtain a better understanding of how and why accidents can occur in spite of the presence of precursors prior to accidents, in the next Section 17 recent accidents from the Dutch chemical process industry will be analysed using the 7-stage protocol.

6.2 Analysing accidents

That precursors are frequently observed in accident trajectories was stated in the previous Section. In this Section 17 recent accidents in the Dutch chemical process industry are taken and their accompanying precursors and ineffective control processes in the companies identified. This study is executed from hindsight using limited accident information which is the reason for adapting the analysis protocol so that the results of most stages can still be retrieved.

6.2.1 The selected accidents

Like the accidents from Chapter 2 and in the previous Section, the accidents used in this Section are retrieved from the FACTS accident database. As in the other studies, in this case the quality of information is also an important 'figure of merit' for analysing underlying causes of previous situations. Therefore, in this case the

'richness of information' about the accidents was used as selection criterion for the accidents analysed. Only the information-rich accidents, coded with 4 stars and 5 stars, are used for this research. Moreover, influences from cultural differences on the results will be kept to a minimum by retrieving only accidents in the Dutch chemical process industry. The only disadvantage from this criterion is the limitation of accidents available from the database, which is small for the homogeneous base for the analysis created in this way. Moreover, in order to ensure that the analysis is based on recent information, only accidents that took place between 1995 until 2000 are considered.
From all accidents 3,916 accidents happening in the process chemical industry, 585 of them occurred from 1995 until 2000. Only 90 accidents were indicated as 'information–rich'. Finally, from these 90 accidents only 17 accidents happened in The Netherlands. These accidents are selected for further analysis.

6.2.2 The analysis

The 7-stage protocol proposed in Chapter 5 is developed to pro-actively analyse a company. However, in this Chapter, the analysis of previous accidents takes place from hindsight using 'limited' information. Due to this retrospective analysis and the 'limited information,' the developed 7-stage protocol has to be adapted. The following modifications and the reasons for them are stated below:

- Stages 1 to 3, the identification and prioritization of precursors, was not necessary anymore because the accident had already happened. The precursors, present in the accident trajectory, could be retrieved from the available accident investigation information in the database.
- Stage 4, the identification of the initial ineffective control element, can only be identified on the operational control level. Due to limited information (in spite of selecting accidents on the basis of information-richness), hierarchical control levels cannot be identified.
- Stages 5 and 6, the identification of latent conditions and affected safety barriers, cannot be retrieved. Due to the lack of the initial ineffective control elements, the corresponding latent conditions and affected safety barriers cannot be retrieved. The affected safety barriers can be independently identified from the accident information (as will be shown in an example given in this sub-Section). However, the causal relationship between ineffective control and the affected safety barrier cannot be established.
- Stage 7, the conclusions, will only concern the results from the Stages which are (partly) performed.

The protocol requires information which is not present in the accident database in sufficient detail. Often detailed information concerning the organization's 'normal way of working' prior to the accident must be retrieved from the accident information itself. This type of information is often not recorded, or only briefly mentioned in the accident investigation reports. However, the 7-stage protocol can still be used to retrieve insights into how and why accidents still occur.

The modified protocol is described below, starting with identifying precursors from the accident trajectory. When precursors can be identified in the accident trajectory, they become subject of analysis, as stated in Stage 4 of the protocol. The elements on

the operational control level are identified from the accident investigation information available. Subsequently, a model of the control process, operating before the accident, is constructed. The model and the modelling process focus especially on how deviations are handled (and how they should have been handled to prevent re-occurrence). Any ineffective control element in the model indicates an ineffective part of the control process. To develop this model, the flow scheme in Stage 4 of the developed protocol, see Figure 33, is slightly adapted, in Figure 35. The adapted flow scheme shows two flow schemes representing a single loop analysis (left) and a double loop analysis (right). The dotted lines mark the differences between the two schemes.
The second difference between the first flow scheme and the flow scheme presented in Figure 35, is the subset of '?' indicating whether control elements can be identified or not from the accident information available. This subset indicates that control elements can neither be identified as effective nor as ineffective from the accident information available.
The third difference between both flow schemes is that in Figure 35, the flow does not stop when an ineffective control element is reached. In the flow scheme in Figure 35, it will continue until all elements of the single control loop, i.e. observation, judgement, intervention are questioned at least once for the left flow scheme and until all elements of the double control loop, i.e. observation, judgement, intervention and steering are questioned at least once for the right flow scheme. The flow schemes are developed in this way in anticipation of incomplete information in the accident database. It is possible that accident information is unable to correctly identify whether a control element is ineffective. Stopping the analysis at this control element can lead to a wrong diagnosis of the effectiveness of successive dependent elements. The developed flow in the flow schemes effectively deals with the gaps in the accident information, by successively checking if all control elements can be identified as effective, ineffective or unknown, as recorded in the accident database.
The fourth difference is the limitation of only including the operational control level, which results in stopping the flow in the flow scheme of Figure 35 after questioning all control elements on the operational control level.

Both flow schemes start with identifying if precursors are present prior to the selected accidents, see the first diamond from the top of both schemes, asking if precursors can be identified yes (y) or no (n). If there is no precursor information available, the accident is characterized as 'unforeseen'. This first step concerns a discrimination between accidents that could have been prevented by proper control and learning from previous deviations and accidents that are 'unforeseen', i.e. accidents were no precursors were present or no precursor information was available in the database.
Once the presence of a precursor is ascertained, the first diamond in the second column of both schemes is left. Starting to check the effectiveness of the subsequent control elements, i.e. an effective observation, judgement and intervention, in three successive Stages as can be seen in the second column of the single loop scheme (left in Figure 35). This single loop scheme in Figure 35 counts the number of ineffective elements in the single loop control mechanism, for each identified precursor.
In the double loop scheme of Figure 35 (right in Figure 35) the effectiveness of the steering process is checked in addition, in case of any ineffective control elements. To do so, an additional condition is tested, i.e. the norm provided by the steering element (double loop) is questioned. Only if one or both of the following criteria is satisfied, then the steering process is considered to be ineffective;

- do the records show that the control function was executed according to the norm?
- do the records show that a norm did not exist?

In all other cases the appropriate control element is considered to be ineffective.
The double loop analysis questions the steering process if any single loop control element seems to be ineffective. So the analysis discriminates between an ineffective single loop control element and an ineffective corresponding (double loop) steering element, where the steering element has the benefit of the doubt.

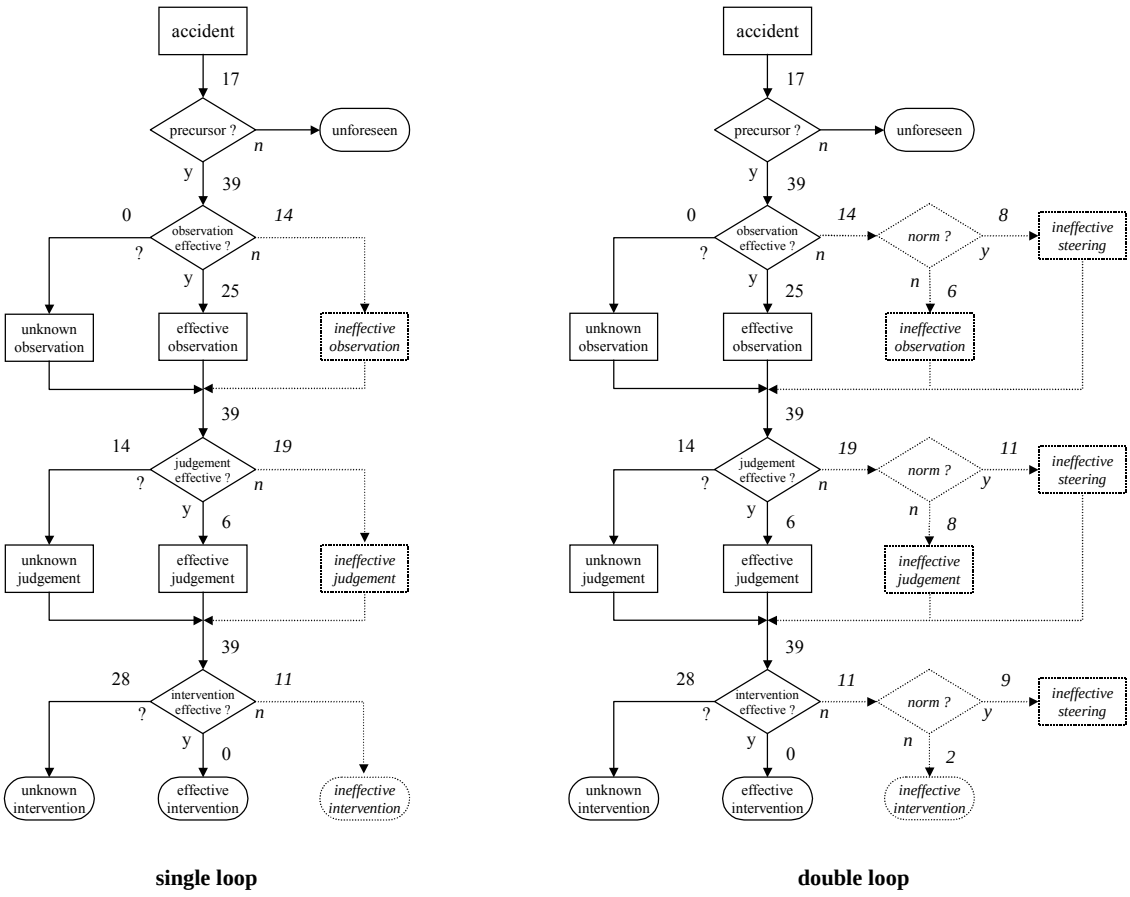


Figure 35 The flow schemes for single and double loop analysis.

In order to demonstrate the use of the analysis flow scheme of Figure 35, one of the accidents from the FACTS database is described and analysed according to this analysis flow scheme. The accident description in the FACTS database is very detailed and only a summary is given here.

In 1997, an explosion occurred in a furnace of an oil distillation unit, resulting in a shutdown of the whole unit. The explosion occurred during a hot restart and resulted in a rupture of the entire furnace, which badly injured one operator. The total costs of damage was estimated to be $10.000.000 for loss of production and business interruption.
Since the initial start-up of the furnace in 1995, the stack damper controlling the oxygen level had been little used, because it was very difficult to operate. Several complaints had been made to direct attention to this problem, but all to no avail.

During start-up, the floor operators near the furnace could often see the flames of the burners flickering, indicating that the furnace was not operating properly. When this happened immediately prior to the accident the control room operators lowered the oxygen inlet as usual. At this particular moment flames were coming out of the inspection hatches, which was a known indication for a lack of oxygen. As a reaction, the floor operators opened the stack dampers to provide more oxygen and the sudden draft extinguished the flames. The temperature in the furnace remained above 700 ^{0}C and the gas supply did not close automatically. After 15-20 seconds the gas-oxygen mixture ignited in a hot spot resulting in the explosion which ruptured the furnace.

This accident will now be analysed according to the analysis flow chart. The first step is to identify re-occurring deviations prior to the accident. In this case the repeated complaints of the operators about the difficulty in operating the stack damper and the re-occurring flickering of the flames are identified as soft and hard precursors, respectively.
In the next steps the elements of the single control loop, i.e. the control elements 'observation', 'judgement' and 'intervention', are checked by questioning their presence and effectiveness, according to the left flow scheme of Figure 35 (single loop).
Starting with the re-occurring complaints as the first precursor, the database information shows that the operators frequently passed this precursor information to the management. Therefore the observation is effective. The management, as the responsible authority, didn't consider the information to be important enough to require any action. No information could be found in the database about any intervening activities concerning this precursor (e.g. maintenance or modification of the stack damper). As a result, the control loop of this precursor, according to the analysis flow chart, is qualified as possessing an effective observation, an ineffective judgement and an unknown intervention.
In case of any ineffective control elements the double control loop is checked by questioning the presence and effectiveness of the corresponding norm. This is illustrated by the right flow scheme of Figure 35 (double loop).
In case of a lacking norm and/or an existing, but ineffective norm, the steering element is considered to be ineffective. In all other cases the appropriate control element is considered to be ineffective. In this particular case no confirmation of an existing norm regarding the judgement could be found, which results in the conclusion that the steering element was ineffective instead of the judgement element.
The observation of the flickering flames (second precursor) by the floor operators and control room operator was effective. The control room operator responded by deciding to lower the oxygen inlet as a usual intervention, which, however, proved to be ineffective because the subsequent lack of oxygen caused the flames to come out of the inspection hatches (which triggered the catastrophic opening of the stack damper by the floor operators). Here, the elements 'judgement' and 'intervention' turned out to be ineffective.
The analyses of the double loop shows that a norm was indeed available for the judgement, in the form of training and procedures in case of flickering flames, prescribing that the oxygen level should be adjusted by lowering the oxygen inlet. In this case the steering element was ineffective twice, because from the accident information it was found that the oxygen level should not have been the focus of the control room operators (wrong norm for judgement) and consequently another intervention would be required (wrong norm for intervention). The accident

information showed that experts agreed that the oxygen level is only of importance when the furnace is fully operating, and then merely for reasons of efficiency. The flames coming out of the inspection hatches is not analysed because it is not a precursor, i.e. it is not a re-occurring deviation. According to the available information this was the first time that this had happened.
This example illustrates the use of the slightly adapted analysis flow scheme, as they have been used for the remaining accidents mentioned in the previous sub-Section.

By hindsight-bias, the presence of precursors (Chapter 3) and the knowledge already obtained about the main outcome of the analysis, as shown in Chapter 5 (especially that the steering element is ineffective), the outcome of this accident analysis can be affected. Therefore, the presence of precursors in an accident trajectory and the identification of ineffective control elements, were independently rated by the author and the experienced accident investigator, also used in Section 6.1. The author rated the accidents with hindsight bias. The other rater didn't have any knowledge of precursors (Chapter 3) and high percentages of ineffective steering elements causing these precursors (Chapter 5). Both raters used the same accident information and independently identified the precursors (operational re-occurring deviations) present in the 17 accident trajectories. The first rater identified 43 precursors from the 17 accidents, while the second rater found 37 precursors. They finally reached consensus on 39 identified precursors. Subsequently, both raters analysed these 39 precursors, using the developed flow-scheme as shown in Figure 35. The results of both raters analysing the 39 precursors are displayed in Appendix A.

To measure the agreement between the two raters (before the final consensus) Cohen's kappa is calculated, this is a statistic in which agreement levels are corrected for change agreement, for each variable separately. In this case κ=0,87, indicating that there is almost a perfect agreement. In this way the hindsight bias is addressed and the inter-rater reliability is expressed as a κ-value, which increases the total validation of the results. The results presented in Appendix A have been scrutinized and subsequently reviewed resulting in a final consensus. This final consensus between both raters is displayed in Table 14 and is used in the remainder of this Chapter.

Table 14 Final consensus both raters.

	effective			unknown			ineffective steering			ineffective		
	observation	judgement	intervention	observation	judgement	intervention	observation	judgement	intervention	observation	judgement	intervention
Consensus	25	6	0	0	14	28	8	11	9	6	8	2

6.2.3 Results of the accident analysis

The information used in this research is based on the information that can be retrieved from the FACTS database. It is possible and even likely that more information about precursors was available before the real accident happened, implying that the amount

of precursor information in reality may be larger than could be identified from the FACTS database.

For all 17 accidents of this study, precursors could be identified. None of the 17 accidents could be classified as 'unforeseen'. A total number of 39 precursors were identified in these 17 accidents which seems extremely low compared to normal accident analysis experience. Detailed accident analysis normally retrieves dozens of near misses and deviations leading to the final accident (e.g. van der Schaaf (Schaaf van der, 1992)), implying the existence of many more precursors. However, the limited amount of detailed information present in the FACTS database is the restricting factor here. The FACTS database reflects the kind of accident information companies and government agencies collect. It demonstrates clearly that detailed information about the period before the accident is not often collected.

For each precursor, one or more control elements turned out to be ineffective. This justifies the remark that this study gives no rise for questioning the completeness of the control model.

Analysing these 39 precursors according to the 'single-loop learning' part of the scheme given in Figure 35, and discussed in the previous sub-Section, results in ineffective, effective, and unknown subsets of control elements as is given in Figure 36, representing the answer for the single loop learning cycle.

From these results it can be seen that for all 39 precursors,

- the observation was ineffective in 14 (36 %) of these cases,
- the judgement was ineffective in 19 - 33 (49 % - 85 %) of these cases,
- the intervention was ineffective in 11 - 39 (28 % - 100 %) of these cases

as is indicated in Figure 36. Note, that there is a range of ineffective judgement and intervention elements which falls into 'unknown' class.

From these 39 precursors, a total of 44 elements in the single-loop can be positively identified as ineffective. The 19 identified ineffective judgements are the largest in number (49 %) and the 11 identified ineffective interventions are the smallest in number (28 %).

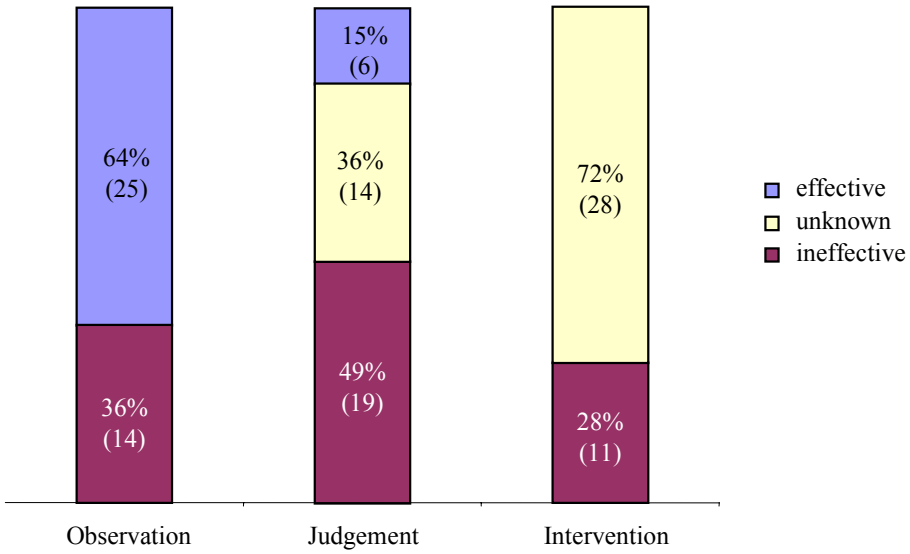


Figure 36 The results of the single loop analysis.

The uncertainty in the identified number of ineffective elements, indicated by the 'unknown' class, grows with the position of the element in the control loop, e.g. the uncertainty about the number of ineffective interventions is larger than the uncertainty about the number of ineffective judgements.

This can be explained by the nature of the documented information. An ineffective observation is easier to detect and to describe than an ineffective judgement.
Another explaining factor is the dependence of the successive elements that make up the control loop. It is very likely that the chance of a subsequent control element being effective, rapidly decreases if one or more preceding elements are ineffective. For example it is not very likely that an intervention will be effective if the necessary preceding judgement was ineffective. This suggests that the number of ineffective control elements does not decrease with the position of the element in the control loop, i.e. the number can only increase. However, this cannot be unambiguously confirmed by the database, due to the growing part of the 'unknown' class.

The additional double loop analysis gives more detailed information regarding the 44 ineffective control elements, distinguishing true ineffective elements of the 'single loop' from the false ineffective elements that in fact concern the 'double loop learning', i.e. an ineffective steering element. The results of this additional analysis are presented in Figure 37.

From Figure 37 it can be observed that 21% from the total of the 36% ineffective observation elements were caused either by a wrong steering element, or the absence of any steering element. For the other two control elements similar conclusions can be made. If the results are arranged differently according to the actual ineffective origins, Figure 38 can be obtained.

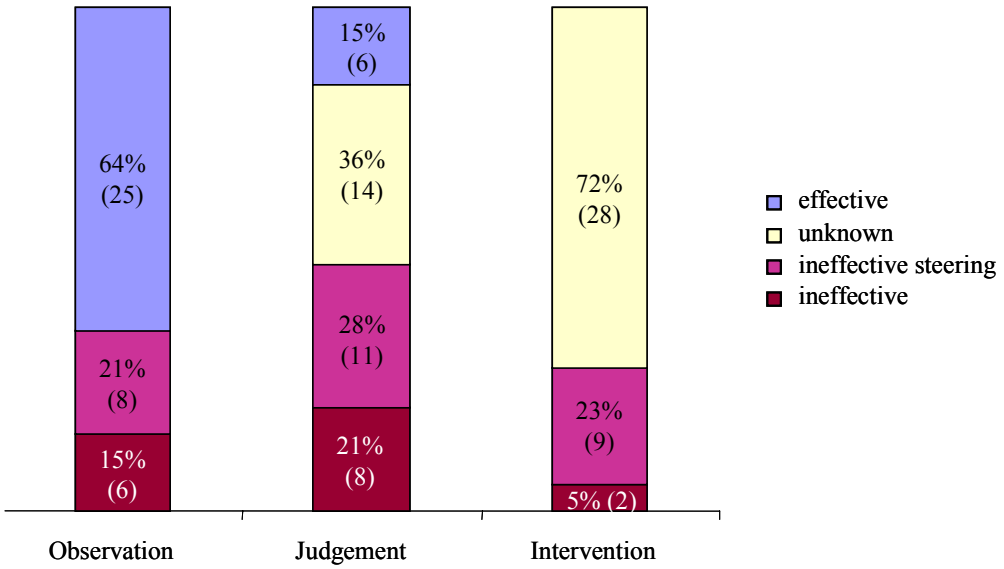


Figure 37 The results of the double loop analysis.

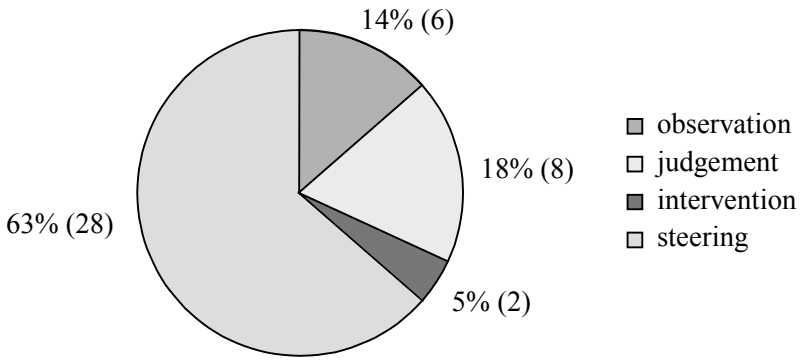


Figure 38 Distribution of ineffective control elements.

From this figure, it can be seen that in more than 60 % of the single loop control elements initially indicated as ineffective (total of 44 elements), the true 'ineffective element' originates from the double loop learning cycle, i.e. the ineffectiveness originates from the steering element. In about only 40 % of the ineffective elements the initial single loop indication was correct.
The additional double loop analysis was constructed in such a way that any ambiguity about the origin of the ineffectiveness would be to the advantage of the steering element, i.e. any ambiguity would not be automatically assigned to the steering part. This implies that the 60 % is a 'best case' result for the steering element. If the FACTS information, concerning the identified ineffective elements, had been entirely unambiguous, the part representing the steering element as ineffective origin, could be even larger.

6.2.4 Important Observations

During the examination of the information from the FACTS database, it became clear that most accidents could be linked to changes or alterations in the company. These include not only technical and organizational changes, but also alterations in human staffing.

The deviations, already present, had not led to any serious consequences yet. In fact the existence of a precursor (re-occurring deviation) implies the ineffectiveness of a corresponding control loop.
Under the stable conditions of the regular way of working re-occurring deviations did not escalate. They remained relatively harmless, until the conditions were changed. Then these harmless deviations could escalate, causing an accident with serious consequences.
A seemingly innocent change in the procedures, e.g. in parts, in staffing, was, almost without exception, the alteration that initiated the propagation and escalation of the deviation. Had the corresponding control loop not been ineffective then the escalation most likely would have been most likely prevented.

6.3 Discussion of the study

Although a common statement is that accidents only happen 'by accident,' from this exhaustive accident study it is demonstrated that, at least for a large group of failures, this is certainly not the case. When analysing several serious industrial accidents gathered in the FACTS database in the Dutch chemical process industry it can be shown that in the vast majority of the cases the occurrence of deviations, together with the process in which they were handled, can be identified as precursors for actual accidents. Although the 7-stage protocol could not be applied in full detail on the selected accidents, the adapted protocol leads to some valuable insights.

The hypothesis posed in Chapter 3; o*ften re-occurring deviations, present in the operational process of an organization, can be identified in the causal path of an accident*, is tested by searching for re-occurring deviations in the operational process, present in accident trajectories. This search led to 39 such events, also called precursors, which were present prior to 17 accidents. As discussed in Chapter 4, not all accidents have precursors present in their accident trajectories, but they are in the minority. Therefore, this hypothesis and the prediction can be confirmed and finally validated.

It is observed due to the existence of precursor information for each accident, none of the investigated accidents could be classified as strictly 'unforeseen'. The accidents are, without exception, the result of one or more uncontrolled process.

In spite of the fact that only the operational control level was considered, it was found that for all 39 precursors

- 14 (36%) of the observation elements were ineffective
- 19 - 33 (49% - 85%) of the judgement elements were ineffective and
- 11 - 39 (28% - 100%) of the intervention elements was ineffective.

Including the double-loop of the control loop, it can be concluded that for at least 60% of the ineffective control elements, the origin of the ineffectiveness has to be sought in the steering element instead of in the ineffective control element itself. From this it is concluded that the steering element of the operational control level (which are the higher control levels in an organization) is the main cause for ineffective control loops.

Applying the adapted 7-stage protocol from hindsight, it highlights that the double loop learning cycle should be the focus of safety improvement programmes. This holds especially true for the double loop learning cycle concerning the control elements that are positioned later in the single loop control cycle, i.e. the elements judgement and intervention. As already shown in the test case of the previous Chapter and also confirmed by the analysis of several recent accidents, the higher control levels in companies are often responsible for letting precursors occur and thereby enable hazardous situations to occur, and even re-occur.

The next Chapter will apply the 7-stage protocol pro-actively in three different case studies in the Dutch chemical process industry, identifying why hazardous situations still exist in the companies in spite of the enormous number of safety measures present.

Chapter 7

THREE CASES IN THE DUTCH CHEMICAL PROCESS INDUSTRY

The protocol developed in Chapter 5, which was applied on accidents as shown in Chapter 6, is applied on three cases in the Dutch chemical process industry. First, the cases are selected according the criteria stated in Chapter 5. Secondly, the developed protocol of analysis is applied on these selected cases, to identify why and how it is still possible that accidents may occur despite precursors and several existing safety barriers. Thirdly, the results from the analysis are further elaborated on, indicating the problems in current safety management systems, allowing accidents to occur.

7.1 The case studies

In the previous Chapter it was shown that the developed protocol for analysis identified the ineffective control elements causing the precursors prior to accidents. However, due to the lack of detailed accident information the conclusions were limited. To perform the analysis, using the developed 7-stage protocol pro-actively (before any accident occurs), cases have to be selected on which the analysis can be performed and from which reliable and generic conclusions about safety indicators and the performance of current safety management systems can be obtained. The next sub-Section will discuss the selection criteria to select suitable cases.

7.1.1 Selecting cases

Like the case study discussed in Chapter 5, the case studies that will be selected in this Chapter are also based upon selection criteria based upon the five major issues as stated by Bickman (Bickman et al., 1998); site selection, authorization, data collection process, accessibility, and other support. Moreover, the cases will be chosen in such a way that all cases can be approached in a similar way, increasing the extent in which the quality of the protocol can be judged, as discussed in Chapter 2.

The selection criteria for the case studies are taken from Chapter 5, i.e. presence of hazardous substances, batch industry, large company, located in The Netherlands. The selection criteria narrowed the search for suitable cases down to large Dutch companies in the batch industry falling under the Dutch Seveso-II directive (BRZO, 1999). To increase the generalizability to Dutch chemical companies in the batch industry, from the around 80 selected companies falling under the previous selection criteria, different companies and different product types were selected.

Eventually, the final criterion, i.e. authorization and access to relevant data, led to the selection of three cases in different chemical companies using batch processes and located in The Netherlands. For reasons of confidentiality the names of these companies cannot be revealed, therefore they are named company A, B and C. Their real names are known to the author. These companies produce coating resins, active pharmaceutical ingredients and plastic granules respectively. By selecting these three

cases according to the replication logic principle as discussed by Yin (Yin, 1994), the extent to which the external validity, establishing the domain to which a study's findings can be generalized, can be increased. According to Yin, by testing a theory through replications of the findings in a second or third neighbourhood, where the same results occur, the results might be accepted for a much larger number of similar neighbourhoods. In the next sub-Section the research areas of all three case studies will be discussed.

7.1.2 The research areas

In this sub-Section the different research areas concerning each of the three selected case studies are shown. The data is collected from the primary process and part of the secondary process, and subsequently analysed to find the underlying problems present in the tertiary process. The primary process and that part of the secondary process which interacts directly with the primary process, e.g. maintenance, internal transportation, etc., is called the operational process and is the area where the required data is collected from. This operational process is shown in this sub-Section by showing the primary processes and secondly by presenting the interacting secondary processes. The tertiary processes will be presented when discussing the analysis of the data retrieved from the operational processes in sub-Section 7.2.4.

For company A, the company producing coating resins, the primary process can be seen in Figure 39. In this figure the upper left arrow represents different raw materials which are delivered by road to the company. These raw materials are initially stored in tanks, drums and bags (storage) and subsequently mixed (mixing). After the mixing the resins are cooled on a conveyor belt (cooling) and transported to a shredder, which shreds the product into pieces (shredding). The shredded product is stored in tanks (storage) and subsequently packed in bags or bins (packaging). Eventually the packaged product is wrapped (wrapping) and stored in a warehouse (storage), awaiting distribution to the customer (lower right arrow).

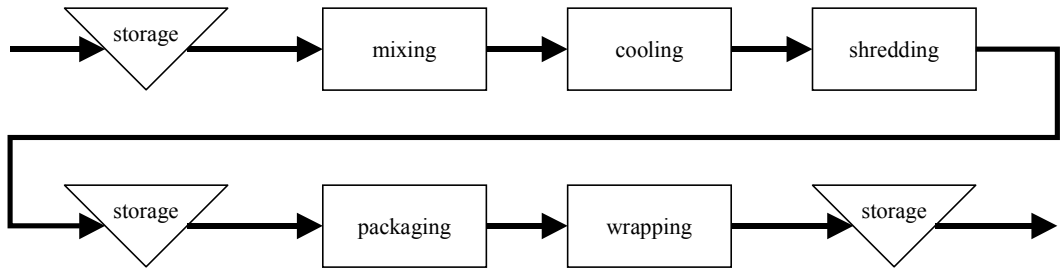


Figure 39 Primary process of coating resins at company A.

For company B, the company producing active ingredients for the pharmaceutical industry, the primary process is depicted in Figure 40. In this figure the upper left arrow represents the different raw materials which are delivered by road to the company. These raw materials are stored in tanks and drums (storage). Subsequently these raw materials are processed by combinations of three different steps: mixing, condensation and cooling, depending on the required end-product. Figure 40 is a simplified representation of this process, by depicting only once mixing + condensation + cooling. After the cooling, the product is filtered or passed through a centrifuge (filtration or centrifugation) and subsequently dried (drying). Finally the

end-product is packed into drums (packing) and put into storage (storage), until distribution to the customer.

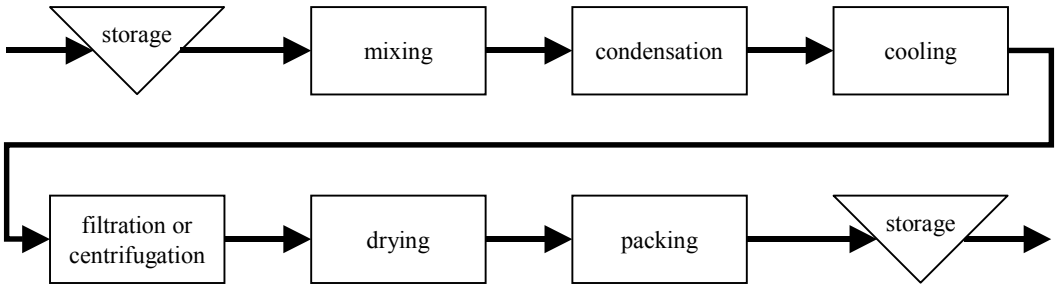


Figure 40 Primary process of active pharmaceutical ingredients at company B.

For company C, the company which produces plastic granules, the primary process is depicted in Figure 41. In this figure the upper left arrow represents the retrieval of solid hydrocarbon from a polymerisation installation. This solid hydrocarbon is stored in several tanks (storage). Subsequently, further ingredients such as stabilisers, anti-oxidisers, etc. are added. By means of an extrusion process the material is pressed through a die-plate and cut into cubes (extrusion + cutting). Subsequently, these cubes are filtered, heated, mixed (filtration + heating + mixing) and packed (packaging) into bags or bins which are eventually wrapped on a pallet (wrapping) and loaded into a truck (loading).

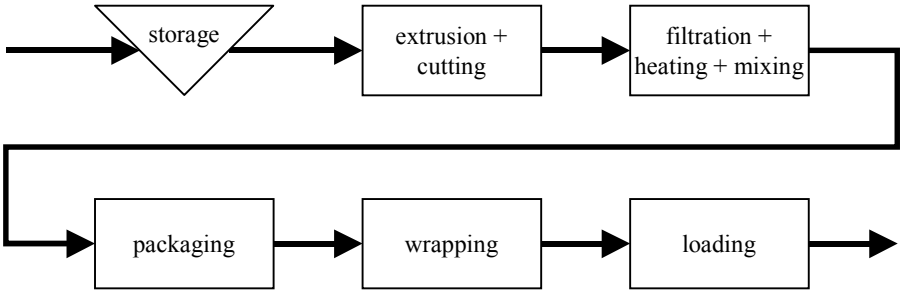


Figure 41 Primary process of plastic granules at company C.

In addition to the primary processes, the following secondary processes are present in all three companies: maintenance, quality and logistics. These processes together with the primary process constitute the operational process, where the initial data for this study was collected. The maintenance process performs scheduled and unscheduled maintenance activities at the different technical installations. The quality process takes samples at different points in the primary process to check the intermediate or final product according to product specifications. The logistic process takes care of the material flow and storage of materials.

After providing this brief overview of the research areas of the three cases, the results of applying the developed 7-stage protocol is presented in the next Section.

7.2 Applying the 7-stage protocol

To establish a good reliability of the analysis and to demonstrate that the analysis can be repeated with the same results (Yin, 1994), the 7-stage protocol was applied on three cases by different researchers. The results of all Stages were obtained by

independently rating of the individual researchers and the author. After discussing the individual results, the consensus was used as the ratings on which further analysis was based. Moreover, by repeating the same approach (the 7-stage protocol) in three different case studies, the reliability was even further increased.
The results of the analysis are discussed in the following sub-Sections, each sub-Section discussing one Stage of the protocol.

7.2.1 Select the research area (Stage 1)

In sub-Section 7.1.2 the operational processes of the three cases were identified. The tertiary processes will be presented in sub-Section 7.2.4, after retrieving the data from the operational processes, which completes the research area, as discussed in Chapter 5.

7.2.2 Identify precursors (Stage 2)

In all three operational processes, deviations from the 'normal' way of working occur due to external and internal changes. Such deviations can be identified by technical means, i.e. automatic registration devices on equipment, and human means, from observations of peoples. Both means are used to construct an overall view of the daily problems present in each operational process.
The construct validity to establish the correct operational measures for the concepts studied (Yin, 1994), is established by using multiple sources of evidence, which are mutually compared to verify the correctness of the data. Moreover, all data are reviewed by key informants, by means of interviews.
All deviations retrieved from the different sources have been divided into hard and soft deviations, as defined in Chapter 3. The sources used to collect data from are depicted in Table 15, together with the associated companies, deviations (hard/soft) and means of identification (technical/human).

Table 15 Overview of sources to collect precursors.

data source	**company**	**deviations**		**means of identification**	
		hard	soft	technical	human
batch reports	A, B, C	X		X	X
reset reports	C	X		X	X
equipment stops	A, C	X		X	X
maintenance reports	A, B, C	X	X	X	X
shift reports	A, B, C	X	X		X
safety reports	A, B, C	X			X
company audits	A, B, C	X	X		X
observation rounds	A, B, C	X	X		X
interviews	A, B, C	X	X		X

From the deviations present in these sources, precursors are derived according the following criteria, taken from Chapter 5:

- The occurrence of three or more individual deviations from the transformation's theory-in-use, or espoused theory
- The deviations must all occur in the same input, output, or resource of a transformation.

- The deviations must be equal to each other on the lowest aggregation level as recorded in a company
- The deviations must occur after each other, with a time lapse in between them large enough for an organization to learn (to take action).

For each individual company, approximately 50 precursors were derived. For reasons of conciseness, only the top 20 precursors from each company are shown in Appendix B. This list of precursors is derived after prioritizing all precursors as discussed in the next Stage, see sub-Section 7.2.3. The top 20 precursors identified in company A, are shown in Table 16.

Table 16 Top 20 precursors identified from company A.

1	vacuum pump trip
2	leakage gasket
3	reactor valve leakage
4	pressure relief valve 1 defect
5	differences between written procedures & computer version
6	dust in packaging hall
7	clogged pipelines
8	conveyer belt error
9	valve 2 leakage
10	pump 1 trip
11	valve 3 leakage
12	release of vapours while adding to reactor
13	trip mixer
14	flow device defect
15	pump 2 leakage
16	steam kettle error
17	false alarms
18	blocked shredder
19	knifes blunt
20	pressure relief valve 2 trip

Please note that, some of the identified precursors (re-occurring deviations) are manifestly affected safety barriers. That is to say the precursor itself is a safety barrier and malfunctions repeatedly e.g. the pressure relief valve defect (number 4 in Table 16). Moreover, the precursor may be a process control measure (often tripping of a pressure relief (safety) valve). The presence of these kinds of precursors illustrates what is stated in Chapter 3, that if actors in the operational process don't perceive a deviation as possessing 'direct' safety related consequences, they permit these deviations to exist in the operational process.

7.2.3 Prioritize precursors (Stage 3)

The identified precursors will be sorted according their 'perceived risk', which means their likelihood and consequences. The likelihood can often be established from the data sources, although the possible consequences for safety are estimated and are therefore always subjective. The likelihood of the precursors is identified by establishing the aggregation level and relative frequency of the identified precursors, as discussed in Chapter 5. Table 17 shows an example of the retrieved likelihood from precursors identified in company A during a specified time period of a year.

Table 17 Example prioritisation of precursors on their likelihood.

	precursors	**aggregation level**	**frequency**
1	differences between written procedures & computer version	high	50/104
2	reactor valve leakage	high	68/365
3	false alarms	high	…/365
4	pressure relief valve 1 defect	low	50/365

In the first two columns of Table 17 the priority according to the likelihood and the precursors retrieved are shown. In the third column the aggregation level of the identified precursors is presented. In the fourth column the actual relative frequency is displayed. The first number in column four represents the total amount of deviations during the specified time period of a year and the second number represents the average frequency of use of the process/equipment/operator experiencing the deviation, during the year. For example 68/365 shows that in 68 times a leakage of the reactor valve was identified, which in turn is used daily (365 times a year). Note that the precursor sorted on the third position has no relative frequency. The reason it is placed third is that the aggregation level is identified as high (prioritized above low aggregation) and is sorted last, because the relative frequency can be higher or lower than the other two known relative frequencies. Moreover, the reason for the missing number is that it is often hard to establish the actual number of deviations from interviews. This missing number is estimated by a multi-disciplinary expert group, which established the consequences for each precursor.

The second step, of sorting the selected precursors according to their perceived safety related consequences, is achieved by studying safety reports and confronting the precursors with multi-disciplinary experts, i.e. experts from production, maintenance and safety. The expert group provided the identified precursors with perceived safety related consequences, by formulating 'possible' scenario's, from which the consequences could be obtained. From both the likelihood (see Table 17) and perceived consequences, the perceived risk class is obtained, as discussed in Chapter 5. Figure 42 shows the risk matrix for the precursors presented in Table 17.

		critical	**marginal**	**negligible**
high aggregation level	**high frequency**	reactor valve leakage	differences procedure & computer	
	low frequency		*false alarms*	
low aggregation level	**high frequency**	pressure relief valve 1 defect		
	low frequency			

Figure 42 The risk matrix for prioritising precursors.

Figure 42 shows vertically the (perceived) likelihood and horizontally the perceived consequences. The precursor 'false alarm,' is the precursor from which the likelihood was estimated by the expert group.
In Figure 42 the different grey-scales of the cells represent the different perceived risk classes, i.e. the precursors present in the four dark grey cells are classified first, precursors present in the four grey cells are classified second and precursors present in

the four light grey cells classified third. In this case the 'reactor valve leakage', the 'differences procedure & computer' and the 'pressure relief valve defect' are ordered as first risk class, the 'false alarms' are ordered second risk class. Because, the total list of ordered precursors is so long that analysing all precursors is impractical, only the top 20 precursors from each case study are analysed further. If it is not clear which precursors belong to the top 20 (for example if more than 20 precursors are indicated as belonging to the same risk class) then the expert group is consulted.
The precursors that are selected in all three companies are shown in Appendix B, containing the prioritized top 20 of each company. The next sub-Section will use these top 20 precursors to identify the corresponding ineffective control element(s) responsible for permitting these deviations to re-occur.

A remark, when discussing the identified precursors with the multi-disciplinary group of experts, led to the safety expert obtaining new insights into the operational process. Moreover, the maintenance and production experts obtained new insights by confronting them with a structured overview of the daily re-occurring deviations. Finally, the meetings enlarged the support and co-operation, helping the researcher to retrieve the relevant data for performing the analysis.
Please, also note that because the establishment of the 'perceived' risks remain subjective (expert group), it is still possible that safety relevant precursors are not taken into account for further analysis and possible accident trajectories are not seen.

7.2.4 Identify the ineffective control processes (Stage 4)

From the identified and prioritized precursors in the operational process, the corresponding control processes and control elements are identified, by taking the general hierarchical control level model as shown in Chapter 5, as a reference. The flow scheme, depicted in Figure 33 is used as a structured guideline to identify the initial ineffective control element. Starting with the given precursors on operational control level, the single and double loops are analysed for any ineffective control element. In case of any ineffective steering element (double loop analysis) this steering element is analysed in more detail by 'unfolding' it into a complete control loop on the next-higher hierarchical control level. In this way it is possible to identify the initial ineffective control element on any of the three hierarchical control levels.

An example of how this Stage works is given for the precursor 'reactor valve leakage' in company A. Graphically this analysis is shown in Appendix C.
The example concerns a re-occurring leakage of a valve, whose function is to add substances to a reactor (reactor valve leakage). In this example the precursor was identified in shift reports, maintenance reports and confirmed by interviews, so the precursor is *observed effectively*. Maintenance, together with a chief operator and a planner decided when and what to do with this leaking valve according to standard operating procedures, so the *judgement* is also *effective*. Subsequently, a repair order was sent from the maintenance department to a maintenance engineer who was to replace or repair the valve at a suitable time according to his order. This *intervention* is also identified as *effective*. From the flow scheme it can be seen that the *steering* element must be *ineffective* (see 1 in Appendix C). The steering element on the operational control level demands a quick repair or replacement of the valve and allows no additional resources to examine and eliminate the actual cause of the problem.

According to the theory presented in Chapter 5, the steering element on operational control level is in itself also a control loop but on the next-higher control level, i.e. observation, judgement, intervention on the tactical level. Therefore, these control elements on the tactical level are checked for their effectiveness. On the tactical control level, the process engineers are not on the site and are not aware of this precursor. Therefore the expertise needed to observe the precursor is missing and consequently, *observation on the tactical control level is ineffective*. However, by questioning the double loop it appeared that the engineers were removed from site due to a re-organization, so actually the steering on the tactical control level was responsible for the ineffective observation (see 2 in Appendix C).

The steering element on the tactical control level is in turn also a control loop, but on the next-higher strategic level, containing the control elements observation, judgement, intervention and steering. The steering element on strategic control level is not 'unfolded' any further, according to the theory presented in Chapter 5, because the strategic control level is the highest hierarchical level possible. On the strategic control level no overview of these problems was present. The strategic control level missed information from the tactical control level, causing the *observation* element on the strategic control level to be *ineffective* (see 3 in Appendix C).

So, summarising the situation, in order to cut costs the company's management relocated most of the process engineers to the headquarters, and thus inadvertently created problems at the operational level. The engineers were not kept informed of developing situations and were no longer able to observe and judge the structural problems effectively. The removal of these engineers from site led to an ineffective observation on the tactical control level, which again led to an ineffective steering on the operational control level, finally enabling a re-occurring leakage of the reactor valve.

The results for the top 20 precursors are obtained by using the flow scheme shown in Figure 33, taken from Chapter 5. All corresponding 'initial ineffective control elements' are obtained similarly as discussed in the example. The initial ineffective control elements from all cases are shown in Figure 43.

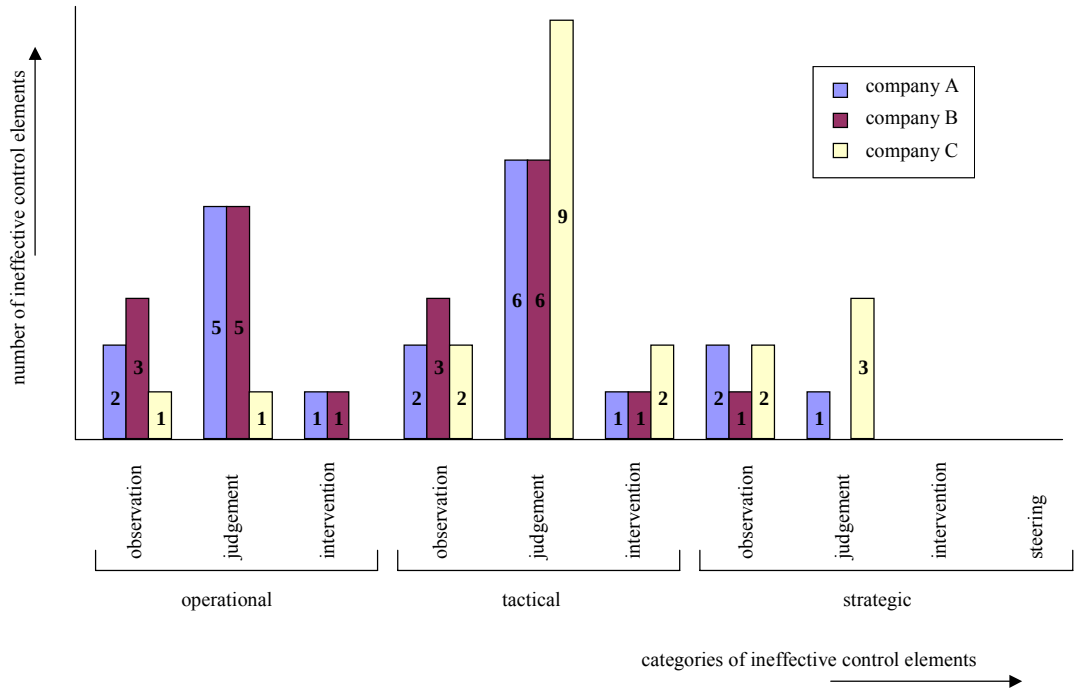


Figure 43 Overview of initial ineffective control elements of the three case studies.

The vertical axis in Figure 43 shows the number of ineffective control elements of all analysed precursors per company. The horizontal axis in Figure 43 shows the distribution of the number of initial ineffective control elements as obtained from the three case studies. In the example, which is graphically shown in Appendix C, the observation element on the strategic control level in company A was identified as being ineffective. This example is represented in Figure 43 by 1 in the ineffective observation on the strategic control level of the bar of company A. For company A, two of the analysed precursors were caused by an ineffective observation element on the strategic control level.

Because, for each of the three cases, 20 precursors are analysed, a comparison between the results of all three cases is possible. From the results of the analysis it appears that in all three cases, most precursors were enabled by the ineffective judgement element on the tactical control level. In companies A and B, the judgement element on the operational control level is the ineffective control element enabling the second most frequent precursors, while for company C the judgement element contains the most precursors on the strategic control level and appears to be a critical element at each control level for all three companies. Moreover, relatively more ineffective control elements are present on the higher (tactical and strategic) control levels in company C (18), than in company A (12) and B (11).

To test whether the results are also statistically significant, a chi-square test for contingency is applied to the results obtained. However, as the values retrieved from the cases shown in Figure 43 are very small, the total number of different hierarchical control levels in that company, were added to that company's total. This led to the categorized results as shown in Table 18, upon which the chi-square test for contingency is applied.

Table 18 Categorised results.

	operational			tactical			strategic				
Company	observation	judgement	intervention	observation	judgement	intervention	observation	judgement	intervention	steering	total
A	8			9			3				20
B	9			10			1				20
C	2			13			5				20
total:	19			32			9				60

The Chi-square test statistic is 8,01, giving a significance level of 0.09, implying that there is no statistically significant relation between the results of the different companies, as shown in figure 43. However, from a practical perspective the differences, if they are real, might be of importance, therefore the results and possible interpretations will be discussed in more detail in sub-Sections 7.2.7 and 7.3.

Please note, that according to the definitions stated in Chapter 4, the existence of a precursor implies an ineffective control element. While scrutinising the control processes it was often found that organizations consciously allowed precursors to exist for reasons of; cost-savings, non-safety impact, etc. and that they consider the process as being 'under control' implying 'no' ineffectiveness. In this thesis the definitions from Chapter 4 are maintained and consequently there must be an initial ineffective control element if a precursor is identified. Analysing the many precursors in the case studies revealed that the situations considered by organizations as being 'under control' actually contain an initial ineffectiveness, most often in one of the judgement elements on one of the hierarchical control levels.
Moreover, while executing this Stage deriving the organizational values and norms on the tactical and strategic control level is more difficult than deriving the organizational values and norms on the operational control level. On the operational control level standard operating procedures (SOPs), etc. are present. These procedures define very clearly how to handle most cases. However, on the tactical control level only broad company guidelines are present, which can often be interpreted in several different ways. Consequently, these interpretations are almost never written down, so they are difficult to retrieve. Finally, on the strategic control level, only mission statements or strategic reports are present, which are even broader and even more susceptible to various interpretations than the organizational values and norms on the tactical control level.

The following sub-Section will use the results as shown in Figure 43 to identify which conditions led to these ineffective control elements.

7.2.5 Identify the latent conditions (Stage 5)

The ineffective control elements are subsequently analysed in detail by retrieving the latent conditions leading to this ineffectiveness. To obtain this 'unfolding situation' as Dekker (Dekker, 2002) calls it, the four types of information flows, i.e. 'transformation,' 'history,' 'organizational values & norms,' 'external environment,'

and the two types of resources, i.e. ‘infrastructure’ and ‘human,’ currently present in the ineffective control element have to be retrieved (see Chapter 4.3.1 and 5.3.5). From the information flows and resources, it can be explained why the actions and assessments that were executed, made sense at that moment, and what information flows and/or resources contribute to causing the ineffective control element.

From the example given in the previous sub-Section, where the observation element on the strategic control level was identified as ineffective, the latent conditions will be retrieved by presenting the ‘unfolding situation.’
The latent condition of the *transformation* type was lacking, i.e. actual information from the transformation was not available on the strategic control level. The latent condition of the *history* type was also lacking, i.e. an overview of previous problems (deviations) in the transformation was also not available on the strategic control level. The latent condition of the *organizational values and norms* type is expressed as the strategic guidelines of the company, which were not causal conditions contributing to the ineffectiveness. The latent condition of the *external environment* type was dominantly present in the form of pressure from stockholders, demanding cost savings. The latent condition of the infrastructure type, was irrelevant in this situation, as was the latent condition of the human type, i.e. enough experts were present on the strategic control level.

So, summarising the situation, the company’s management on the strategic control level, had to decrease their costs under pressure from stockholders. Both, the current information and historical information from the transformation and its deviations were not available. These three types of latent conditions led to the ineffective observation on the strategic control level, i.e. the failure to realise the necessity that engineers with the necessary expertise should be present on site. So, the latent conditions that caused the ineffective observation element on the strategic control level, are ‘transformation,’ ‘history,’ and ‘external environment.’

Please note, that if the identified contributing types of latent conditions were resolved, i.e. sufficient information from the transformation process its history of deviations and no cost pressure from stockholders were present, the control element turns effective. However, this does not automatically imply that the corresponding precursor will be alleviated. It is still possible that a control element preceding the previous initial ineffective control element, is also ineffective.

The latent conditions from all initial ineffective control elements are derived in a similar way. The final results are shown in Figure 44. The data from which this figure has been derived is depicted in three tables, for company A, B and C successively, as shown and explained in Appendix D. By adding the numbers of each type of latent condition per company (see the last row of all three tables in Appendix D), the results graphically shown in Figure 44 are derived.

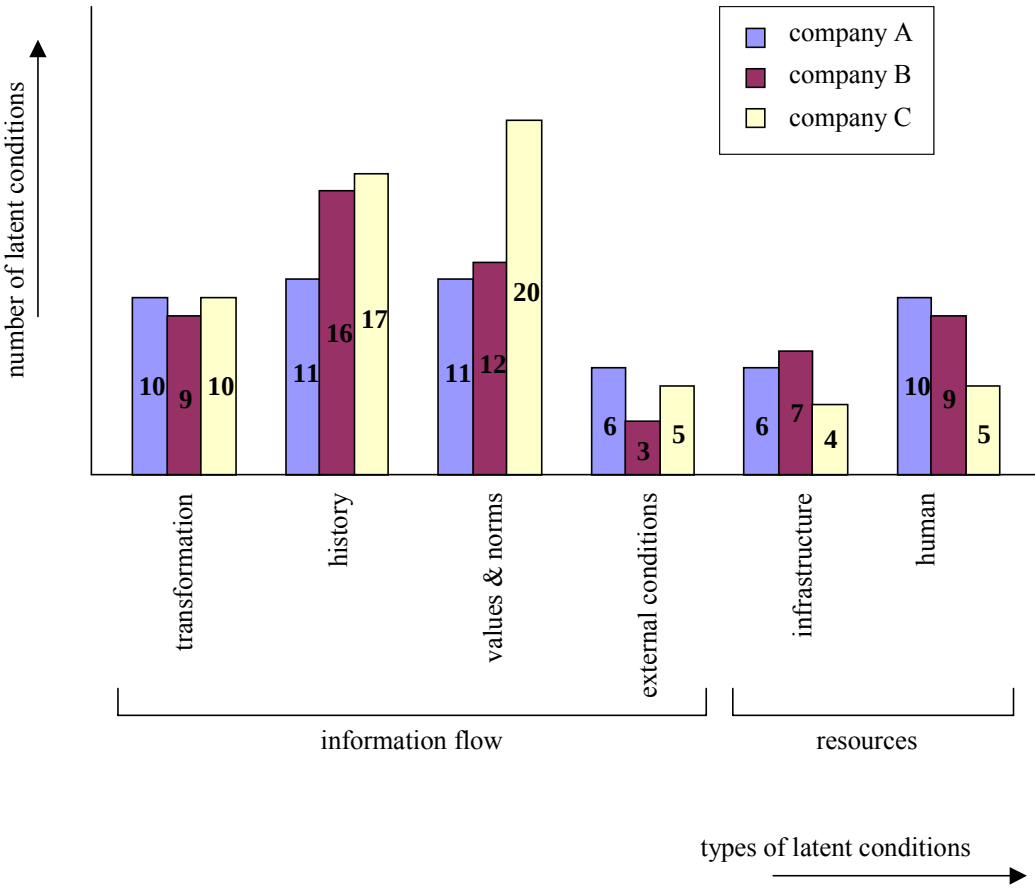


Figure 44 *The number of contributing latent conditions per company.*

The vertical axis in Figure 44 shows the numbers of contributing latent conditions for all ineffective control elements per company. The horizontal axis in Figure 44 shows the types of latent conditions. For example, 'transformation' is a latent condition type that contributes to the occurrence of ten out of the 20 precursors in company A (because the top 20 precursors were analysed for each company), and to nine out of the 20 in company B and for company C this type of latent condition contributes to the occurrence of ten out of the 20 precursors.

For each of the three cases 20 precursors were analysed, which makes a comparison possible between the results of all three cases. From the results as shown in Figure 44, it can be retrieved that the type 'values & norms' latent condition seems predominantly present in all companies, especially company C (20). Moreover, the high numbers of 'transformation' and 'history' type of latent conditions in all three companies is striking. As is, the small numbers of the 'human' type of latent condition for company C (5) compared to companies A (10) and B (9). To test if these differences are statistically significant, a chi-square test for contingency was applied to the obtained results. The test statistic was 7,89, implying that there was no statistically significant relation between the results of the different companies, as shown in Figure 44 (please note that each event can fall into six different types of latent conditions, which means that in this case a chi-square test was not entirely suitable). Though, from a practical perspective some differences might be of importance, therefore all results and possible interpretations are discussed in more detail in sub-Sections 7.2.7 and 7.3.

While executing this Stage it was noted that some precursors had been present for a long time. This implies that the ineffectiveness had occurred previously and was ongoing. This also means that the latent conditions from the past were used, which differ from the latent conditions currently present. However, when analysing, only the current latent conditions were taken into account, and the activities executed by the ineffective control element in the past were not adapted to the current situation (latent conditions). This difference, in past and present situation began to reveal, in part, the types of latent conditions which caused the ineffective control element.

The following sub-Section uses the results shown in Appendix D and Figure 44 to establish if safety barriers of the companies are affected.

7.2.6 Identify affected safety barriers (Stage 6)

As stated by Reason (Reason, 1997), the 'active failures' resulting in precursors and the 'latent conditions' cause the holes in the safety barriers, leading to an accident. The active failures result in precursors which were identified, while the latent conditions were roughly divided into 'information flows' and 'resources' types. The latent conditions explain why precursors still exist. They also explain the holes in the safety barriers. Subsequently, the identified types of latent conditions are used to check if they affect the identified safety barriers. The safety barriers can be affected; negatively, positively or not at all, by the identified types of latent conditions.

Taking the example, also used in the previous sub-Sections, it can be seen that the latent conditions, i.e. transformation, history and external environment, enable the re-occurring leak of a reactor valve. The leakage of hazardous substances has to be resolved in time by repairing or replacing the reactor valve by qualified maintenance personnel. The use of qualified maintenance personnel, with the knowledge and expertise to handle these situations is a safety barrier present around the transformation process. However, due to the high frequency of occurrence and the lack of qualified maintenance personnel, untrained operators sometimes have to replace the reactor valve themselves. The indicated latent conditions on the strategic control level, i.e. cost savings, lack of the current information and historical information from the transformation and its deviations, enabled an increase in unresolved problems, which subsequently caused an enormous maintenance backlog. Both, latent conditions and precursor affected a safety barrier (human) in this example, namely replacing the experienced maintenance personnel by untrained operators to solve the leakage of a reactor valve.

The affected safety barriers from all precursors and latent conditions are derived in a similar way. The final results are shown in Figure 45. The data from which this figure has been derived is depicted in three tables, for company A, B and C successively, as shown and explained in Appendix E. By totalling up the numbers of each functional category of safety barrier in each company (see the last row of all three tables in Appendix E), the results graphically shown in Figure 45 are derived.

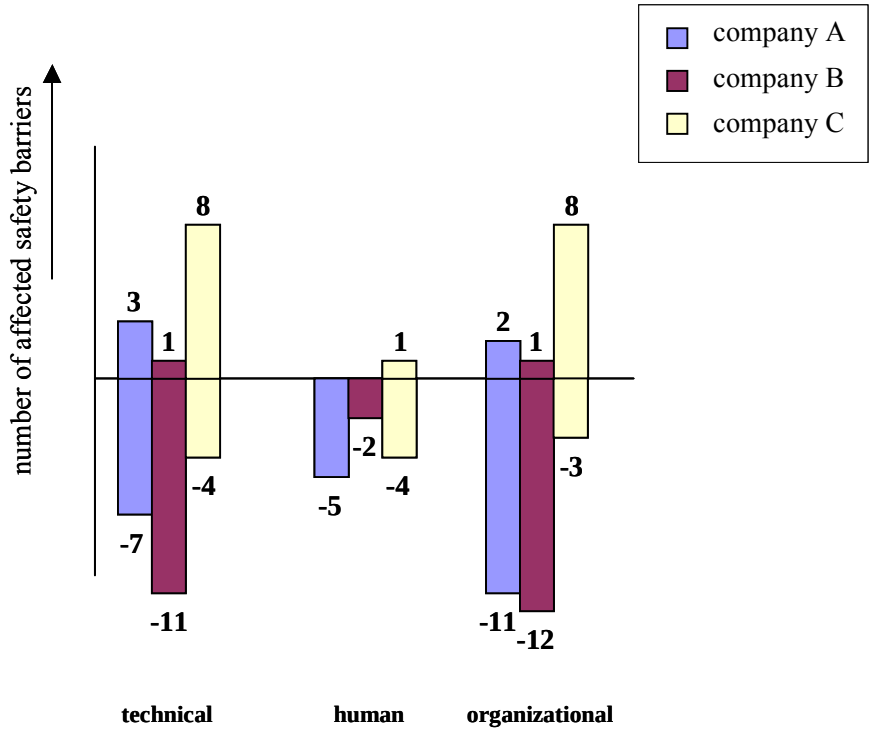


Figure 45 The number of affected safety barriers per company.

The vertical axis in Figure 45 shows, the numbers of positive or negative affected safety barriers per company. The horizontal axis in Figure 45, shows the functional categories of affected safety barriers, i.e. technical, human, organizational. From the first bar in Figure 45, it can be seen that the 'technical' functional category of affected safety barriers is affected three times in a positive way (adding an additional safety barrier) and seven times in a negative way (penetrating or removing a safety barrier) in company A.

From Appendix E, it can be seen that all precursors affect some safety barrier. From Figure 45 it can be seen that the affected safety barriers are not all affected in a negative way. In some cases, especially for company C (+17, see Figure 45), they are also affected positively (this means an additional safety barrier is implemented to relieve the consequences of an ineffective barrier). Especially the technical functional category of safety barriers and the organizational safety barriers are affected positively in company C (both +8, see Figure 45). The relatively small numbers of negatively affected 'technical' and 'organizational' functional safety barriers in company C (-4 and –3, respectively, see Figure 45) in comparison with the other two companies (–7 and –11 for company A and –11 and –12 for company B, see Figure 45) is striking. The differences between the three companies are so obvious that a test for statistical significance is unnecessary. The differences are both statistically and practically relevant and therefore all results and possible interpretations will be discussed in more detail in sub-Sections 7.2.7 and 7.3.

The following sub-Section will use these results, to derive some general conclusions for individual cases and mutually for all cases.

7.2.7 Derive conclusions (Stage 7)

From each case study the number of initial ineffective control elements and the 'latent conditions' leading to these ineffective control elements will be discussed. Moreover, the individual affected safety barriers will be combined, to find the possible alignment of affected safety barriers. These findings will indicate possible weaknesses of the current safety management system. Finally, all three case studies will be compared to derive some conclusions regarding both differences and similarities between the three cases.

In company A, most precursors occurred due to an ineffective judgement on the tactical control level, see Figure 43. These judgements were mainly ineffective because there were not enough *resource*s, no *historical information* of previous deviations and cost considerations (*organizational values & norms*), which could be taken into account (see Appendix D). In spite of these conditions, risks were considered from the perspective that one safety barrier can easily be ignored, because there are sufficient other safety barriers in place to prevent possible accidents from occurring. On the operational control level the judgement element was ineffective due to the presence of time constraints (*organizational values & norms*), shortage of *human resources* or *human resources* that were not trained properly. Safety was therefore not always considered and operators were not familiar with the risks of the different hazardous substances (see Appendix D).
When combining several precursors and latent conditions in company A, the following scenario, which is an alignment of several affected safety barriers, could be identified:

A mismatch between operator procedures and the automatic control system of the reactor (see also Table 17) was the first 'active failure' identified in this scenario. This precursor was still present mainly due to a shortage of people. Literally it was said that 'the pressure relief valve would open if the wrong value was inserted into the reactor's control system.' The second precursor was the failure of the pressure relief valve (see also Table 17), which was not known to the responsible person who decided to ignore the difference between procedures and control system. The pressure relief valve failed, because resins stuck in the valve after it was used for the first time. Consequently the second time the valve was opened it was at a much higher pressure due to the build up of resins in the valve. If this second precursor had not been observed in time by 'damp on the pipes situated above the pressure relief valve' or by the alarms in the control room a possible accident scenario existed. This was especially dangerous as the alarms in the control room are often ignored because of the high incidence of false alarms (see also Table 17), which was the third precursor present.

The scenario sketched above occurred mainly because the individual actors on the different control levels were 'forced' by the 'latent conditions' to let precursors exist. However, due to the missing overview of precursors and affected safety barriers, a precursor remained in the operational process and suddenly enabled a possible high risk scenario.
Mainly by cost constraints, lack of historical information about deviations and by lack of experienced personnel, safety was ignored from several individual or 'local' standpoints. This caused the main weakness of the SMS: a lack of overview of

deviations, of their underlying latent conditions and of their influences on the present safety barriers in the operational process.

In company B, most precursors also occurred due to an ineffective judgement on the tactical control level, see Figure 43. These judgements were mainly ineffective because often there was a lack of information, regarding the *transformation* process and *historical information* of previous deviations. Moreover, cost and product quality considerations (*organizational values & norms*) had to be taken into account. Safety was not always considered, and even when it was, it was considered in a similar way to company A, i.e. one safety barrier can easily be ignored, because there are enough other safety barriers in place to prevent an accident. On the operational control level the judgement element was ineffective due to the lack of *historical information* of previous deviations and lack of properly trained *human resources*. Other factors like product quality and quantity were therefore often considered instead of safety. When combining several precursors and latent conditions in company B, the following scenario, which is an alignment of several affected safety barriers, could be identified:

An old drying chamber often leaked air, preventing the chamber from getting the required vacuum (see Appendix B). This precursor was judged by the tactical control level to be unimportant. The cost of a new chamber and no other problems reported allowed the precursor to remain. Moreover, the temperature in the chamber was often set higher than required due to a lack of information of the transformation process. If the 'fault' was observed operators recovered the situation according to procedures. However, the fault was not reported to the tactical control level in spite of repeated re-occurrences. Once the high temperature setting caused a hazardous powder to melt completely. This deviation was observed, but did not result in any further action to fix the underlying holes in the safety barriers. The company's comments were: 'there was only a product quality problem, which was solved by reprocessing, so what's the problem!' Next time, the precursors could result in an explosion instead of the near miss which was not properly identified as such!

The conclusions for company B are similar to company A in that safety was ignored from several individual or 'local' standpoints, mainly by product quality and cost constraints, lack of historical information about deviations and lack of experienced people. This contributes to the main weakness of the safety management system, which are a lack of overview of: deviations, their underlying latent conditions and of their influences on the safety barriers in the operational process.

In company C, almost half of all precursors occurred through ineffective judgement on the tactical control level. These judgements were mainly ineffective owing to a lack of *historical information* from previous deviations and to time constraints (*organizational values and norms*). However, all deviations were considered thoroughly for consequences impacting on safety. If any deviation might affect safety, additional measures were implemented. Alas, on the strategic control level, judgement was ineffective due to cost considerations (*organizational values and norms*), lack of information about the *transformation processes*, pressure from shareholders (*external environment*) and the lack of *historical* information of previous deviations. In spite of these conditions, safety was almost always taken into account. Although on one occasion a safety barrier was found to have been penetrated, because a reported

problem had not been addressed in a timely manner, i.e. the deviation had been observed and judged, but no intervention had been executed.

For company C, the main weakness of the safety management system is the implementation of the additional measures to enhance the safety barriers. The time lapse between observation and actual intervention is sometimes very long. No examples of affected safety barriers lining up could be retrieved, because most analysed precursors are immediately alleviated, preventing any escalation.

From the four case studies several suggestions for improvement were made, according to the identified latent conditions and specific precursors. However, the implementation and validation of these suggestions was not performed and are recognised as steps still missing in the final validation of the 7-stage protocol. The analysis was performed in close co-operation with company employees and the remedies implemented were derived together with the employees. As Schein (Schein, 1999) clearly states, the success of the remedies depends heavily upon the involvement of the company employees, because they know what will work and are ultimately responsible for the implemented remedy and its consequences.

Statistically no significant differences could be identified between companies A, B, and C between the distributions of ineffective control elements and latent conditions. However, from executing the 7-stages, the differences between the three companies observed from practice, match the apparently insignificant differences present in the results. Therefore, these differences, although statistically insignificant, are discussed.
In sub-Section 7.2.4, it was seen that in company C many more ineffective control elements were present on the hierarchical higher control levels, when compared with the other two companies. A possible interpretation for the differences from practical experiences is that in company C the plant managers are held directly responsible for any accident in their part of the company, while responsibilities in companies A and B are kept closer to the operational level.
In sub-Section 7.2.5, it was seen that in company C a higher number of latent conditions of the organizational values and norms type was present (20, see figure 44), compared to companies A (11) and B (12). A possible interpretation for the differences from practical experiences is that in company C severe risk constraints are present on all hierarchical control levels, while in companies A and B risk is not a constraint, but something which has to be taken into account never-the-less. The organizational values and norms represent all sorts of constraints, i.e. constraints with respect to time, product quality, etc. but also with respect to risks. It seems that these constraints, which can be seen as the ‘company’s culture,’ has a great influence on the normal way of working in a company and largely determines the effectiveness of an SMS. For a large part, the difference between the distributions of affected safety barriers, is based on these aforementioned issues. Company C compared to companies A and B, responds to many precursors by alleviating the ‘problem’ or adding additional safety barriers, preventing an alignment of different effected safety barriers.

In the following Section the results and conclusions of the three case studies will be discussed in more detail, especially in regard to safety.

7.3 A reflection on the results of the analysis

From the analysis of the three case studies, by using the developed protocol from Chapter 5, it was concluded that there are still severe safety risks present in the chemical process industry, that have a high potential for escalating into an accident. These 'obvious' risks, as retrieved from the analysis, are still present in spite of all the (legally) required and (company) implemented safety indicators and safety measures. The previous analysis revealed that an overview of; deviations, their underlying latent conditions and of their influences on the safety barriers in the operational process is often missing. This conclusion is not derived directly from the analysis' results but indirectly from executing the analysis. It is the execution of the analysis, which provides the way to interpret the results retrieved from the analysis. The overall conclusion can be derived by executing the protocol, which creates a specific context from which the results (the graphs as shown in the previous Section) can be explained in terms of how the SMS works, or not. Note that the results from each Stage of the 7-stage protocol are mutually dependent, and by placing them in the practical context it can be concluded where the weaknesses lay in the SMS, as will be discussed in the next sub-Section.

7.3.1 Safety management systems

In all three case studies, a SMS is in place, which starts with stating the commitment of top-management and their goal to prevent all accidents on their sites. All three companies have: inspections, audits, meetings, training and assessments in place. Moreover, all three companies perform several risk assessments for new products and new production processes. However, during the actual production, the SMS concentrates on situations which could cause direct damage to people, e.g. a loose pavement stone, a low ceiling, no handrail, etc. The operational re-occurring deviations (precursors) collected in the previous analysis, are often not known to the SMS. The SMS, often doesn't know what is going on in daily operation and the meeting of multi-disciplinary experts to review the identified precursors, revealed deviations which safety experts did not know about. In the few opportunities in which safety personnel are involved in the daily operation, the emphasis is especially on those situations in which possible 'slips and trips' occur. This lack of overview, leads to situations in which decisions are made possibly affecting the existing safety barriers. For example in company B, performing a safety review depends purely on the department initiating an intervention in the operational process, and only if the intervention exceeds a specified amount of money, do safety experts have to be consulted. If safety is considered, several unco-ordinated decisions are made on different control levels, with the potential for different departments each to accept a gap in a single safety barrier. However, this lack of co-ordination raises the possibility that the gap aligned with others could permit a precursor to penetrate the different safety barriers and result in an accident.

To prevent a possible alignment of holes in safety barriers, company C has as opposed to companies A and B, severe risk constraints present, which strictly require additional safety measures to be implemented when holes are identified in a safety barrier, as illustrated by the number of positively affected safety barriers in the other two companies. Moreover, in company C safety critical decisions are made on the highest level, creating an overview and also commitment of all employees to identify, report and reduce risks as soon and as effectively as possible.

How this developed 7-stage protocol differs in respect to existing methods identifying risks is shown in the next sub-Section.

7.3.2 Additional value

When looking at the results of the applied 7-stage protocol, the advantages of this method, compared to existing methods become apparent. To compare three existing pro-active methods identifying safety risks, as discussed in Chapter 3, with the developed 7-stage protocol, the differences between the three existing methods and the 7-stage method are briefly discussed.

The main differences between the developed 7-stage protocol and currently available methods, like MORT, TRIPOD, and PRISMA is the use of deviations/problems of different aspects in the operational process, not necessarily related to safety, as perceived by the actors. In this way a lot of additional safety relevant information is retrieved, as are shortcomings which enable accidents to occur (Chapter 3). Moreover, as the whole analysis is based on identifying ineffective control processes, a link between causes, problems and remedies in the normal way of working (which is represented by control processes) is obviously present in the 7-stage method. The clear causal relationships between observable facts in the operational process, the normal way of working, the 'vague' latent conditions, and the observable degradation of safety barriers causing the opportunity for an accident, is the major advantage of the 7-stage protocol compared to existing methods. By explicitly showing how an accident develops, safety risks can be specifically pinpointed in an organization, which illustrates the advantage of the 7-stage protocol over existing methods.
Expert knowledge of the actors, in the organization at which the protocol is applied, is needed. They have to 'iteratively' check the collected data and establish the consequences for the retrieved precursors. For the researcher himself, however, no specific training or skills are required to apply the 7-stages, which are laid down in a structured protocol.
Further benefits of the 7-stage protocol are the ability to derive ranked general conclusions from the different types of latent conditions. Correspondingly, by using operational data as a basis, the detailed cause-effect relationship between operational deviations and eventual (root)causes is obtained.
A limitation of the developed 7-stage protocol is the substantial amount of time needed to apply the method. Moreover, the 7-stage protocol is applied only in four cases and the recommendations obtained from the analysis and implemented in practice are not yet evaluated, which means that exact value of this method in practice is not yet precisely known. Though, in Table 19, the four methods are compared on the requirements derived in Chapter 3.

Table 19 Comparison of different risk analysis methods.

	usage of indirect safety related operational deviations	general conclusions	detailed cause-effect relationship	feasibility	reliability	limited resources	rank results	clear link between risk reduction and operational benefit
MORT	-	+	+	-	-	-	+/-	+/-
TRIPOD	-	+	-	-	+	+	+	-
PRISMA	+/-	+	+	+	+	+/-	+	+/-
7-stage	+	+	+	+	+	+/-	+	+

The following Chapter will use the results and conclusions from the analysis performed in this Chapter, to derive some final conclusions and recommendations. Moreover, the posed research questions from Chapter 1 will be addressed and some open problems will be stated, to improve the current way in which companies manage safety.

Chapter 8

CONCLUSIONS, DISCUSSION AND OPEN PROBLEMS

In this concluding Chapter the problems identified from practice and literature and the research questions derived from these observations will be reviewed. Subsequently, the results from the previous Chapters will be used to obtain the answers to these research questions. Moreover, a reflection on the results and answers will be stated. Finally, some opportunities for future research will be presented.

8.1 Conclusions

This thesis deals with the problem of how to find ways of preventing accidents, by observing, measuring and analysing pre-warning signs that an accident is imminent in the operational process of high risk companies. Therefore, it is necessary to discover pro-active 'safety indicators' that can measure safety in a high risk industry, which in this research is limited to those companies in the Dutch chemical process industry.
To define the problem, current literature and practice were studied in Chapter 1. This revealed that from the many studies performed in the past century, a great deal of knowledge about safety is available today. The increasing scope and increasing external environment of safety show that it is not only the technical and human elements that cause accidents. Moreover, in many cases, the entire socio-technical system and its interactions with the external environment 'push' a company towards an accident. Despite the many preventive efforts, accidents still happen and finding effective indicators for safety risks is still difficult. The visibility of deviations (active failures) leading to an accident is often very low. Measuring damage is too late and cannot be used as an indicator to point out future damage. Measuring elements in an organization, raises the questions of which elements to measure and how to measure them. Additionally there is the problem of how to include influences from outside the organization, which play an ever more important role. Therefore, how to find factors or signs that effectively and unambiguously indicate a safety risk in an organization, is a major problem in safety research and practice. That is why indicators or precursors are needed which are clear and specific, and from which the causes of accidents can be derived. This resulted into the following four research questions:

1. Is it possible to identify precursors of accidents in an operational process?
2. Is it possible to retrieve the causal factors of such precursors, which can explain accidents?
3. Why do accidents still occur despite the pre-warning presence of such precursors?
4. How can the pro-active identification of accidents be improved, by using precursors?

In the next sub-Sections these research questions will be answered, using the results and conclusions from previous Chapters.

8.1.1 Question 1: Is it possible to identify precursors of accidents in an operational process?

The answer to the question is that in the vast majority of all accidents, re-occurring deviations, which were defined as precursors, are present. That a variety of events were present prior to accidents, was stated by Heinrich (Heinrich, 1931). He combined the common cause model and the descriptive iceberg model, stating that prior to an accident, increased numbers of near misses, errors and recoveries are present. Subsequently, Turner (Turner, 1978) identified a so-called 'incubation' period prior to accidents, in which all sorts of events occur unnoticed or are misinterpreted. However, neither study indicates types, or categories of events that can act as precursors of accidents.

From a study into recent accidents in the chemical process industry, it appeared that a specific class of events was dominantly present prior to current accidents (Chapter 3). This specific class of events consists of re-occurring deviations in the operational process which are present in the accident trajectory, which were defined as precursors (Chapters 3 and 4). The presence of these precursors prior to accidents was subsequently verified in the analysis of other accidents (Chapters 5, 6 and 7). However, the reverse logic that precursors indicate that an accident is imminent cannot be so easily proven. Therefore, some additional criteria had to reinforce the definition of a precursor, as were stated in Chapter 5. Subsequently, with these additional criteria, precursors were used to successfully identify high safety risks (Chapter 7). Thus precursors of accidents were identified and defined. However, in some rare cases, no precursors could be identified prior to accidents and these were classed as unforeseen accidents because they were often caused by exceptional conditions from outside the organization such as criminal damage, e.g. shooting with a rifle at a pipeline, setting fire to a storage depot, etc.

8.1.2 Question 2: Is it possible to retrieve the causal factors of such precursors, which can explain accidents?

The answer to this question is that from precursors, causal factors could be derived in terms of latent conditions, which explain the precursors and allow the corresponding accidents. Precursors are re-occurring deviations, which are indicators of an ineffective control process in the organization (Chapter 4). In an organization the control processes and their ineffectiveness must be identified to show how the normal way of working leads to a possible safety risk. Therefore, the controlling processes in practice are projected on a theoretical control model, which consist of four control elements on three hierarchical control levels (Chapters 4 and 5). In this way the initial ineffective control element can be identified, and is considered to be the 'origin' which initially enabled the precursor to occur (Chapter 5). According to Dekker (Dekker, 2002), the initial ineffective control element is caused by the presence of several conditions creating the ineffectiveness. The conditions which actually cause the initial ineffective control element, are called the latent conditions, as stated by Reason (Reason, 1997) (Chapter 4). By developing a 7-stage protocol of the foregoing reasoning and applying it to several case studies, the latent conditions (causal factors), which cause the presence of precursors have been derived (Chapters 5 and 7).

8.1.3 Question 3: Why do accidents still occur despite the pre-warning presence of precursors?

The answer to this question is that the actors may not be aware of the precursors or recognise them as such. Moreover, often actors in an organization permit certain precursors to exist without having a complete overview of: precursors, their underlying latent conditions and the safety barriers they can affect. Latent conditions cause initial ineffective control elements, which enable precursors to occur (Chapters 4 and 5). These precursors and the corresponding latent conditions may affect the safety barriers in an organization, in a positive way (adding an additional safety barrier) and/or a negative way (creating a hole in a safety barrier) (Chapter 4). If several safety barriers are affected in a negative way and the holes in the safety barriers 'line up,' precursors are allowed to escalate into a possible accident, Reason (Reason, 1997). Why the accidents happened in each of the case studies could be explained by: structurally identifying precursors, latent conditions and affected safety barriers, using the developed 7-stage protocol (Chapters 5 and 7). Moreover, the use of this protocol identified that precursors are often accepted because of a lack of overview of the underlying latent conditions and possible effects on the safety barriers.

8.1.4 Question 4: How can the pro-active identification of accidents be improved, by using precursors?

The answer to this question is that possible accident scenario's can be derived by identifying precursors, retrieving the corresponding latent conditions and negatively affected safety barriers. By retrieving these factors using the developed 7-stage protocol, the overview is retrieved to pro-actively identify possible weak spots. Acceptance of the 'wrong precursors' if a cause-effect relationship is present, can be prevented in this way. Companies can respond to the identified accident scenario's, by interrupting the cause-effect relationships, as shown in Figure 26 of Chapter 4 in several different ways. In four case studies, high risk scenarios have been pro-actively derived with help of the 7-stage protocol (Chapters 5 and 7).

8.1.5 General conclusion

Current safety indicators do not comprehensively signal all possible accidents (Chapter 3), therefore the developed 7-stage protocol must be used to pro-actively indicate precursors and the underlying root causes like the latent conditions, which together affect the safety barriers and enable accidents to occur. The construct validity and reliability of the research findings is ensured by a combination of different data collection methods, the use of different researchers using the same analysis method and the use of several independent experts to verify and discuss results. Moreover, by selecting the three case studies by applying replication logic, these findings can be generalized to a much larger neighbourhood, e.g. other countries and other high risk organizations.

8.2 Discussion and reflection

In this Section the research and conclusions as stated in the previous Section will be discussed, showing the validity of the research and conclusions. Moreover, some personal observations while performing this research are discussed.

8.2.1 Reflection on the research and conclusions

In the following sub-Section some concepts from the research are discussed. The answer to the first question states that precursors of accident can be defined as re-occurring deviations in the operational process. The opposite reasoning that precursors always mean that an accident is imminent is not that evident. First because precursors of an accident must be able to inflict harm and secondly the reasonable probability to actually inflict harm must be present before an accident can actually happen. Therefore, only precursors that satisfy these conditions are considered by prioritizing precursors to their risks, as done in Stage 3 of the 7-stage protocol (Chapter 5). So not all 'precursors' indicate an imminent accident and each need to be prioritized against their risk. Moreover, in practice it is difficult to identify precursors from the large amount of unstructured and incomplete data present. In spite of the precursor criteria, it appears that events classified as precursors, sometimes still have to be seen as individual deviations in the operational process. Establishing the 're-occurrence' of an event is difficult, which means that events can be erroneously classified as precursors and correspondingly events that are precursors can be classified as non-precursors. However, this problem is answered by using multiple sources for data collection and confronting the data with actors in the operational process (operators, managers, engineers). Additionally by 'iteratively' updating the precursor-data, the final collection of precursors will give a fair representation of the daily re-occurring deviations in the operational process, which provides a more validated set of data. Finally, it has to be considered that when the latent conditions of an initial ineffective control element are resolved, it does not automatically mean that the corresponding precursor will disappear. It is still possible that another control element preceding the initial ineffective control element is also ineffective.

8.2.2 Personal observations

By executing the 7-stage protocol in practice, several personal observations were made that could not be validated from the analysis results. Some observations were made as to why actors accepted precursors and why the overview is so difficult to retrieve.

Observed precursors were judged and often accepted in the past, even though the conditions in the operational process and the latent conditions present when judging changed over time. So in spite of these changing conditions the judgements were never re-evaluated which allowed 'high-risk events' to appear in the operational process. The results from the 7-stage protocol partially verify this observation, by showing high numbers of 'history' and 'transformation' types of latent conditions, which implies a lack of information about the current operational process (Chapters 5 and 7).

It was noted that in some organization an increase in the number of safety barriers increases the willingness of actors in these organization to accept precursors and to

accept ‘holes’ in these safety barriers. Often the ‘individual’ actors do not have an overview of other ‘holes’ in different safety barriers, which can result into an alignment of holes throughout all safety barriers. So, although additional safety barriers look good from a safety point of view it was observed that with additional barriers, additional holes are allowed to evolve which dissolves and even negates the safety improvement.

Finally, precursors are accepted by different actors on different control levels, each allowing a single gap in different safety barriers. In this way many gaps in different safety barriers are allowed to evolve. This enables precursors to penetrate the different safety barriers through an alignment of these gaps which can result in an accident. The results obtained from applying the 7-stage protocol verify this observation partly by showing high numbers of accepted precursors (high numbers of ineffective judgements on all three hierarchical control levels), causing high numbers of affected safety barriers (Chapters 5 and 7).

8.3 Some open problems

It is acknowledged that identifying events in the operational process that signal a possible accident is imminent, is very difficult. The fundamental problem is that these ‘active failures’ as Reason (Reason, 1997) called them, emerge in innumerable ways. Never-the-less, from additional research into the FACTS database (FACTS, 2002), only a limited collection of events seemed to be present prior to the vast majority of accidents. Like Kletz (Kletz, 1993) stated, some events keep re-occurring and keep escalating into accidents, over and over again. It must be stressed that only identifying these events is not enough, the final aim should address the underlying root-causes, to actually prevent the accidents from occurring. Although the direct measurement of root causes seems the preferred option this in isolation looses the qualitative insight into how events develop into actual accidents and part of the warning function that events have in organizations is also lost, van der Schaaf (Schaaf van der, 1991). Therefore, searching for precursors that signal possible accidents are imminent, is worthy of further study.

An interesting problem for further research is the observed and partly verified situation, where organizations accept precursors, although they do not monitor this precursor over time when several conditions, affecting these precursors, change. The deviations are so commonplace that they are accepted as being part of the normal way of working, without considering the possible consequences. Research into the causal factors of this mechanism and ways to overcome this problem seem promising to reduce risks and possible accidents.

Another problem, also identified by Rasmussen (Rasmussen et al., 2000), is that individual actors in the control processes cannot see the effects of their actions in respect to the total picture. Subsequently, acceptance by different actors on different control levels, allows more gaps in different safety barriers. Together, this enables precursors to penetrate the different safety barriers through an alignment of these gaps resulting in an accident scenario. Further research is needed to retrieve insights into how the overview of the total picture and the different effects of the actions of individual actors can be retrieved in theory and practice.

Finally, an interesting problem for further research is the suspected relationship between the amount of safety barriers around a potential hazard and the willingness of actors in organizations to allow penetration of some of these safety barriers. The risk homeostasis theory, Wilde (Wilde, 1982), can provide some answers by showing that individuals posses a target risk that he or she is willing to accept. Whenever there is a discrepancy between this target risk and the risk perceived, adjustment actions will be performed aimed at reducing this discrepancy. This means that the implementation of safety barriers above a certain target risk is of no avail and can even work counter-actively. So that when additional safety barriers are created, additional 'holes' are accepted in the barriers which in turn increase the probability of alignment, thus it can be seen that additional safety barriers do not directly increase the safety in an organization, and may actually decrease the 'total' safety in an organization.

A lot of research has to be performed to totally understanding why accidents can still happen in spite of the amount of research performed nowadays. The research presented in this thesis is especially focused on this subject and although accidents will always remain, it helps both practitioners and researchers to have a greater understanding of accident precursors.

REFERENCES

Adams J., 1995. *Risk*, UCL Press, London.

Aken van J.E., 1994. De bedrijfskunde als Ontwerpwetenschap: de regulatieve en de reflectieve cyclus, *Bedrijfskunde 66 (in Dutch)*, pp. 16-22.

Amelsvoort van P., 1989. Een model voor de moderne besturingsstructuur volgens de sociotechnische theorie, *Gedrag en Organisatie Vol. 2 No. 4/5 (in Dutch)*, pp. 253-267.

American Institute of Chemical Engineers (AIChE), 1981. *DOW's Fire & Explosion Index: Hazard classification guide*, New York.

Argyris C., Schön D.A., 1996. *Organizational learning II; theory, method, and practice*, Addison-Wesley, Amsterdam.

Ashby W.R., 1956. *An introduction to Cybernetics*, Methuen, London.

Baram M., 1998. Process Safety Management and the Implications of Organizational Change, in: Hale A., et al. (Eds.), *Safety Management, the challenge of change*, Pergamon, Oxford, pp. 191-205.

Bateson G., 1972. *Steps to an ecology of mind*, Ballantine books, New York.

Bayutt P., 2003. Major Hazards Analysis: An improved method for Process Hazard Analysis, *Process Safety Progress Vol. 22 (1)*, pp. 21-26.

Bechhofer F., 1974. *Current approaches to empirical research: some central ideas*, Routledge, London.

Bertalanffy von L., 1968. *General System Theory*, Braziller, New York.

Bickman L., Rog D.J., 1998. *Handbook of Applied Social Research Methods*, Sage Publications, London.

Boreham N.C., Shea C.E., Mackway-Jones K., 2000. Clinical risk and collective competence in the hospital emergency department in the UK, *Social Science & Medicine 51*, pp. 83-91.

Bourrier M., 1998. Elements for designing a self-correcting organization: examples from the nuclear power plants, in: Hale A., Baram M., (Eds.). *Safety Management, the challenge of organizational change*, Pergamon, Oxford, pp. 133-146.

Brombacher A.C., Graef M.R., 2001. Anticiperen op trends, in Graef M.R. (ed.), *Betrouwbaarheid van technische systemen (in Dutch)*, STT 64, Den Haag, pp. 392-417.

BRZO, 1999. *Besluit Risico's Zware Ongevallen (in Dutch)*, Staatsblad van het Koninkrijk der Nederlanden 1999 234.

Busby J.S., Hughes E.J., 2003. Projects, pathogens and incubation periods, *International journal of project management*, in press.

Checkland P., 1991. *Systems thinking, systems practice*, John Wiley & Sons, Chichester.

Christensen-Szalanski J.J.J., Willham C.F., 1991. The hindsight bias: A meta-analysis, *Organizational behavior and human decision processes 48*, pp. 147-168.

Clarke S., 1997. Violations as a Source of Project Risk, *The international journal of Project and Business Risk Management, 1(2)*, pp. 155-167.

Croom S., 2001. *Topic Issues and Methodological Concerns for Operations Management Research*, EDEN Seminars, Brussels.

Cutts G., 1991. *Structured Systems Analysis and Design Technology*, Blackwell scientific publications. Oxford.

Davenport T.H., Short J.E., 1990. The New Engineering: Information Technology and Business Process Redesign, *Sloan Management Review, 31(4)*, pp. 11-27.
Davoudian K., Wu J-S., Apostolakis G., 1994. The work process analysis model (WPAM), *Reliability Engineering & System Safety 45*, pp. 107-125.
Dekker S., 2002. *The field guide to human error investigations*, 1st edition, Ashgate Publ., Aldershot.
Deming W.E., 1986. *Out of the crisis*, Massachusetts Institute of Technology, Centre for advanced Engineering study, Cambridge.
FACTS, 2002. *Failure and ACcidents Technical information System*, Department of Industrial Safety TNO-MEP, Apeldoorn, The Netherlands.
Falster P., 1997. Describing Production Situations, in: Wortmann et al. (Eds.), *Customer Driven Manufacturing*, Chapmann & Hall, London.
Fryer D.M., Harvey J.F., 1998. *High pressure Vessels*, Chapman & Hall, London.
Galbraith J.R., 1977. *Organizational Design*, Addison-Wesley, Reading, MA.
Gill J., Johnson P., 1991. *Research Methods for Managers*, Paul Chapman Publishing, London.
Groeneweg J., 1992. *Controlling the controllable: the management of safety*, DSWO Press, Leiden.
Groeneweg J., 1998. *Controlling the controllable: the management of safety*, 4th edition, DSWO Press, Leiden.
Groot de A.D., 1994. *Methodologie: Grondslagen van het onderzoek en denken in de gedragswetenschappen (in Dutch)*, Koniklijke Bibliotheek, Den Haag.
Guldenmund F.W., 2000. The nature of safety culture: a review of theory and research, *Safety Science 34*, pp. 215-257.
Haas de M., 2000. *Strategic Dialogue: In Search of Goal Coherence*, thesis Beta, Eindhoven.
Hale A.R., Heming B.H.J., Carthey J., Kirwan B., 1997. Modelling of safety management systems, *Safety Science Vol. 26 No. 1/2*, pp. 121-140.
Hale A., Baram M., Hovden J., 1998. Perspectives on safety management and change, in: Hale A., et al., (Eds.), *Safety Management, the challenge of organizational change*, Pergamon, Oxford, pp. 1-15.
Hale A.R., Guldenmund F., Bellamy L., Wilson C., 1999. IRMA: Integrated Risk Management Audit for major hazard sites, in: Schueller et al. (Eds.), *Safety & Reliability*, Balkema, Rotterdam, pp. 1315-1320.
Hale A., Guldenmund F., Goossens L., Bellamy L., 2000. Focused auditing of major hazard management systems, *Proceedings of the 18th ESReDA*, Karlstad.
Health and Safety Executive (HSE), 1995. *Out of control*, HSE books, United Kingdom.
Heinrich H.W., 1931. *Industrial Accident Prevention,* McGraw Hill, New York.
Hopkins, A., 2000. *Lessons from Longford: The Esso Gas Plant Explosion*, CCH, Sydney.
HSE, 1995. *Out of control (why control systems go wrong and how to prevent failure)*, HSE books.
HSE, 2003. *Health and Safety statistics highlights 2002/2003*, http:// www.hse.gov.uk /statistics/overall/hssh0203.pdf.
Hudson P.T.W., Wagenaar W.A., Reason J.T., Groeneweg J., Meeren van der R.W., Visser J.P., 1991. Enhancing safety in drilling: Implementing TRIPOD in a desert drilling operation. *SPE paper 23248 First International Conference on Health, Safety, and Evironment*, The Hague.

IEC 61508, 2000. *Functional Safety of electronical/electronic/programmable electronic safety-related systems*, Bureau Central de la Commission Electrotechnique International, Genève.

Jacobs R., Haber S., 1994. Organizational processes and nuclear power plant safety, *Reliability Engineering & System Safety 45*, pp. 75-83.

Johnson W.G., 1980. *MORT: Safety Assurance System*, National Safety Council and Marcel Dekker Inc., New York.

Kanse L., 2004. *Recovery uncovered: How people in the chemical process industry recover from failures*, PhD thesis Technische Universiteit Einhoven, Eindhoven.

Kaplan S., 1981. On the quantitative definition of risk, *Risk Analysis Vol. 1 (1)*, pp. 11-27.

Kennedy R., Kirwan B., 1998. Development of a Hazard and Operability-based method for identifying safety management vulnerabilities in high risk systems, *Safety Science 30*, pp. 249-274.

Keuning D., 1991. *Organiseren en leidinggeven*, 3th edition, Stenfert Kroese, Leiden.

Khan F.I., Abbasi S.A., 1999. Major accidents in process industries and an analysis of causes and consequences, *Journal of Loss Prevention in the Process Industries 12*, pp. 361-378.

Kirwan B., 1998a. Soft systems, hard lessons, *Applied Ergonomics 31*, pp. 663-678.

Kirwan B., 1998b. Safety management assessment and task analysis – a missing link?, in: Hale et al. (Eds.), *Safety Management the challenge of change*, Pergamon, Oxford.

Kirwan B., 2001. Coping with accelerating socio-technical systems, *Safety Science (37)*, pp. 77-107.

Kletz T.A., 1974. *HAZOP and HAZAN – Notes on the Identification of Hazards*, Institute of Chemical Engineers, Rugby.

Kletz T., 1993. *Lessons from disaster, How organizations have no memory and accidents recur*, IChemE, UK.

Kletz T.A., 1998. *Process Plants: A handbook for Inherently Safer Design*, 2nd ed, Taylor and Francis, Washington D.C.

Knegtering B., 2002. *Safety Lifecycle Management in the process industry*, PhD-thesis, Eindhoven University Press, Eindhoven.

Koornneef F., 2000. *Organised Learning from Small-scale Incidents*, PhD thesis, Delft University of Technology, Delft.

Körvers P.M.W., Schaafsma J., Sonnemans P.J.M., 2001a. Investing in safety or production: a dilemma?, *Proceedings 16th Annual International CCPS conference and workshop: Making process safety pay*, Toronto, AIChE, New York, pp. 177 – 191.

Körvers P.M.W., Schaafsma, J., Brombacher, A.C., Sonnemans, P.J.M., 2001b. The value of safety control in business operations, *Proceedings of the European Conference on Safety and Reliability (ESREL): Towards a Safer World*, Torino, pp. 467 – 474.

Körvers P.M.W., Sonnemans P.J.M., Beek van P.C., 2002. Ongevallen zijn geen toeval!, NVVK – *Leren van ongevallen en rampen (in Dutch)*, pp. 45 - 50.

Körvers P.M.W., Sonnemans P.J.M., Beek van P.C., 2003. Are accidents always unforeseeable? – learning from accident analysis, *Proceedings of the 37th Annual Loss Prevention Symposium*, AIChE, New Orleans, pp. 483-492.

Körvers P.M.W., Sonnemans P.J.M., 2004. Accidents a discrepancy between indicators and FACTS!, *Safety Science* (submitted for publication).

Kuipers H., Amelsvoort van P., 1990. *Slagvaardig organiseren (in Dutch)*, Kluwer, Deventer.
Lagadec P., 1997. Learning Processes for Crisis Management in Complex Organizations, *Journal of Contingencies and Crisis Management 5 (1)*, pp. 24-31.
Landau M., Stout. Jr. R., 1979. To manage Is Not To Control: Or the Folly of Type II Errors, *Public Administrative Review March/April*, pp. 148-156.
Lees F.P., 1996. *Loss Prevention in the process industries*, Butterwoth-Heinemann 2nd edition.
Leeuw de A.C.J., 1986. *Organisatie: management, ontwerp en verandering (in Dutch)*, 2nd edition, van Gorcum, Assen.
Leplat J., 1987. Accidents and Incidents Production: Methods of Analysis, in: Rasmussen et al. (Eds.), *New Technology and Human Error*, Chichester.
Lewins F., 1992. *Social Science Methodology*, Macmillam, Melbourne.
Mal van H., 1999. *Levenscyclus van product en productiesysteem (in Dutch)*, lecture notes course LPP, Technische Universiteit Eindhoven, Eindhoven.
Marco de T., 1979. *Structured Analysis and System Specification*, Prentice Hall Inc., New Jersey.
Marono M., Correa M.A., Sola R., 1998. Strategy for the development of operational safety indicators in the chemical industry, *Proceedings of the 9th International symposium on Loss Prevention and Safety Promotion in the process industries*, Barcelona, pp. 205-215.
Meredith J.R., Raturi A., Gyampah K.A., Kaplan B., 1989. Alternative Research Paradigms in Operations, *Journal of Operations Management 8 No. 4*, pp. 297-326.
Mesarovic M.D., Macko D., Takahara Y., 1970. *Theory of Hierarchical, Multilevel, Systems*, Academic Press, New York.
Mintzberg H., 1983. *Structures in Fives: Designing effective organizations*, Prentice Hall, Englewood Cliffs.
Modarres M., Mosleh A., Wreathall J., 1994. A framework for assessing influence of organization on plant safety, *Reliability Engineering & System Safety 45*, pp. 157-171.
Murphy D.M., Paté-Cornell M.E., 1996. The SAM-framework: modeling the effects of management factors on human behavior in risk analysis, *Risk Analysis 16*, pp. 501-515.
Øien K., 2001. A framework for the establishment of organizational risk indicators, *Reliability Engineering & System Safety 74*, pp. 174-167.
Osborn R.N., Jackson D.H., 1988. Leaders, Riverboat Gamblers, or Purposeful Unintended Consequences in the management of complex dangerous technologies, *Academy of Management Journal Vol. 31 (4)*, pp. 924-947.
OSHA-1910.119, 1996. *Process safety management of highly hazardous chemicals*, U.S. Department of Labor.
Parsons T., 1960. *Structure and Process in Modern Societies*, Free Press, New York.
Pasman H.J., Grollier Baron R., 2002. How is it possible? Why didn't we do anything? A case history!, *Journal of Hazardous Materials 93*, pp. 147-154.
Pasman H.J., Vrijling J.K., 2003. Social Risk Assessment of Large Technical Systems, *Human Factors and Ergonomics in Manufacturing Vol. 13(4)*, pp. 305-316.
Patton M.Q., 1987. *How to use qualitative methods in evaluation*, Sage publishing, Newbury Park.

Perrow C., 1984. *Normal accidents*, Basic Books, New York.
Petersen D., 1996. *Safety by objectives, what gets measured and rewarded gets done*, 2nd edition, Van Nostrand Reinhold, New York.
Pidgeon N., O'Leary M., 2000. Man-made disasters: why technology and organizations (sometimes) fail, *Safety Science (34)*, pp. 15-30.
Punch K.F., 1998. *Introduction to social research: quantitative and qualitative approaches*, Sage Publishing, Thousands Oaks.
Rasmussen J., 1997. Risk management in a dynamic society: a modelling problem, *Safety Science Vol. 27 No. 2/3*, pp. 183-213.
Rasmussen J., Svendung I., 2000. *Pro-active Risk Management in a Dynamic Society*, Swedish Rescue Services Agency, Karlstad.
Reason J.T., 1990. *Human Error*, Cambridge University Press, Cambridge.
Reason J., 1991. Too little and too late: a commentary on accident and incident reporting systems, in: Schaaf van der, et al. (Eds.), *Near miss reporting as a safety tool*, Butterworth Heinemann, Oxford.
Reason J., 1997. *Managing the Risks of Organizational Accidents*, Ashgate Publ., Aldershot.
Reason J.T., Carthey J., Leval de M.R., 2001. Diagnosing 'Vulnerable system syndrome': an essential prerequisite to effective risk management, *Quality in Health Care Vol. 10 (Suppl. II)*, pp. 21-25.
Roberts K., 1989. The Significance of Perrow's Normal Accidents: Living with High-Risk Technologies, *Academy of Management Review 14 (2)*, pp. 285-289.
Roberts K.H., Bea R., 2001. Must accidents happen? Lessons from high-reliability organizations, *Academy of Management Executive Vol. 15 (3)*, pp. 70-79.
Rosenthal , 2000. *Jan de Kroes lezing (in Dutch)*, NVVK.
Schaaf van der T.W., 1991. A framework for designing near miss management systems, in: Schaaf van der, et al. (Eds.), *Near miss reporting as a safety tool*, Butterworth Heinemann, Oxford.
Schaaf van der T.W., 1992. *Near miss reporting in the chemical process industry*, PhD thesis, Eindhoven University of Technology, Eindhoven.
Schaaf van der T.W., Kanse L., 2004. Biases in incident reporting databases: an empirical study in the chemical process industry, *Safety Science 42*, pp. 57-67.
Schein E.H., 1999. *Process Consultation revisited: building the helping relationship*, Addison Wesley, Amsterdam.
Seppala A., Participative Management models and the role of groups and supervision, in: Hale et al. (Eds.), *Safety Management the challenge of change*, Pergamon, Oxford.
Seveso II directive [96/082/EEC], 1996. *Council Directive of December 9, 1996 on the control of major accident hazards involving dangerous substances*, The council of the European union.
Sitter de L.U., 1987. *Op weg naar nieuwe fabrieken en kantoren (in Dutch)*, 5th edition, Kluwer, Deventer.
Smith M., 1997. Esso Asutralia's approach to safety management, *Proceedings of the Queensland Mining Industry Health and Safety Conference*, Queensland.
SofTech, 1976. *An Introduction to SADT, Structured Analysis and Design Technique*, SofTech Inc., Waltham.
Sonnemans P.J.M., Körvers P.M.W., Brombacher A.C., Beek van P.C., Reinders J.E.A., 2003. Accidents, often the result of an 'uncontrolled business process' – a study in the (Dutch) chemical industry, *Quality & Reliability Engineering International 19 (3)*, pp. 183-196.

Sonnemans P.J.M., Körvers P.M.W., Brombacher A.C., 2004. Effective Safety management – A case study in chemical industry, *Quality & Reliability Engineering International 20 (2),* pp.

Sorensen J.N., 2002. Safety culture: a survey of the state-of-the-art, *Reliability Engineering and System Safety 76*, pp. 189-204.

Steen van J., 1996. *Safety Performance Measurement*, European Process Safety Council, Bookcraft Ltd, Somerset.

Strauss A.L., 1987. *Qualitative analysis for social scientists*, Cambridge University Press, Cambridge.

Strauss A.L., Corbin J., 1990. *Basics of Qualitative Research: Grounded Theory, Procedures and Techniques*, Sage Publications, London.

Strien van P.J., 1986. *Praktijk als Wetenschap (in Dutch)*, Van Gorcum, Assen.

Suokas J., Rouhiainen V., 1993. *Quality Management of Safety and Risk Analysis*, Elsevier, Amsterdam.

Svenson P., 2001. Accident and Incident Analysis Based on the Accident Evoluation and Barrier Function (AEB) Model, *Cognition, Technology & Work 3*, pp. 42-52.

Thompson J.D., 1967. *Organizations in Actions*, McGraw-Hill, New York.

Tielemans H.J., 1995. De risico-samenleving als management probleem, *Holland Management Review 44 (in Dutch)*, pp. 77-81.

Tixier J., Dusserre G., Salvi O., Gaston D., 2002. Review of 62 risk analysis methodologies of industrial plants, *Journal of Loss Prevention in the process industries 15*, pp. 291-303.

Trochim W., 1989. Outcome pattern matching and program theory, *Evaluation and Program Planning No. 12*, pp. 355-366.

Turner B.A., 1978. *Man-made disasters*, Wykeham Publications Ltd., London.

Tweeddale H.M., 1995. Principles and practises for designing of process safety monitoring and auditing programmes, *Proceedings of the 8th International symposium on Loss Prevention and Safety Promotion in the process industries*, Antwerpen, pp. 71-82.

Vaughan D., 1996. *The Challanger Launch Decision: Risk Technology, Culture, and deviance at NASA*, Chicago University Press, Chicago.

Veld in het J., 1999. *Analyse van organisatieproblemen – een toepassing van denken in systemen en processen (in Dutch)*, 7th edition, Educatieve Partners Nederland BV, Houten.

Visser J.P., 1998. Development in HSE Management in oil and gas exploration and production, in: Hale et al. (Eds.), *Safety Management the challenge of change*, Pergamon, Oxford.

Vosselman S.G.J., 1996. De ontwerpgerichte benadering in management accounting en control onderzoek, in: Boneco M. et al. (Eds.), *FMA-kroniek (in Dutch)*, Samson, Alphen a/d Rijn, pp. 397-417.

Vuuren van W., 1998. *Organizational failure: an exploratory study in the steel industry and the medical domain,* PhD thesis, Eindhoven University of Technology, Eindhoven.

Wagenaar W.A., 1983. Human error (in Dutch), Inaugural lecture, Leiden University, Leiden.

Wagenaar J., Groeneweg J., Hudson P.T.W., Reason J.T., 1994. Safety in the oil industry, *Ergonomics 37(12)*, pp. 1999-2013.

Wagenaar W.A., Schrier van der J.H., 1997. Accident analysis. The goal and how to get there, *Safety Science 26 (1/2)*, pp. 25-33.

Watson, 1971. *Fault tree analysis as an aid to improved performance*, AMC Safety Digest. US Army Material Command.

Weick KE., Sutcliffe K., Obstfeld D., 1999. Organizing for High Reliability, *Research in Organizational Behavior 1 (21)*, pp. 81-123.

Weil R., Apostolakis G., 1999, Identification of important organizational factors using operating experience, *Proceedings of the 3rd International Conference on Human Factor Research in Nuclear Power Operations*, Japan.

Wiener N., 1948. *Cybernetics*, Wiley, New York.

Wilde G.J.S., 1982. The theory of risk homeostasis: implications for safety and health, *Risk Analysis 2*, pp. 209-225.

Wilpert B., 2002. Foreword, in: Wilpert B., et al. (Eds.), *System Safety, challenges and pitfalls of intervention*, Pergamon, Oxford, pp. VII-XII.

Wright L.B., 2002. *Accident versus near miss causation*, PhD thesis, University of Strathcycle, Glasgow.

Wright L.B., Schaaf van der T.W., 2003. Accident versus near miss causation: a critical review of the literature, an empirical test in the UK railway domain, and their implications for other Sections, *ESReDA Seminar on Safety Investigation of Accidents*, Petten.

Yin R.K., 1994. *Case Study Research: Design and Methods*, 2nd ed. Sage Publications, London.

Zwaan van der A.H., 1990. *Organisatie-onderzoek. Leerboek voor de praktijk: het ontwerp van onderzoek in organisaties (in Dutch)*, Van Gorcum, Assen.

APPENDIX A

Table showing the results of the two raters

In the table shown in this Appendix, the first column shows the results of rater 1, divided into three sub-columns stating if the control element (observation, judgement, or intervention) was effective, unknown, ineffective, or the steering element was ineffective. Furthermore the total score from rater 2 for each control element is shown in the final row. In the second column the individual results for each control element from rater 2 are shown. The third column shows the total scores of rater 1.
For example, rater 1 rated that 27 precursors had an effective observation. However, rater 2 rated that only 23 precursors had an effective observation and that one precursor had an ineffective observation and the three other precursors had an ineffective steering, causing an ineffective observation.

			Rater 2												
			effective			unknown			ineffective			ineffective steering			total
			observation	judgement	intervention	observation	judgement	intervention	observation	judgement	intervention	observation	judgement	intervention	
Rater 1	effective	observation	23						1			3			27
		judgement								2			4		6
		intervention													
	unknown	observation													
		judgement					14								14
		intervention						28							28
	ineffective	observation							5						5
		judgement								8					8
		intervention									1				1
	ineffective steering	observation										7			7
		judgement											11		11
		intervention									3			7	10
total			23				14	28	6	10	4	10	15	7	117

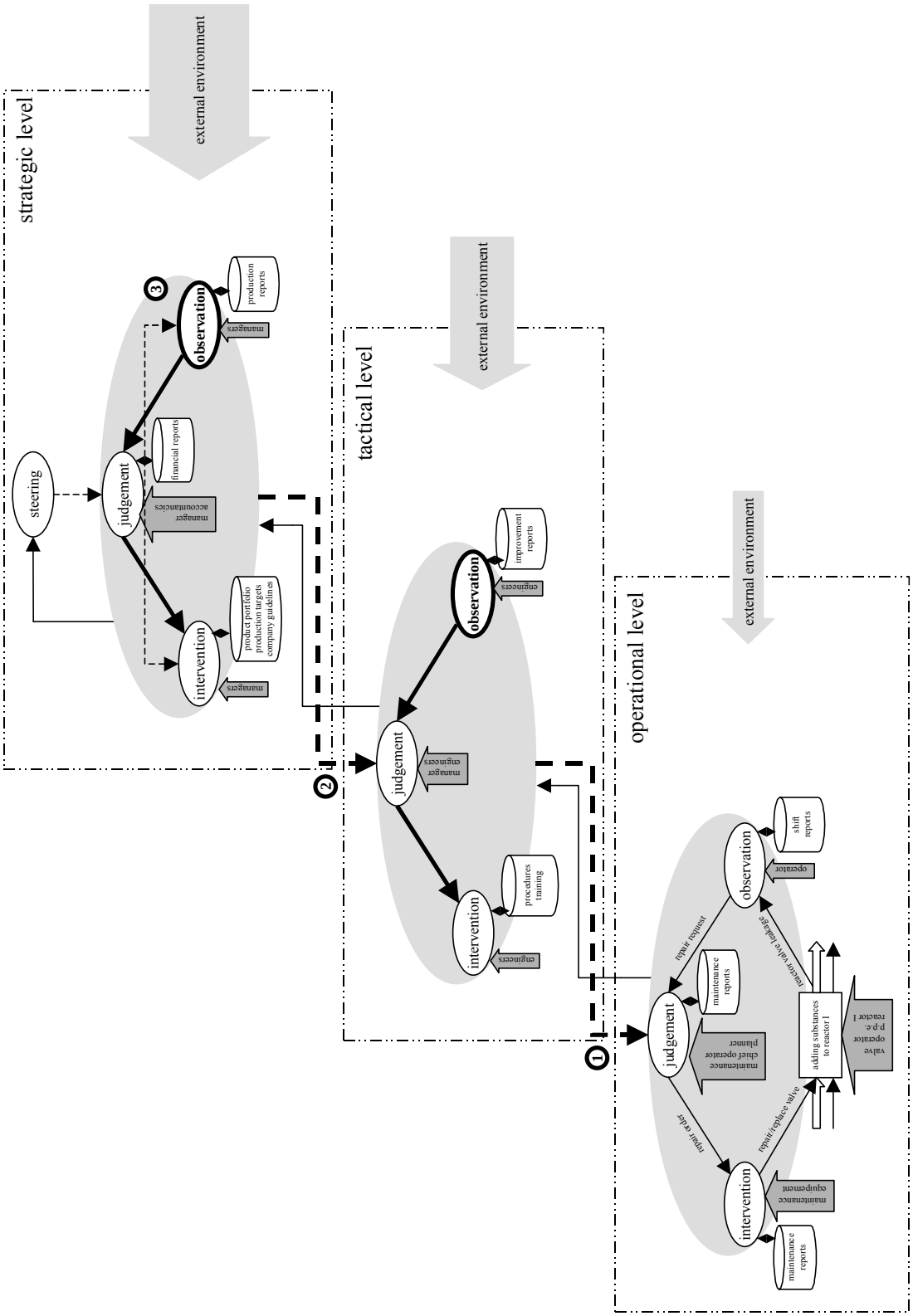
APPENDIX B

Top 20 precursors of companies A, B and C.

	Company A	Company B	Company C
1	vacuumpump trip	reactor valve leakage	heater from extruder fails
2	leakage gasket	leakage gasket	concentration feeder trips
3	reactor valve leakage	trip mixer	wet cubesystem
4	pressure relief valve 1 defect	leakage cooling unit	dowel broken
5	differences between written procedures & computer version	trip cooling unit	die-plate clogged
6	dust in packaging hall	trip vacuum pump	temperature rise instantaniously
7	clogged pipelines	clogged valve	pump 1 trips
8	conveyer belt error	clogged pipes	clogged filter
9	valve 2 leakage	missing blind flange	water leakage
10	pump 1 trip	equipment not always present	valve 1 clogged
11	valve 3 leakage	instantanious pressure change reactor 1	false alarms
12	release of vapours while adding to reactor	ventialtion of reactor 1 & 2 via office ventialtion system	pressure rise inside extruder
13	trip mixer	procedures not possible	gaskets leak
14	flow device defect	leaking vacuum drying chamber	pressure relief valve trips
15	pump 2 leakage	adding substances not under vacuum	dryer is set too high
16	steam kettle error	release of vapours while adding to reactor	trip blower
17	false alarms	temperature setting often higher	hot bags fall from conveyer belt
18	blocked shredder	false alarms	pump 2 clogged
19	knifes blunt	no ventilation at necessary places	palletizer error
20	pressure relief valve 2 trip	disorderly storage of hazardous substances	cutter blunt

APPENDIX C

Example of a graphical representation to identify an initial ineffective control element.



APPENDIX D

Tables showing types of latent conditions per initial ineffective control element per company.

In the tables shown in this Appendix, the first column states the company and is further divided into a column identifying the control level, i.e. operational, tactical or strategic level, a column identifying the ineffective control elements, i.e. observation, judgement, intervention or steering and the number of ineffective control elements that were found, which is taken from Figure 43. The second column shows the information flow relating to latent conditions and is further divided into a column transformation, history, (organizational) values & norms, and external environment. The third column shows the resources related latent conditions and is further divided into a column infrastructure and human.

The values in the table represent the number of contributions a latent condition makes to the corresponding ineffective control element. For example, the identified latent conditions of an ineffective observation element on strategic control level in company A can be found in the row 'strategic control level' and 'observation' in the table of company A. This row subsequently shows transformation 2, history 1, and external environment 2. This means that in company A of the two initial ineffective observation elements on the strategic control level, in both cases the transformation was a latent condition type, in one case the history was a latent condition type, and in both cases the external environment was a latent condition type, that contributed to the ineffectiveness, finally leading to the corresponding precursors.

company A			information				resources	
			transformation	history	values & norms	external environment	infrastructure	human
operational control level	observation	2		2	1			2
	judgement	5		3	4		1	4
	intervention	1	1		1			1
tactical control level	observation	2	2		1	1		1
	judgement	6	3	4	4	2	4	2
	intervention	1	1				1	
strategic control level	observation	2	2	1		2		
	judgement	1	1	1		1		
	intervention							
	steering							
total company A		**20**	**10**	**11**	**11**	**6**	**6**	**10**

company B			information				resources	
			transformation	history	values & norms	external environment	infrastructure	human
operational control level	observation	3		2	2		1	3
	judgement	5	1	4	2		1	4
	intervention	1			1		1	1
tactical control level	observation	3	2	3	2			
	judgement	6	4	5	4	2	3	
	intervention	1	1	1	1		1	
strategic control level	observation	1	1	1		1		1
	judgement							
	intervention							
	steering							
total company B		**20**	**9**	**16**	**12**	**3**	**7**	**9**

company C			information				resources	
			transformation	history	values & norms	external environment	infrastructure	human
operational control level	observation	1		1	1			1
	judgement	1		1	1			1
	intervention							
tactical control level	observation	2		2	2		1	
	judgement	9	4	7	9	2	3	3
	intervention	2	2	2	2			
strategic control level	observation	2	1	2	2	1		
	judgement	3	3	2	3	2		
	intervention							
	steering							
total company C		**20**	**10**	**17**	**20**	**5**	**4**	**5**

APPENDIX E

Tables showing precursors, latent conditions and affected safety barriers per company.

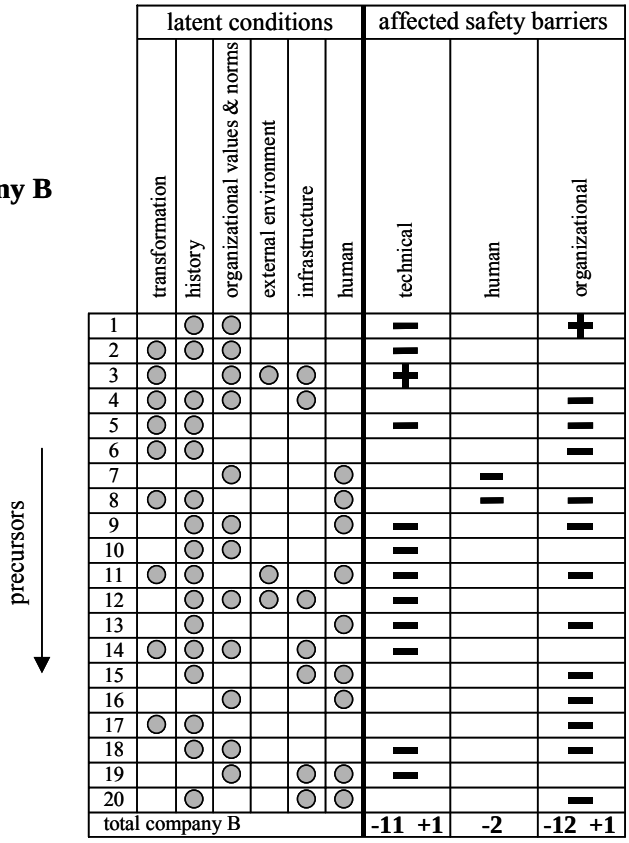
In the tables shown in this Appendix, the first column shows the top 20 precursors. The numbers in the column correspond with the numbers as shown in Appendix B, where the top 20 precursors of all three cases are stated. The second column shows the latent conditions and is further divided into a column transformation, history, organizational values & norms, external environment, infrastructure, and human. The third column shows the affected safety barriers and is further divided into a column technical, human, and organizational.

The grey dots in the table represent the types of latent conditions corresponding to the precursors. For example, precursor 1 in the table of company A, is enabled by 'history,' 'organizational values and norms,' and 'infrastructure' types of latent conditions. The minus sign (-) and the plus sign (+) in the table represent the negatively or positively affected safety barrier functional categories successively, corresponding to the types of latent conditions and precursors. For example, the similar precursor 1 in company A, is taken. This precursor, together with the identified latent conditions indicated above, affects a technical safety barrier in a negative way.

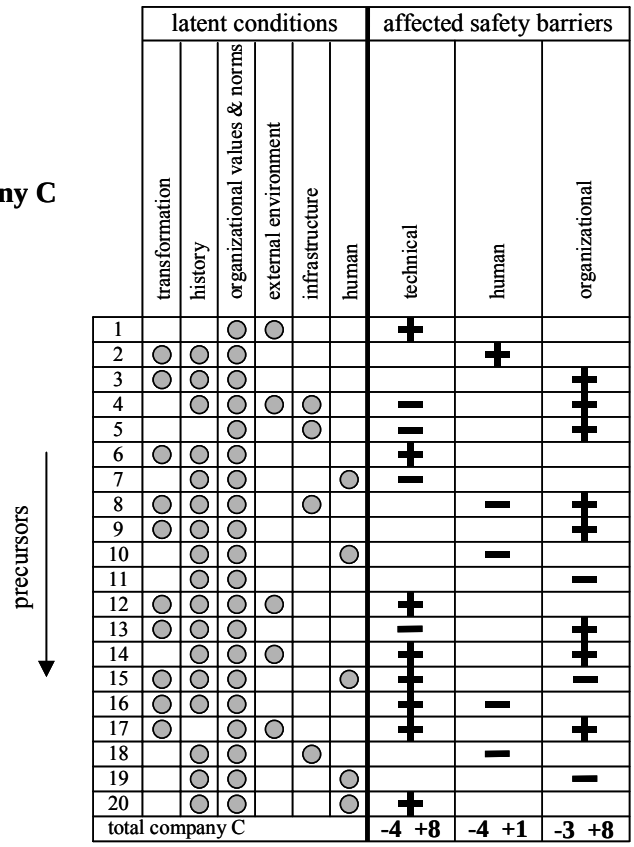
company A

precursors	latent conditions						affected safety barriers		
	transformation	history	organizational values & norms	external environment	infrastructure	human	technical	human	organizational
1		●	●		●		−		
2			●			●			−
3	●	●		●				−	
4		●	●			●	−		−
5	●	●	●			●			−
6	●				●				−
7	●			●			−	−	
8	●		●			●	−		−
9	●	●		●				−	−
10	●		●					−	
11	●	●		●	●				−
12	●			●		●	+		−
13					●		+		+
14		●				●	−		
15	●		●	●		●		−	
16		●	●		●		+		+
17		●				●			−
18		●	●			●	−		
19		●	●			●	−		−
20			●		●				−
total company A							**-7 +3**	**-5**	**-11 +2**

company B



company C



ABOUT THE AUTHOR

Patrick Körvers was born on January 10, 1976 in Hunsel, The Netherlands. In 1994 he received his VWO diploma from the Bisschoppelijk College in Echt, after which he started his study in Mechanical Engineering at the Technische Universiteit Eindhoven. He received his Master's Degree in 1999 after a research project at Philips BU Monitors Chungli, Taiwan, concerning the development of efficient reliability tests. In 1999, he started his Ph.D. work as a member of the Quality of Products & Processes Section of the department of Technology Management, Technische Universiteit Eindhoven. The research project was initiated by the department of Industrial Safety of the TNO Institute of Environmental Sciences, Energy Research and Process Innovation, concerning accident precursors. This thesis concludes the research.

Apart from this thesis, the PhD work resulted in a number of papers that have been presented at international conferences and published in various international journals. The research was performed in co-operation with various companies in the Dutch chemical industry and the department of industrial safety at TNO. While TNO will continue with the results of this research, Patrick starts working for SABIC Euro Petrochemicals B.V., from the 1st of March onwards.

Propositions

supplementing the PhD thesis

Accident precursors: pro-active identification of safety risks in the chemical process industry

by

P.M.W. Körvers

22 March 2004

I. Achieving a required safety level *can* be a matter of selecting the appropriate safety performance indicator.

- *This thesis*

II. Safety reports created by safety departments do not give a proper indication of the actual safety level because they are not based on knowledge of the normal way of working in the operational process of a company.

- *This thesis*

III. From a technical process perspective, the concept of independent safety barriers appears to be excellent. However, in practice implementing this concept upon the organizational process will inevitable lead to potential new safety risks.

- *This thesis*

IV. Ignoring dominant classes of deviations in models of operational processes may reduce the predicted probability of occurrence of high-potential safety risks in a numerical sense, but it will certainly not reduce the actual likelihood or impact for society.

- *This thesis*

V. Determining root causes of accidents in today's society often stops at the level of technical malfunctions and procedures. The underlying organizational causes are forgotten and never looked at.

- *FNV Bondgenoten, 2001. Veiligheid van papier, Stichting FNV Pers, Utrecht.*

VI. The design of inherently safe plants is feasible, running such a plant in a safe way is not.

- *Kletz T.A., 1998. Process Plants: A Handbook for Inherently Safer Design, Taylor & Francis Inc., London.*

VII. Although politicians use risk profiles as being discrete transitions, these profiles actually represent a continuous phenomenon with a high degree of uncertainty.

- *Ham J.M., 2001. Kwantitatieve risico analyse generiek voor LPG tankstations (hoofdrapport ref. 2001/435a), TNO-MEP, Apeldoorn.*

VIII. Near misses do not lead to enhanced safety awareness; big accidents do.

IX. Honesty takes a great deal, especially money. Dishonesty however always costs more, especially in the long term.

X. 'Chemistry' is not only relevant on the operational level in the chemical process industry. Also on tactical and strategical level it plays an important role in all types of industries.

XI. Excessive attention paid to political correctness leads to social incorrectness.

- *CWI (Centrum voor Werk en Inkomen)*

XII. In general, the 'achievable' success of one's career path is more correlated to the size of one's network, rather than one's personal quality.