Preventing major hazard accidents through barrier performance monitoring

Schmitz, P.J.H.

DOI
10.4233/uuid:782fcd3e-0db4-42ee-965a-c180586759f4

Publication date
2021

Document Version
Final published version

Citation (APA)
Schmitz, P. J. H. (2021). *Preventing major hazard accidents through barrier performance monitoring*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:782fcd3e-0db4-42ee-965a-c180586759f4

PREVENTING MAJOR HAZARD ACCIDENTS THROUGH BARRIER PERFORMANCE MONITORING

Peter Schmitz

Preventing major hazard accidents through barrier performance monitoring

Peter Schmitz

Cover image:
The Horse Problem was an installation of sculptures Claudia Fontes made on the occasion of representing Argentina at the Venice Biennial in 2017.
The installation shows a bullet-time frozen scene in which a horse, a woman and a young man are trapped in an infinite causality loop for which fear is the cause and the symptom at once. The horse's fear of being trapped in the building creates an avalanche of rocks travelling into his direction, the shadows of which form a mirrored image of himself, albeit exploding. The whiteness and smoothness of the material give the scene the quality of an apparition as if the characters and their circumstances existed in a parallel temporality. The audience, as onlookers, complete the narrative.
(source: https://claudiafontes.com/project/the-horse-problem/)

From the author:
The horse on the cover has become gripped with fear and has turned against the two youngsters. The horse instills fear in both the woman and the young man (whom we don't see in this photo). Fear as cause and effect. In this artwork, the horse symbolizes danger. The woman so close to the horse runs the risk of being trampled. It seems impossible to stop the menacing and powerful horse. But if she succeeds, and we can only hope so, she has saved the young man and herself from being injured or worse. This symbolism is metaphorical for our process installations where the barriers or safeguards have to protect us against the lurking hazards: the trapped energy, and the flammable and toxic substances. The smallest barrier, if trustworthy, can stop an accident process and prevent the hazards being released.

Key words: process safety, indicator, ammonia, barrier, bowtie
Printed by: Gildeprint b.v., Enschede
Cover by: Ilse Modder, www.ilsemodder.nl
Lay-out by: Ilse Modder, www.ilsemodder.nl
ISBN: 978-94-6419-348-0

An electronic copy of this dissertation is available at https://repository.tudelft.nl/.

Preventing major hazard accidents through barrier performance monitoring

Dissertation

for the purpose of obtaining the degree of doctor
at Delft University of Technology,
by the authority of the Rector Magnificus, Prof. dr. ir. T.H.J.J. van der Hagen,
chair of the Board of Doctorates,
to be defended publicly on Monday 15 November 2021 at 15:00 o'clock

by

Petrus Joseph Hubertus SCHMITZ
Master in the field of Safety, Health and Environment
Delft University of Technology, the Netherlands
Born in Hoensbroek, the Netherlands

This dissertation has been approved by the promotor.

Composition of the doctoral committee:

Rector Magnificus	chairperson
Prof. dr. ir. G.L.L.M.E. Reniers	Delft University of Technology, promotor
Dr. P.H.J.J. Swuste	Delft University of Technology, copromotor

Independent members:

Prof. dr. J. Groeneweg	Delft University of Technology
Prof. dr. E. Albrechtsen	Norwegian University of Science and Technology, Norway
Prof. dr. ir. H.J. Pasman	Texas A&M University, United States of America
Prof. dr. ir. C. van Gulijk	University of Huddersfield, United Kingdom
Dr. ir. G. Hoedemakers	Anqore, Geleen, The Netherlands

Reserve member:

Prof. dr. ir. P.H.A.J.M. van Gelder	Delft University of Technology

Dedicated to my parents

TABLE OF CONTENTS

SUMMARY

Foreseeing or even predicting major accidents is understandably challenging, both for any practitioner involved as for safety scientists and other academics. Understanding these events and trying to prevent them is a primary goal of a safety theory. Major hazard-related accidents rarely occur but when they do, they can cause many casualties and injured, and have major financial consequences due to production loss, material damage to the installation and/or environmental damage. Ultimately, major hazard-related accidents may ruin the company involved. Process safety is becoming more and more important in the process industry and is strongly linked to reliability, quality, productivity, security of supply, and good business.

OCI, one of Chemelot's largest site users, has faced several serious, sudden process safety related accidents, including those at its two ammonia plants. Although no physical injuries were suffered in any of the incidents, in some cases the ammonia plant had to be shut down for a longer period, resulting in both hardware damage and a substantial loss of production. An external investigation, looking at several incidents at Chemelot in 2015 and 2016, concluded that there was insufficient anticipation of "early warnings" from the chemical processes. OCI initiated its own investigation which resulted in this doctoral research for process safety and how targeted measures can be taken at an early stage to stop the development of major accident processes. The main question of this doctoral research is:

> *To what extent can major hazard accidents in the process industry be prevented?*

In this doctoral research, major hazard accidents are visualised using bowties. Bowties comprise one or more hazards, the initiating events of scenarios, the central event, the consequences and the barriers that can stop the scenario from happening. Barriers at scenario level have an immediate influence on the accident process. On the other hand, organisational factors or management delivery systems have an indirect influence on major hazard accident processes, and should be seen as systems giving support to the functioning of barriers. Proper barrier management through effective organisational factors or management delivery systems guarantees the quality or trustworthiness of the barrier systems, being designed to stop the development of the accident processes. Organisational factors or management delivery systems are non-technical in nature and should be regarded as work processes and procedures in which human action or decision-making predominates. By precisely defining indicators, insight can

be gained into the quality or trustworthiness of the barrier systems, as well as into the effectivity of the organisational factors, or management delivery systems. These defined indicators do not only determine the urgency but also indicate what needs to be done.

In the first step of this research, the magnitude of major process safety incidents of the ammonia process has been investigated. In other words: the equipment which can give rise to the most severe consequences in case of failure. From the calculations, it was concluded that the equipment with the highest pressure and the equipment with liquid ammonia are the most dangerous ones. This equipment has the potential to cause the largest adverse health impact on humans in the event of failure. The effects and thus the adverse health impact on people increase as pressure, temperature and mass increase. In addition, liquid, 'warm' ammonia is a severe threat as it evaporates quickly at release and forms a large toxic cloud.

The next step answers the question how the possibility of major process safety incidents can be monitored over time. The answer has been given using scenarios caused by mechanical failure of static process equipment. In response, the primary focus was on probable and very probable scenarios, which either have already occurred at OCI, or are known from the international literature on accidents at ammonia plants. Based on operating parameters like pressure, temperature, and flow, it is deemed possible to monitor the development of these scenarios. Early warnings derived from these operating parameters can serve as an indicator to show the development of the scenarios.

In two subsequent studies the extent has been investigated to which such indicators provide information which relates to the likelihood of the central event. In the first sub-study, indicators have been derived from the status of the barrier system. An indicator, referred to as 'preventive barrier indicator', has been developed which has proven to monitor the level of safety, and enable the operators to decide when, where, and which action is necessary. The preventive barrier indicator shows the development and possibility of a certain scenario, which is not an absolute value, but rather an indication of the change in the *status quo* that should initiate further action or not. In the second sub-study the aim was to investigate organisational factors or management delivery systems. A list of nine organisational factors or management delivery systems has been compiled which are applicable for OCI Nitrogen, but also for the process industry as a whole. Audits and peer reviews are the right tools to assess the efficiency of organisational factors in both a qualitative and quantitative way. However, determining threshold values for which action is required, is an intricate matter because the influence on the accident processes is difficult to determine. But,

once threshold values have been set, management indicators can be developed, which are measured at a certain frequency of, for example, once a month or once a quarter. Finally, the BP Texas City refinery accident of 2005 has been taken as an example to validate the model. The bowtie metaphor is used to visually present the BP Texas City refinery accident, showing the barrier system from three different perspectives. The risk reductions of these different views have been calculated and compared to their original design. In addition, evidence and findings from the BP and US Chemical Safety Board investigations have been categorised as flaws and allocated to the nine organisational factors. The validation sheds new light on the monitoring of accident processes and the barrier management to control them, and demonstrates that the BP Texas City refinery accident could have been foreseen using preventive barrier indicators and monitoring organisational factors.

Barrier performance monitoring, using preventive barrier indicators and an audit technique focussed on organisational factors, is a very promising possible way forward to prevent major hazard accidents in the process industry. To set up an operational barrier management, it is recommended to follow the step by step approach below:

- Conduct a thorough literature research in order to obtain an overview of the major hazard accidents from the chemical process concerned;
- Determine the adverse health effects on failure of each process equipment and focus on the most dangerous ones;
- Select the most credible scenarios, and visualise them in bowties;
- Establish the early warnings derived from process parameters and act when they indicate the initiation of an accident process;
- Monitor the trustworthiness of the main barrier systems using indicators showing the likelihood and development of the accident scenarios;
- Select the organisational factors and assess them both qualitatively and quantitatively on a regular basis.

Some future work would be needed to strengthen and improve this model. Firstly, the use of systemic accident models for major hazard accident prediction should be investigated to discover the influence of extra-organisational factors from which additional indicators may be derived. Secondly, the use of Bayesian Network to reduce data uncertainty of the bowtie should be explored to see whether this approach can improve the prediction of major hazard accidents. And thirdly, this model should be validated prospectively to demonstrate the extent to which major hazard accidents are prevented.

This research is innovative in the sense that the likelihood and development of major process-related accidents are monitored before the consequences become apparent. This is done on the basis of a combination of three indicators: 1. Early warnings based on process parameters such as pressure and temperature that show the initiation of an accident process, 2. Preventive barrier indicators that indicate the quality of the barrier system, but also the development of the scenario once the scenario has been initiated, and 3. Management indicators that provide information about the effectiveness of the organisational factors. In conclusion, with this research, process safety is one step closer to a much-needed theory.

SAMENVATTING

Zware ongevallen voorzien of zelfs voorspellen is begrijpelijkerwijs een uitdaging, zowel voor elke betrokken beroepsbeoefenaar als voor veiligheidswetenschappers en andere academici. Het begrijpen van deze gebeurtenissen en ze proberen te voorkomen is een primair doel van een veiligheidstheorie. Majeure proces gerelateerde ongevallen komen zelden voor, maar kunnen wel veel slachtoffers en gewonden veroorzaken en grote financiële gevolgen hebben door productieverlies, materiële schade aan de installatie en/of milieuschade. Uiteindelijk kunnen majeure, proces gerelateerde ongevallen het betrokken bedrijf te gronde richten. Procesveiligheid wordt steeds belangrijker in de procesindustrie en hangt sterk samen met betrouwbaarheid, kwaliteit, productiviteit, leveringszekerheid en een goede bedrijfsvoering.

OCI, één van de grootste bedrijven van Chemelot, heeft te maken gehad met verschillende ernstige, plotselinge procesveiligheid gerelateerde ongevallen, waaronder die bij de twee ammoniakfabrieken. Hoewel bij geen van de incidenten lichamelijk letsel werd opgelopen, moest de ammoniakfabriek in sommige gevallen voor een langere periode worden stilgelegd, met zowel materiële schade als substantieel productieverlies tot gevolg. Een extern onderzoek, waarbij gekeken werd naar enkele incidenten op Chemelot in 2015 en 2016, kwam tot de conclusie dat onvoldoende werd geanticipeerd op "early warnings" van de chemische processen. OCI startte een eigen onderzoek, dat resulteerde in dit promotieonderzoek naar procesveiligheid en hoe in een vroeg stadium gerichte maatregelen kunnen worden genomen om de ontwikkeling van zware ongevallenprocessen te stoppen. De hoofdvraag van dit promotieonderzoek is:

> *In hoeverre kunnen majeure proces gerelateerde ongevallen in de procesindustrie worden voorkomen?*

In dit promotieonderzoek worden majeure proces gerelateerde ongevallen in beeld gebracht met "bowties". "Bowties" omvatten één of meer gevaren, de initiërende gebeurtenissen van scenario's, de centrale gebeurtenis, de gevolgen en de barrières die het scenario kunnen tegenhouden. Barrières op scenarioniveau hebben direct invloed op het ongevalsproces. Aan de andere kant hebben organisatorische factoren of "management delivery systems" een indirecte invloed op grote ongevalsprocessen en moeten ze worden gezien als systemen die het functioneren van barrières ondersteunen. Een goed beheer van de barrières door effectieve organisatorische factoren of "management delivery systems" garandeert de kwaliteit

of betrouwbaarheid van deze systemen, en is zo ontworpen dat het de ontwikkeling van de ongevallenprocessen stopt. Organisatorische factoren of "management delivery systems" zijn niet-technisch van aard en moeten worden beschouwd als werkprocessen en procedures waarin menselijk handelen of besluitvorming de boventoon voert. Door indicatoren nauwkeurig te definiëren, kan inzicht worden verkregen in de kwaliteit of betrouwbaarheid van de barrièresystemen, evenals in de effectiviteit van de organisatorische factoren of de "management delivery systemen". Deze gedefinieerde indicatoren bepalen niet alleen de urgentie, maar geven ook aan wat er moet gebeuren.

In de eerste stap van dit onderzoek is de omvang van grote procesveiligheidsincidenten van het ammoniakproces onderzocht. Met andere woorden: de apparaten die bij falen leiden tot de meest ernstige gevolgen. Uit de berekeningen werd geconcludeerd dat de apparaten waarin de hoogste druk heerst en de apparaten met vloeibare ammoniak de gevaarlijkste zijn. Deze apparaten hebben in geval van falen de grootste nadelige gezondheidsgevolgen voor mensen. De effecten en daarmee de nadelige gezondheidsimpact op mensen worden groter als druk, temperatuur en massa toenemen. Bovendien vormt vloeibare, 'warme' ammoniak een ernstige bedreiging, omdat het bij het vrijkomen snel verdampt en een grote giftige wolk vormt.

De volgende stap beantwoordt de vraag hoe de kans op grote procesveiligheidsincidenten in de loop van de tijd kan worden bewaakt. Deze vraag is beantwoord aan de hand van scenario's veroorzaakt door mechanisch falen van statische procesapparaten. De focus lag daarbij primair op waarschijnlijke en zeer waarschijnlijke scenario's, die óf al hebben plaatsgevonden bij OCI, óf bekend zijn uit de internationale literatuur over ongevallen bij ammoniakfabrieken. Op basis van procesparameters zoals druk, temperatuur en debiet wordt het mogelijk geacht de ontwikkeling van deze scenario's te volgen. "Early warnings" afgeleid van deze procesparameters kunnen dienen als een indicator om de ontwikkeling van de scenario's te volgen.

In twee opeenvolgende studies is onderzocht in hoeverre dergelijke indicatoren informatie geven die betrekking heeft op de waarschijnlijkheid van de centrale gebeurtenis. In het eerste deelonderzoek zijn indicatoren afgeleid uit de status van het barrièresysteem. Er is een indicator ontwikkeld, 'preventieve barrière-indicator' genoemd, die heeft bewezen het veiligheidsniveau te bewaken en de operators in staat te stellen te beslissen wanneer, waar en welke actie nodig is. De preventieve barrière-indicator laat de ontwikkeling zien en de waarschijnlijkheid van een bepaald scenario, wat geen absolute waarde is, maar eerder een indicatie van de verandering in de *status quo* die al dan niet tot verdere actie zou moeten leiden. In de tweede deelstudie was het doel om organisatorische factoren of "management delivery

systems" te onderzoeken. Er is een lijst opgesteld van negen organisatorische factoren of "management delivery systems", die toepasbaar zijn voor OCI Nitrogen, maar ook voor de procesindustrie als geheel. Audits en peer reviews zijn de juiste instrumenten om de efficiëntie van organisatorische factoren zowel kwalitatief als kwantitatief te beoordelen. Het bepalen van drempelwaarden waarvoor actie vereist is, is echter ingewikkeld omdat de invloed op de ongevalsprocessen moeilijk te bepalen is. Maar als er eenmaal drempelwaarden zijn vastgesteld, kunnen er managementindicatoren worden ontwikkeld die met een bepaalde frequentie van bijvoorbeeld eens per maand of eenmaal per kwartaal worden gemeten.

Ten slotte is het ongeval van de BP-raffinaderij in Texas City in 2005 als voorbeeld genomen om het model te valideren. De "bowtie"-metafoor is gebruikt om het ongeval visueel weer te geven, waarbij het barrièresysteem vanuit drie verschillende perspectieven wordt getoond. De risicoreductie van deze verschillende perspectieven is berekend en vergeleken met hun oorspronkelijke ontwerp. Bovendien zijn bewijsmateriaal en bevindingen van de onderzoeken van BP en de US Chemical Safety Board gecategoriseerd als gebreken en toegewezen aan de negen organisatorische factoren. De validatie werpt een nieuw licht op de monitoring van ongevalsprocessen en het barrièrebeheer, en toont aan dat dit ongeval van BP had kunnen worden verwacht met behulp van preventieve barrière-indicatoren en het monitoren van organisatorische factoren.

Het monitoren van de barrières, met behulp van preventieve barrière-indicatoren en een audittechniek gericht op organisatorische factoren, is de beste manier om majeure proces gerelateerde ongevallen in de procesindustrie te voorkomen. Om een operationeel barrière management op te zetten, wordt aanbevolen om de onderstaande stapsgewijze aanpak te volgen:

- Voer een gedegen literatuuronderzoek uit om een overzicht te krijgen van de grote, proces gerelateerde ongevallen van het betreffende chemische proces;
- Bepaal de nadelige gezondheidseffecten bij falen van elke procesapparatuur en focus op de gevaarlijkste;
- Selecteer de meest waarschijnlijke scenario's en visualiseer ze d.m.v. bowties;
- Stel de 'early warnings' vast die zijn afgeleid van procesparameters en neem actie wanneer deze aangeven dat een ongevalsproces is begonnen;
- Bewaak de betrouwbaarheid van de belangrijkste barrièresystemen met behulp van indicatoren, die de waarschijnlijkheid en ontwikkeling van de ongeval scenario's aangeven;
- Selecteer de organisatorische factoren en beoordeel ze regelmatig zowel kwalitatief als kwantitatief.

Er is toekomstig onderzoek nodig om dit model te versterken en te verbeteren. Ten eerste zou het gebruik van systemische ongevalsmodellen voor het voorspellen van majeure proces gerelateerde ongevallen onderzocht moeten worden om de invloed te ontdekken van buiten-organisatorische factoren waaruit aanvullende indicatoren kunnen worden afgeleid. Ten tweede moet het gebruik van "Bayesian Network" worden onderzocht om de onzekerheid van data van de "bowtie" te verminderen, opdat deze benadering de voorspelling van majeure proces gerelateerde ongevallen kan verbeteren. En ten derde moet dit model prospectief gevalideerd worden om aan te tonen in welke mate majeure proces gerelateerde ongevallen worden voorkomen.

Dit onderzoek is innovatief in de zin dat de waarschijnlijkheid en ontwikkeling van majeure proces gerelateerde ongevallen worden bewaakt voordat de gevolgen duidelijk worden. Dat gebeurt op basis van een combinatie van drie indicatoren: 1. "Early warnings" gebaseerd op procesparameters zoals druk en temperatuur die de initiatie van een ongevalsproces aangeven, 2. Preventieve barrière indicatoren die iets zeggen over de kwaliteit van het barrièresysteem, maar ook de ontwikkeling van het scenario als het scenario geïnitieerd is, en 3. Management indicatoren die informatie geven over de effectiviteit van de organisatorische factoren. Concluderend, met dit onderzoek komt procesveiligheid een stap dichter bij een broodnodige theorie.

1

INTRODUCTION

1.1 BACKGROUND

1.1.1 The importance of process safety

Foreseeing or even predicting major accidents is understandably challenging, both for any practitioner involved as for safety scientists and other academics. Predicting these events is a primary goal of a safety theory[1]. Major hazard-related accidents rarely occur but when they do, they can cause many casualties and injuries and have major financial consequences due to production loss, material damage to the installation and/or environmental damage. Ultimately, major hazard-related accidents may ruin the company involved. For major hazard installations and chemical manufacturers, process safety risks are a significant aspect of business risk, asset integrity and reputation (HSE, 2006). Although low frequencies of occupational accidents are still sometimes seen as an indicator for process safety, a relation is doubted and contested in literature (Hale, 2002). Process safety is becoming more and more important in the process industry and is increasingly used for benchmarking purposes (Swuste et al., 2016). After all, process safety is strongly linked to reliability, quality, productivity, security of supply, and good business. A reliable company is predictable and a supplier you can count on.

1.1.2 Bowties as a means to visualise accident processes

In this doctoral research major hazard accidents are visualised using bowties. A bowtie is a safety metaphor for accident processes, and is appropriate and user-friendly for the mapping of scenarios (Visser, 1998; Chevreau et al., 2006; de Ruijter and Guldenmund, 2016). They have not only been applied in major hazard scenarios but also in occupational safety scenarios (Bellamy et al., 2007). As shown in Figure 1.1, the bowtie indicates one or more hazards, the initiating event of a scenario, the central event, the consequences and the barriers that can stop the scenario from happening. The development from hazard to the central event can take days, weeks or even years. When the central event occurs, the catastrophic consequences usually unfold very quickly (in minutes or even seconds).

A hazard has the intrinsic ability to cause material damage, casualties and injuries, and consists of energy (usually related to the characteristics of the substance(s) present) encapsulated in a process unit. The central event in (petro)chemical installations is often characterised by an undesirable and uncontrolled release of energy from the plant, which could be hazardous substances, or a temperature or pressure wave. Cockshott (2005) defines a central event as “the initial consequence which includes the release of a hazard”. It is a condition that could potentially lead to injury, damage to property or to the environment.

1 A theory is a validated model; a model is a representation of reality.

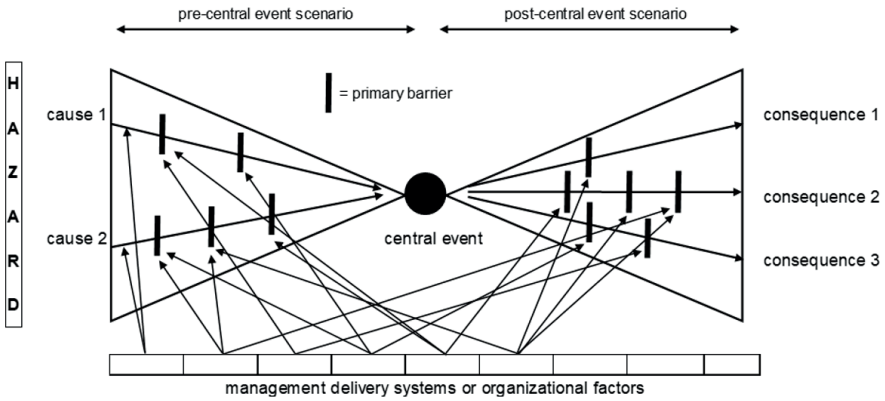

Fig. 1.1, the bowtie and the management delivery systems or organisational factors

1.1.3 Process safety control with barrier management

A barrier system is a set of barriers that are present to prevent causes from developing into consequences. Barriers have an immediate influence on the accident process and are able to prevent, delay or mitigate an accident from happening. In general, barriers at scenario level consist of elements that detect, decide or act (Guldenmund et al., 2006). Barrier elements can be physical (technical) and non-physical (non-technical). Although the simple, sequential design of bowties is strongly reminiscent of the "Swiss cheese model" by Reason (1990), bowties may have multiple scenarios leading to the central event, and from the central event to consequences. The holes in the Swiss cheese correspond to the flaws in organisational aspects. The bowtie does not address system failures as the pathogens, but addresses managerial delivery systems, primarily focussing on barrier status.

Organisational factors or management delivery systems have an indirect influence on (major hazard) accident processes and should be seen as systems giving support to (the functioning of) primary barriers (Bellamy, 2007). To ensure the performance of the barrier systems, the barrier systems themselves should be monitored, as well as the management delivery systems supporting them. Management must ensure that barriers work effectively via the management delivery systems (Guillaume, 2011). Management delivery systems are non-technical in nature. They are work processes and procedures in which human action and decision-making predominate.

This research focusses on barriers at two levels: those directly related to the (major hazard) accident processes, also called primary barriers, and those related to the operational management. The first level comprises the barriers stopping, delaying and/or mitigating the development of the accident processes, and the second level relates

to the organisational factors or management delivery systems, which support the first level. This research is innovative in the sense that the likelihood and development of (major hazard) accident processes is monitored before consequences become apparent, through observing (primary) barrier systems and management delivery systems. In order to do so, indicators have been developed that show the status of the barriers as well as the effectiveness of the management delivery systems supporting them.

1.1.4 The contribution of management delivery systems in accident processes

Kletz, Perrow and Turner showed from the late 1970s onwards that major accident processes often started from less noticeable events, which were later called 'early warnings' (Turner, 1978; Perrow, 1984; Kletz, 1988). It was Turner who postulated the Incubation Theory, showing various organisational failures leading to major accidents. Incubation referred to mechanisms in organisations which denied hazards and risks. In the late 1980s, Reason used the metaphor of resident pathogens for the denial of early warnings. These pathogens were later visualised as holes in barriers in his well-known Swiss Cheese metaphor (Reason, 1987, 1997). The origin of these holes lies in the decision-making processes of the so-called blunt-end managers and in the impact of these decisions on unsafe acts by front-line operators at the so-called sharp end. For the first time the Tripod model made the concept of latent factors operational with the Basic Risk Factors (Groeneweg, 1992). Thirty years after Turner's publication, the 'early warnings' were part of the so-called Management Delivery Systems of the Bowtie metaphor. These delivery systems were necessary actions of management to ensure the presence of barriers and to monitor their quality (Guillaume, 2011; Guldenmund et al., 2006).

When monitoring management delivery systems, it should be determined whether and to what extent they deliver such an output that (1) the barrier systems can be expected to be trustworthy, meaning reliable/available and effective (Schmitz et al., 2020b, 2021c) and (2) no latent, dangerous conditions are created. To assess the quality of the management delivery systems, both qualitative and quantitative monitoring can show their operation and efficiency (Schmitz et al., 2020c, 2021b).

1.1.5 The development of process safety performance indicators

Process safety indicators have been in the spotlight for some time. From a literature review at the start of this research, it was concluded that it seems too futuristic yet, to use indicators as a predictive signal for forthcoming major hazard accidents (Swuste et al., 2016). However, the chemical industry has been using (leading) process safety performance indicators for quite some time, using various guidelines from HSE (2006), CCPS (2010), Cefic (2016), OGP (2011) and ANSI/API (2010). In a special edition of

Safety Science (volume 47, issue 4, April 2009) these indicators have been placed more prominently on the science agenda.

Installations in production processes can, for various reasons, reach the border of their so-called (safety) design envelop. Based upon their craftsmanship, experienced operators will take action preventing a further development of major accident scenarios. Process safety indicators may act as an additional instrument, showing these changes in risk levels and their relationship with the effectiveness of the safety management system in place.

The safety metaphors, models, and theories discussed should be a basis for the search of indicators. These metaphors, models, and theories have been developed at different periods in time for different reasons and in different industries, explaining their different conclusions and insights. Both the bowtie and the Swiss cheese metaphor point in the direction of barriers and of management, or latent factors. In Rasmussen's 'drift to danger' model one of these latent factors refers to the impact of decisions and conflicts that may arise between safety on the one hand, and other company goals on the other hand, as well as with external actors competing the company's safety.

There are differences between the scientific and professional literature, regarding process safety indicators. Professional literature puts much emphasis on quantification of indicators used to monitor progression over time within a company or to compare results between companies, the so-called benchmark. In scientific literature, the nature of indicators and their impact on accident processes is discussed. Also, scientific literature questions a difference between leading and lagging indicators. The more general term of 'safety indicator' is recommended.

Safety metaphors, models, and theories can guide the formulation of process safety indicators, although there is a complicated metaphor/model/theory-indicator relationship. But scientific literature seems to agree on a scenario/barriers-indicator relation. One of the main conclusions from the scientific literature review was that safety indicators associated with the barrier's quality, scenarios, and the effects of decision-making appear to be the most obvious ones. They are not yet developed, hence this investigation is contributing to this topic. Logically, this will make safety indicators, process-specific and therefore company-specific. The challenge is to define indicators that provide insight into the quality of barriers and development of scenarios.

1.2 PROBLEM STATEMENT

1.2.1 The safety performance of OCI at Chemelot

OCI Nitrogen is part of OCI, one of the world's largest fertilizer manufacturers. OCI Nitrogen is located at Chemelot, a chemical industrial park in Geleen, The Netherlands. It operates two ammonia plants, two nitric acid and three fertilizer plants, one urea, and two melamine plants. The ammonia plants at Chemelot provide several OCI plants and site users with ammonia via a grid. In addition, it has an ammonia terminal in the Rotterdam harbour from which ammonia and aqueous ammonia are distributed by truck, rail and barge.

In 2015, several major process-related accidents occurred at some site users at Chemelot. OCI Nitrogen, one of Chemelot's larger site users, also faced several serious process safety related accidents, including some at its two ammonia plants. In some occurrences, the relevant ammonia production process had to be shut down immediately to prevent worse from happening. The increase in the frequency and severity of the accidents made the Chemelot Board decide to have an external investigation conducted. One of the conclusions was that process safety did not receive the necessary attention due to an increased focus on personal safety (Crisislab, 2016). Apparently, the focus on occupational safety was so high that the potential hazards of the plant and the chemical processes were not sufficiently highlighted. In other words, there was insufficient anticipation of "early warnings" from the chemical processes.

The deteriorated safety performance at Chemelot with several major accidents in 2015 and 2016 prompted the Dutch Safety Board to investigate the safety at Chemelot. Their report was published in 2018 (OVV, 2018) and revealed a number of shortcomings in process safety control. Among other things, the report recommends implementing a strategic approach to process safety management, improving visibility into process parameters, and assessing the risks associated with ageing designs. In addition, the installations must be adapted to the current standards of best engineering practises and be innovated using the latest knowledge. OCI's ammonia plants at Chemelot date back from 1969 and 1983 respectively.

1.2.2 Major accidents in the high-tech – high-hazard sector

The process industry belongs to the high-tech – high-hazard sector with processes which can release hazardous substances or energy leading to catastrophic consequences. Under the influence of market forces, cost reduction and process intensification become more important, and processes are scaled up to the limit of their design. When the technology of chemical installations becomes complex and the

process steps are tightly coupled, there is an increased risk of major hazard accidents. The complexity makes it difficult for employees to understand the (chemical) processes, while the tight coupling of the process steps does not give ample time to correct mistakes (Perrow, 1984).

In the late 1980s, improvements were sought in the way in which companies and organisations are organised and the concept of high reliability organisations was introduced (Weick, 1989; Roberts, 1989). High reliability organisations perform complex, inherently dangerous and technically advanced tasks surprisingly safely. There is redundancy in several aspects, organisational, technical and in decision-making. At the beginning of the millenium, resilience and resilience engineering make their appearance, where the focus is not on the dangers and mistakes of people, installations and systems, but on recovery options by improved ergonomic design and introduction of cognitive systems. These systems include a design which is adapted to what is important to an operator in the safe operation of the installation.

1.2.3 The use of early warnings and the efficiency of process safety performance indicators

Minor accidents and near incidents (sometimes also called 'near miss incidents') with a potential for major hazard accidents are useful "early warnings", as organisations can learn a considerable amount from them while the damage suffered is limited. However, it is better to prevent accidents and stop the development prematurely. In this thesis, the focus is on barrier management as a way to prevent (major hazard) accidents. Proper barrier management through effective organisational factors or management delivery systems guarantees the quality or trustworthiness of the barrier systems, being designed to stop the development of the accident processes. Organisational factors or management delivery systems are non-technical in nature and should be regarded as work processes and procedures in which human action or decision-making predominates.

By properly defining the right indicators, insight can be gained into the quality or trustworthiness of the barrier systems, as well as into the effectivity of the organisational factors or management delivery systems. Well-defined indicators do not only determine the urgency but also indicate what needs to be done.

1.3 RESEARCH QUESTION

OCI Nitrogen acknowledges that major process-related incidents can be very harmful and reflect badly on the company's standing. It is also recognised that there is

insufficient anticipation on 'early warnings', even though several incidents have been reported in recent years and followed up to prevent recurrence.

In anticipation of the results of the Crisislab investigation, OCI Nitrogen initiated its own research in 2015, in which management asked whether process safety could be measured and monitored. The aim is to prematurely detect enhanced process safety risks in their ammonia plants and take timely and appropriate measures to prevent major process safety incidents from happening. It was asked to focus on the ammonia plants as they comprise the highest risks in terms of process safety and security of supply. Although the outcome was not defined at the start, it was expected to be a set of process safety performance indicators providing information concerning the likelihood and development of potential major hazard accidents, taking ammonia plant #3 as a starting point.

At present, OCI's process safety incidents are registered using the Cefic guidance (Cefic, 2016). This monitoring only provides information in retrospect and the numbers only serve as lagging indicators. However, the purpose of this research is to develop an efficient approach to prevent process safety incidents in the process industry. It aims to systematically link (process safety) indicators to major hazard accident processes. The research question is formulated as follows:

> *To what extent can major hazard accidents in the process industry be prevented?*

At the start of this research, a complete overview of the possible major hazard accidents in ammonia plants was drawn up, obtained from the documentation of OCI and from a literature study into major hazard accidents in the international ammonia sector (Pattabathula et al., 2005, 2015). From a prior literature review (Swuste et al., 2016) it became clear that the key to answer the research question laid in the barrier systems and their management. Trustworthy barrier systems should be able to stop, delay and/or mitigate the development of accident processes, and efficient organisational factors or management delivery systems should guarantee their trustworthiness or quality. Indicators need to be defined that provide insight into the quality of the socio-technical barrier systems and the efficiency of the organisational factors or management delivery systems. To answer the research question, five sub research questions have been formulated:

1. How scientifically and practically sound are process safety indicators?
2. What are major process safety incidents?
3. How can the likelihood of major process safety incidents be monitored over time?

4. To what extent can indicators provide this information?
5. How valid is the concept of indicators for preventing major hazard accidents?

1.4 OUTLINE OF THE THESIS

Figure 1.2 shows an outline of the research with a breakdown of the research question into the five sub research questions. For each sub research question the published and submitted papers are given on the right-hand side as well as the chapters of this thesis in which these research subjects are described. Further details on each topic are given in the section below.

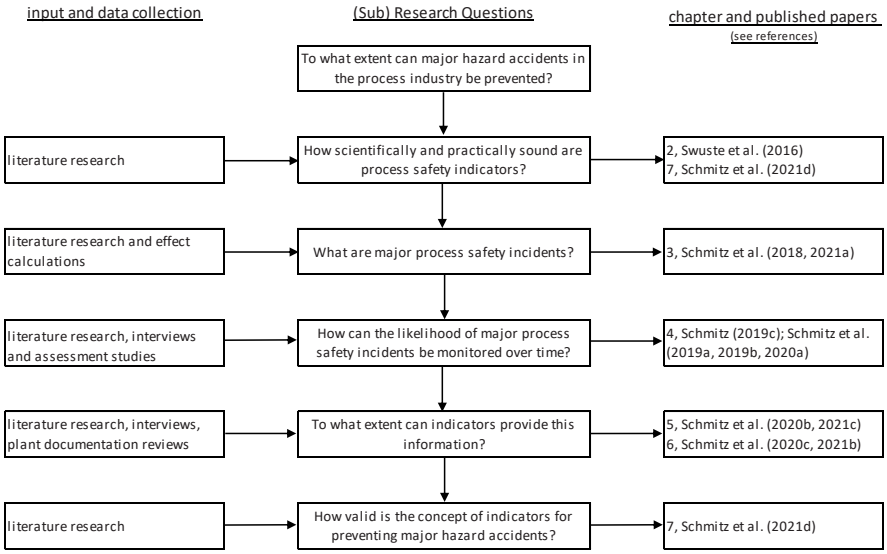

Fig. 1.2, outline of the research

Chapter 2 shows a review of literature which was conducted at the start of this doctoral research (Swuste et al., 2016). This review shows the latest developments and uses regarding process safety performance indicators and comprises an inventory of their definitions in both scientific and professional literature. It elaborates on the difference between leading and lagging indicators as well as on the purpose of safety indicators. Finally, it indicates the need for quantification, dominant in industry, if numbers do not contain information on quality.

Chapter 3 focusses on the consequences of major hazard accidents and provides guidance on how major hazard equipment can be selected. Calculations have been

conducted on the main equipment of ammonia plant #3 resulting from a defined loss of containment using DNV GL's Phast™ dispersion model (Schmitz et al., 2018, 2021a). The flammable and toxic effects resulted in a (relative) ranking of the most hazardous process equipment. The ranking is based on an adverse health impact on humans using the calculated effect distance as a starting point for a chance of death of at least 95%. The results from the effect calculations can be used for risk mapping of an entire chemical plant or can be applied in a layer of protection analysis (LOPA) to establish risk mitigation measures. In this research the ranking has been used for the selection of scenarios with the highest consequence potential.

Chapter 4 deals with mechanical integrity of process installations and demonstrates how barrier alarm management can be based on bowties (Schmitz, 2019c; Schmitz et al., 2019a, 2019b, 2020a). In this part of the research a method has been developed to monitor accident processes caused by mechanical integrity failures of static equipment like vessels, tanks and heat exchangers. A significant part of the mechanical integrity failure scenarios originates from material degradation and corrosion mechanisms which may develop over a relatively long time period, and may take months, years or even longer. Mechanical failure scenarios from two process units have been elaborated and visualised using a bowtie. It is shown that the monitoring of early warnings can provide information about the current development of mechanical failure scenarios. In addition, early warnings can be used to initiate inspections if there is a likelihood that the mechanical failure scenario has been activated. Considering the shift from breakdown maintenance to preventive and predictive maintenance and risk-based inspection (RBI), inspections based on early warnings could also be a new step in the field of maintenance efficiency.

Chapter 5 elaborates on the (preventive) barrier systems by looking at their status (Schmitz et al., 2020b, 2021c). Both the quality, expressed in reliability/availability and effectiveness, and the activation of the barrier system give an indication of the development of the accident scenarios and the likelihood of the central event. This likelihood is calculated as a loss of risk reduction compared to the original design. The calculation results in an indicator called "preventive barrier indicator", which should initiate further action. Based on an example, it is demonstrated which actions should be taken when an indicator changes its status and what the urgency of the actions is.
In chapter 6 organisational factors or management delivery systems are linked to accident processes and their barrier systems, using the bowtie metaphor (Schmitz et al., 2020c, 2021b). It is shown that organisational factors indirectly impact accident processes as they strongly influence the quality or trustworthiness of the barrier systems. By putting the right focus on organisational factors during audits or reviews, major accident processes get the attention they deserve, and the necessary actions

are taken at the right management level. Qualitative and quantitative monitoring of organisational factors can display their operation and efficiency. Using an example on retrospective data, it is demonstrated that information from organisational factors could have stopped the development of a near-accident prematurely. However, organisational factors should first be qualitatively assessed before they are quantitatively monitored. A quantitative assessment has been conducted for one of the management delivery systems so to provide an example of management indicators.

Chapter 7 validates the model by assessing the BP Texas City refinery incident in 2005 (Schmitz et al., 2021d). The bowtie metaphor is used to visually present the incident, showing the barrier system from three different perspectives. Firstly, the barrier system is discussed from its trustworthiness on the day of the incident, meaning from a general perspective of everyone present on site. Secondly, the barrier system is discussed from the view of the control room operator who came on site in the early morning, and started his shift without proper hand-over. And thirdly, the barrier system is reviewed from a design to current standards of best practise, meaning how it should have been designed. The risk reductions of these different views are calculated and compared to their original design. In addition, evidence and findings from the investigations have been categorised as flaws and allocated to the nine organisational factors used by OCI, assuming these organisational factors are generic and less company and scenario specific. These flaws may affect the barrier system's quality or trustworthiness, or may act as 'accident pathogens' (Reason, 1990) creating latent, dangerous conditions. This validation sheds new light on the monitoring of accident processes and the barrier management to control them, and demonstrates that the BP Texas City refinery incident could have been foreseen using preventive barrier indicators and monitoring organisational factors.

Chapter 8 answers the main and sub-research questions from this doctoral research. In addition, this chapter provides recommendations to prevent major hazard accidents in the process industry, the most important of which is related to barrier performance monitoring, using preventive barrier indicators and an audit technique focussed on organisational factors. In the last two paragraphs, the limitations of this doctoral research are discussed, and proposals are given for future research.

1.5 REFERENCES

ANSI/API. (2010). *Process Safety Performance Indicators for the Refining and Petrochemical Industries*, first edition ANSI/API RP 754.

Bellamy, L.J., Ale, B.J.M., Geyer, T.A.W., Goossens, L.H.J., Hale, A.R., Oh, J., Mud, M., Bloemhof, A., Papazoglou, I.A., Whiston, J.Y. (2007). Storybuilder – A tool for the analysis of accident reports. *Reliability Engineering and System Safety, 92*, 735–744. http://dx.doi.org/10.1016/j.ress.2006.02.010.

Centre for Chemical Process Safety (CCPS). (2010). *Guidance for Process Safety Metrics*. New Jersey, US: American Institute of Chemical Engineers.

Chevreau, F., Wybo, J., Cauchois, D. (2006). Organizing learning processes on risks by using the bow-tie representation. *Journal of Hazardous Materials 130*, 276–283. http://dx.doi.org/10.1016/j.jhazmat.2005.07.018.

Cockshot, J.E. (2005). Probability Bow-Ties – A Transparant Risk Management Tool. *Process Safety and Environmental Protection, 83*(B4), 307–316. http://dx.doi.org/10.1205/psep.04380.

Crisislab. (2016). *Toeval of structureel incidentalisme? Negen incidenten uit 2015 bij Chemelot nader beschouwd.* Retrieved from http://crisislab.nl/wordpress/wp-content/uploads/2016-06-07-rapport-Chemelot-def.pdf.

European Chemical Industry Council (Cefic). (2016). *Guidance for reporting on the ICCA globally harmonised process safety metric*. Retrieved from https://cefic.org/app/uploads/2019/02/Cefic-ICCA-Guidance-on-Process-Safety-Performance-Indicators.pdf.

Groeneweg, J. (1992). *Controlling the controllable, the management of safety.* Leiden, the Netherlands: DSWO Press.

Guillaume, E. (2011). *Identifying and responding to weak signals to improve learning from experiences in high-risk industry* (Doctoral's thesis). Retrieved from https://repository.tudelft.nl/islandora/object/uuid:f455e8a0-cce5-4a36-8a98-f83371dc2a2a.

Guldenmund, F., Hale, A., Goossens, L., Betten, J., Duijn, N., (2006). The development of an audit technique to assess the quality of safety barrier management. *Journal of Hazardous Materials 130*, 234–241. http://dx.doi.org/10.1016/j.jhazmat.2005.07.011.

Hale, A. (2002). Conditions of occurrence of major and minor accidents. Urban myths, deviations and accident scenario's. *Tijdschrift voor toegepaste Arbowetenschap, 2002*(3), 34–41.

Health and Safety Executives (HSE). (2006). *Developing process safety indicators, a step-by-step guide for the chemical and major hazards industries*. Retrieved from http://www.hse.gov.uk/pUbns/priced/hsg254.pdf.

International Association of Oil and Gas Producers (OGP). (2011). *Process safety, recommended practice on key performance indicators. Report nr 456*. Retrieved from https://www.iogp.org/bookstore/product/process-safety-recommended-practice-on-key-performance-indicators/.

Kletz, T. (1988). On the need to publish more case histories. *Plant/Operation Progress, 7*, 145–147.

Onderzoeksraad Voor Veiligheid (OVV). (2018). *Chemie in samenwerking – Veiligheid op het industriecomplex Chemelot*. Retrieved from https://www.onderzoeksraad.nl/nl/page/4707/chemie-in-samenwerking---veiligheid-op-het-industriecomplex-chemelot.

Pattabathula, V., Rani, B., Timbres, D. (2005). The AIChE Ammonia Safety Symposium 50 Years of Shared Experiences. *AIChE Technical Manual 2005, Safety in ammonia plants and related facilities Symposium, vol. 46*, 12–54.

Pattabathula, V., Richardson, J. (2015). Sixty Years of History of the AIChE Ammonia Safety Symposium. *AIChE Technical Manual 2015, Safety in ammonia plants and related facilities symposium, vol. 56*, 1–26.

Perrow, C. (1984). *Normal accidents. Living with high-risk technologies*. New York, US: Basic Books.

Reason, J. (1987). The Chernobyl errors. *Bulletin of the British Psychological Society, 40*, 201–206.

Reason, J. (1990). *Human error*. Cambridge, UK: University Press.

Reason, J. (1997). *Managing the risks of organizational accidents*. Abingdon, UK: Taylor & Francis.

Roberts, K. (1989). New challenges in organizational research: high reliability organizations. *Industrial Crisis Quarterly, 3*, 111–125.

Ruijter, A. de, & Guldenmund, F. (2016). The bowtie method: A review. *Safety Science, 88*, 211–218. http://dx.doi.org/10.1016/j.ssci.2016.03.001.

Schmitz, P., Swuste, P., Theunissen, J., Reniers, G., Decramer, G., & Uijterlinde, P. (2018). Een aanpak voor het bepalen van een realistische ranking van de gevaarlijkste procesonderdelen van het ammoniakproductieproces. *Tijdschrift voor toegepaste Arbowetenschap, 2018*(2), 42–56.

Schmitz, P., Swuste, P., Reniers, G., & Nunen van, K. (2019a). Mechanical integrity of process installations: an assessment based on bow-ties. *Chemical Engineering transactions, 77*, 97–102. https://doi.org/10.3303/CET1977017.

Schmitz, P., Swuste, P., Reniers, G., & Decramer, G. (2019b). Een aanpak voor het beoordelen van mechanische faalmechanismen van statische apparaten van het ammoniakproductieproces. *Tijdschrift voor toegepaste*

Arbowetenschap, 2019(2), 34–54.
Schmitz, P. (2019c). Mechanical Integrity of Process Installations: An Assessment Based on Bow-Ties. *Ammonia Technical Manual, 2019*, 17–28.
Schmitz, P., Swuste, P., Reniers, G. & Nunen van, K. (2020a). Mechanical integrity of process installations: Barrier alarm management based on bowties. *Process Safety and Environmental Protection, 138*, 139–147. https://doi.org/10.1016/j.psep.2020.03.009.
Schmitz, P., Swuste, P., Reniers, G., & Nunen van, K. (2020b). Een praktische aanpak voor het voorspellen van majeure ongevallen in de procesindustrie op basis van de barrière status op scenario niveau. *Tijdschrift voor toegepaste Arbowetenschap, 2020*(2), 47–66.
Schmitz, P., Swuste, P., Reniers, G., & Nunen van, K. (2020c). Een praktische, kwalitatieve aanpak voor het voorspellen van majeure ongevallen in de procesindustrie op basis van organisatorische factoren. *Tijdschrift voor toegepaste Arbowetenschap, 2020*(4), 124–134.
Schmitz, P., Reniers, G. & Swuste, P. (2021a). Determining a realistic ranking of the most dangerous process equipment of the ammonia production process: A practical approach. *Journal of Loss Prevention in the Process Industries, 70*, 104395. https://doi.org/10.1016/j.jlp.2021.104395.
Schmitz, P., Reniers, G., Swuste, P. & Nunen van, K. (2021b). Predicting major hazard accidents in the process industry based on organizational factors: a practical, qualitative approach. *Process Safety and Environmental Protection, 148*, 1268–1278. https://doi.org/10.1016/j.psep.2021.02.040.
Schmitz, P., Swuste, P., Reniers, G. & Nunen van, K. (2021c). Predicting major accidents in the process industry based on the barrier status at scenario level: a practical approach. *Journal of Loss Prevention in the Process Industries, 71*, 104519. https://doi.org/10.1016/j.jlp.2021.104519.
Schmitz, P., Reniers, G. & Swuste, P. (2021d). Predicting major hazard accidents by monitoring their barrier systems: a validation in retrospective. *Process Safety and Environmental Protection, 153*, 19–28. https://doi.org/10.1016/j.psep.2021.07.006.
Swuste, P., Theunissen, J., Schmitz, P., Reniers, G., Blokland, P. (2016). Process safety indicators, a review of literature. *Journal of Loss Prevention in the Process Industries, 40*, 162–173. http://dx.doi.org/10.1016/j.jlp.2015.12.020.
Turner, B. (1978). *Man-made disasters*. Oxford, UK: Butterworth-Heinemann.
Visser, K. (1998). Developments in HSE management in oil and gas exploration and production. In: *Safety Management, the challenge of change*, 43–65. Hale, A. & Baram, M. (Editors). Amsterdam, the Netherlands: Pergamon.
Weick, K. (1989). Mental models of high reliability systems. *Industrial Crisis Quarterly, 3*, 127–142.

2

PROCESS SAFETY INDICATORS, A REVIEW OF LITERATURE [2]

2 The Chapter is based on the paper: Swuste, P., Theunissen, J., Schmitz, P., Reniers, G., & Blokland, P. (2016). Process safety indicators, a review of literature. *Journal of Loss Prevention in the Process Industries, 40*, 162–173. http://dx.doi.org/10.1016/j.jlp.2015.12.020, and was formatted and edited for this thesis.

ABSTRACT

Indicators for process safety can provide insight into safety levels of a process or of a company, but it is clear that the 'silver bullet' has not yet been identified. In secondary literature a difference is made between leading and lagging safety indicators. Primary literature questions this distinction, as well as the quantification of safety indicators. Safety Indicators for management and organisation have an ambiguous relationship with latent errors and conditions, being mentioned over and over in retrospective safety analyses of major accidents. Indicators for occupational safety do not necessarily have a relationship with process safety. In addition, it can be expected that regulators of major hazard companies will ask to identify and implement both lagging and leading indicators, and anchor these indicators in a safety management system. Therefore, the subject 'safety indicators' will remain in the spotlight, at least in the time to come.

2.1 INTRODUCTION

In a competitive market environment, companies need to perform optimally if they want to survive in the long term and to be amongst the top of the sector. In the 1990s the term 'Performance Management' was introduced in management literature. Performance can be translated in this context as managing performance with the ultimate goal to perform better. First one thinks of financial and economic matters in terms of productivity, quality and environment. However, safety is also an important area for performance indicators. In practise, performance management becomes evident in the selection of representative indicators. These indicators reflect the status of the working environment and production processes realistically, and are used to obtain an optimal situation. A specific type of indicator for the safety domain is presented in this chapter, that is, the process safety indicator.

Literature on this topic sometimes refers to boilers of steam engines and trains. In the 19th century boilers exploded regularly, until it was understood that pressure, temperature, and strength-thickness of boiler walls were important technical indicators for these explosions (Figure 2.1).

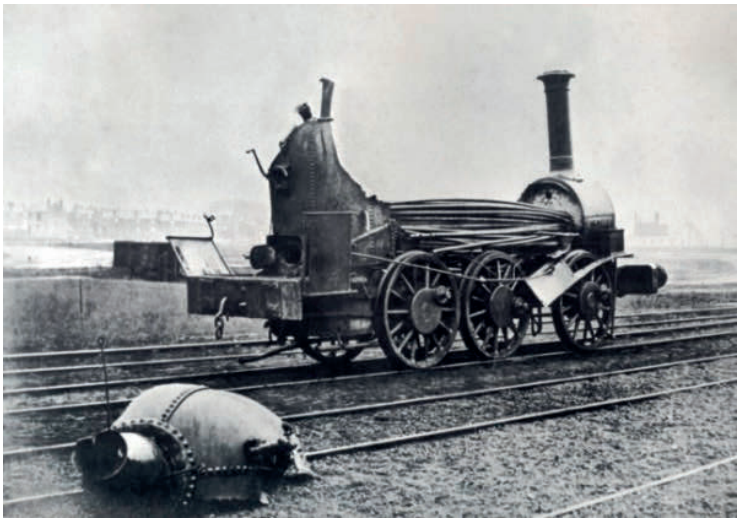

Fig. 2.1, exploded train steam boilers

The frequency of these explosions dropped dramatically after the introduction of safety valves. In the second half of the 19th century, with the Siemens Martin and the Bessemer process, steel boilers could be produced and the strength of the boiler wall was under control. (Rolt, 1955; Hijmans, 1963).

One hundred years later two publications on safety indicators for occupational safety appeared in America, one by Thomas Rockwell (1959) and one by William Tarrants (1963). Rockwell was looking for a measure of safety performance, and formulated requirements for indicators, which should be reliable, quantifiable and easy to understand. The indicator should also be stable, reproducible, sensitive to changes, and cost-effective. According to the author, accidents, with or without lost time did not meet these requirements. In line with a common safety metaphor of that time, Heinrich's domino's, unsafe acts were taken as starting point for indicators (Table 2.1) (Heinrich, 1941; see also Gulijk et al., 2015).

Table 2.1, unsafe acts as safety indicators (Rockwell, 1959)

1.	Working with loose tools underfoot
2.	Working without goggles when required
3.	Working under suspended loads
4.	Failure to use guards as provided
5.	Working in unsafe postures
6.	Wearing improper or loose clothing
7.	Use of shock tools with mushroomed heads
8.	Improvising unsafe ladders and platforms
9.	Running
10.	Misuse of air hose

Four years later, William Tarrants obtained his PhD at the University of New York on causes of accidents. Accidents and near-accidents were defined as unplanned events interfering with a job and not necessarily resulting in damage or adverse effects. This definition of accidents differed from Rockwell's focus on unsafe acts, and followed the insights after World War II of external factors as causes of occupational accidents, like for instance Winsemius (1951) (for an overview see Swuste et al., 2014). According to Tarrants, accidents were always preceded by errors or unsafe conditions, or a combination of errors and unsafe conditions (Tarrants 1963, 1970). He proposed to include incidents and accidents as a basis for indicators.

Various authors indicated that well into the 1990s, and even till now, one particular indicator had been the key safety indicator in process industry, the LTIF, the Lost Time Incident Frequency (Visser, 1995; Hale, 2009; Harms-Ringdahl, 2009; Pasman and Rogers, 2014; Leveson, 2015; Pasman, 2015). LTIF represents the number of days of absence to work due to an accident, per million hours worked. At that time, improvements in safety performances were equal to improvements in LTIF values. For example by Shell, between 1957 and 1994 the indicator dropped from about 20 to less than 2. The same focus on LTIF was present in many other companies in the process industry. Therefore many companies in the late 1990s promoted a zero accidents

approach. This appeared to be a miscalculation. Obviously, process disturbances accelerating major accident scenarios might also induce scenarios of occupational accidents, meaning that occupational safety and process safety can be intertwined. But, because of the accepted difference between the origin and pathways of major accidents and occupational accidents, LTIF figures have a poor correlation with indicators of process safety.

In the 1990s major accidents in high-risk industries reoccurred (Kletz 1993). Examples were: exploding tanks during welding, radioactive emissions, tripping reactors, overfilling storage tanks, failing pipelines, metal fractures by extreme temperature variations, etc. (Pigeon, and O'Leary, 2000; Hopkins, 2000; Körvers, 2004; Sonnemans and Körvers, 2006; Körvers and Sonnemans, 2008; Guillaume, 2011 Kidam and Hurme, 2013). Apparently, companies were, and still are, unable to recognise so-called 'weak signals' or process deviations with potentially major effects. From the second half of the 1970s these weak signals and deviations were divided in three groups, being technical/process engineering, organisational and human factors, including the quality of leadership (see Swuste et al., 2015). A comparison of major accidents worldwide between 1970-1980 and the first decade of this century showed no difference between these two periods. Apparently, recognition of weak signals at all levels of the organisation as well as by (sub) contractors work is still a problem, and managing disaster scenarios seems an extremely difficult topic (Table 2.2).

Table 2.2, major accidents, a déjà vu (Le Coze, 2013)

High-risk industries	Period	
	1790s-1980s	2000-2010
Nuclear	Chernobyl, 1986	Fukushima, 2011
Offshore drilling	Piper Alpha, 1988	Deepwater Horizon, 2010
Fuel storage	Port Eduard Heriot, 1987	Buncefield, 2005
Aerospace	Challenger, 1986	Columbia, 2013
Aviation	Tenerife, 1977	Rio Paris, 2009
Chemical - petrochemical	Flixborough, 1976, Bhopal, 1984	Toulouse, 2001, Texas City, 2005
Railway	Clapham Junction, 1987	Ladbroke grove, 1999
Maritime I	Zeebrugge, 1987	Costa Concordia, 2012
Maritime II	Exxon Valdez, 1987	Erika, 2003
Air Traffic Management	Zagreb, 1976	Umberlingen, 2002

Apart from not recognising these 'weak signals' as precursors to major accidents, other explanations are possible, like limited analysis capabilities of process safety techniques, safety management systems that do not have sufficient control over potentially hazardous processes, or limitations of existing safety metaphors, models and theories. However, these metaphors, models and theories are still too conceptual in nature to predict accidents and to deduce relevant safety indicators

(Knegtering and Pasman, 2009; Le Coze, 2013). Also, the increased numbers play a role. There are ever more nuclear plants operating, ever more process installations, air traffic increased substantially, etc. Furthermore, the vulnerability of these systems is enhanced by an increased complexity and dominant market forces. This latter influence leads to outsourcing, increased production efficiency and modular or fragmented organisational structures (Le Coze, 2014). Against this background, this chapter answers the following two questions:

> *Can process safety indicators provide insight and knowledge in levels of safety of processes or business, both current and future? And if so, which indicators are qualified?*

2.2 MATERIALS AND METHODS

In 2009 Andrew Hopkins and Andrew Hale issued a Safety Science special issue on process safety indicators (Hopkins and Hale, 2009), with nineteen different contributions from researchers, consultants and safety experts working in large companies. This issue was the start of this literature review, both in scientific and in professional literature. Scientific literature publishes results of original studies, and includes a formalised, anonymous referee system. Professional literature can be original work, or can report, summarise, comment on scientific literature, making it accessible to a wider audience than the scientific community and interested parties. Usually a referee system similar to scientific journals, is lacking. The scientific journals in this overview, presenting papers on this topic from North American, European, Central Asian. and Australian authors, were restricted to Ergonomics, Journal of Hazardous Materials, Journal of Industrial Engineering, Journal of Loss Prevention in the Process Industries, Journal of Management, Journal of Safety Research, Process Safety and Environmental Protection, Reliability Engineering and System Safety, Safety Science, and the Dutch Journal of Occupational Sciences

Professional literature was mainly restricted to reports of national organisations, like the American Baker report (2007), reports of the Centre for Chemical Process Safety (CCPS, 2010, 2011, 2014), British reports of the Control of Major Accident Hazards (COMAH, 2012), of the Health and Safety Executive (HSE, 2006), and of the UK Oil and Gas Industry, "step change in safety" (2006). Professional literature from international organisations comes from the International Organisation of Oil and Gas Producers (OGP, 2011), the Organisation for Economic Co-operation and Development (OECD, 2008a, b), the European Process Safety Centre (EPSC, 2012), and the European Chemical Industry Council (Cefic, 2011). Professional literature includes books on

management, as Olivier and Hove (2010), Heuverswyn and Reniers (2013), and Pasman (2015). For each type of information source following topics are covered in separate sections:

- safety expert metaphors, models and theories as a basis for process safety indicators;
- leading and lagging indicators;
- indicators of management and organisation.

2.3 PROCESS SAFETY INDICATORS IN THE SCIENTIFIC LITERATURE

2.3.1 Safety metaphors, models and theories as a basis for process safety indicators

The history of safety metaphors, models and theories are described in publications of Swuste and co-authors (2010, 2014, 2015) and Van Gulijk and co-authors (2015). This literature distinguishes between sequential, epidemiological and system-dynamic metaphors, models and theories. The domino metaphor Heinrich describes an occupational accident process as a linear sequence of events caused by human or technical errors. The technical errors related to exposure to mechanical, electrical or chemical hazards, like order and cleanliness, missing enclosures of rotating parts of machine, with irregular floors and unguarded holes and heights (Heinrich, 1941). Examples of human errors, according to Heinrich are far-out the most the dominant cause of accidents and shown in the aforementioned Table 2.1.

Next to immediate causes, epidemiological models and theories are emphasizing latent failures and conditions originating from the organisation and management of production. Turner (1976, 1978) was the first to highlight the concept of 'incubation period of major accidents', a period weak signals of serious accidents are undetected. The bowtie metaphor (Nielsen, 1971; Johnson, 1973; Wijk, 1977), the Tripod theory (Groeneweg, 1992; Wagenaar et al., 1994) and Swiss cheese metaphor (Reason, 1997) are also examples of this group, all used for the analysis of occupational and major accident. These metaphors and theories are still sequential in origin and focus on errors of so-called 'front line operators'. However, these errors are almost unavoidable in the context of the organisation in which they occur. The models are also called complex sequential, because several scenarios may lead to accidents.

System dynamic models and theories emerged in the 1980s. Like epidemiological models these models and theories are based on cybernetics, and provide explanations for major accidents. The 'normal accident' theory of Perrow (1984) is an example.

Not errors of front-line operators will determine risks of major accidents, but characteristics of production systems. Two determinants are leading; the degree of coupling of a production process and the complexity of interactions. The coupling reflects the presence or absence of buffers between system elements, and variability of the sequence of process steps. Interaction refers to physical or chemical transformations of processes and the presence or absence of so-called common-mode functions, where one system element will steer two or more following system elements. When coupling is tight, and interactions are complex serious accidents are inevitable and characterised as 'normal accidents'. Late 1980s the concept of 'high reliability organisation (HRO)' appeared. HRO's are organisations, which in terms of Perrow have complex interactions and tightly coupled processes. Air traffic control and flight manoeuvres on aircraft carriers are examples of HRO's where hardly any normal accident occurs. The core concept of a HRO is the reliability of processes and system characteristics, and of people who have to operate these processes (Rochlin, 1986; Weick, 1987; Roberts, 1988). HRO's are extremely effective 'learning organisations'. In the same period Wildavsky postulates the notion of resilience. Within organisational theory the concept of resilience has been known already for some time. Competition and the economic climate will create various setbacks and organisations have to respond effectively to these threats (Wildavsky, 1988).

Almost a generation later the HRO concept was introduced in Europe as 'resilience engineering' (Hollnagel et al., 2006). A final example of the system-dynamic group is the 'drift to danger' model of Rasmussen (1997), wherein the dynamic information flow between stakeholders can bring a system beyond its safety envelop. In the sections below a few examples of the metaphors, models and theories mentioned above will be discussed.

2.3.2 Leading and following indicators

A lot has been written on process safety indicators. However, there is little published empirical research on this topic. Often in the literature a distinction is made between so-called leading and lagging, providing insight into the level of safety of a system (Allford, 2009). However, safety is a dynamic condition of a system and is only measurable indirectly by proxies.

The bowtie metaphor illustrates the relationships between scenarios barriers and management factors. In the centre is a state where energy (hazard) has become uncontrollable, the central event, leading to consequences (Figure 2.2).

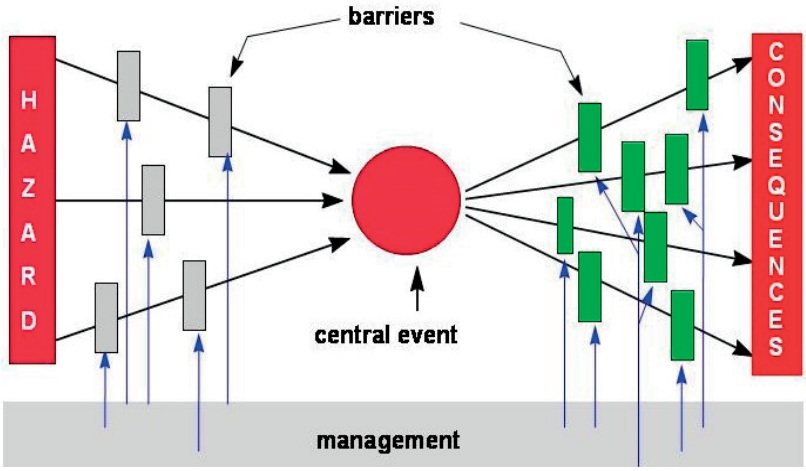

Fig. 2.2, the bowtie metaphor

The model has a hidden time factor. Management factors taking care of the acquisition, maintenance and, more generally, the quality of barriers, may undermine insidiously the effectiveness of these barriers over a long time period of time. If a hazard, energy, becomes uncontrollable and reaches the central event, scenarios reaching consequences usually will unroll very quickly. Scenarios left to the central event may take days, week, months, or even longer, while the ones at the right side develop in seconds, or even shorter. The distinction between leading and lagging indicators in this model is relatively easy. Leading indicators provide information on the left-hand side of the central event and the lagging indicators on the right-hand side. Thus, leading indicators basically are proxies for hazards, for barriers, for scenarios and management factors. Lagging indicators are proxies of the central event, of 'loss of control' and of consequences (Grabowski et al., 2007; Øien et al 2011a). According to this approach, leading indicators provide information on distortions of processes and thus on the stability of a system. Effects of interventions, which can be applied on both sides of the bowtie, will be reflected in these lagging indicators.

Indicators are seen as tools for safety monitoring of a system. In addition, leading indicators are associated with active and lagging indicators with a reactive safety monitoring (Hopkins, 2009). Hale (2009) has a different view: both leading and lagging indicators should provide information about the quality and effectiveness of barriers. From the list of definitions (Table 2.3), however, the distinction between the lead and lag is less obvious than one would expect.

Table 2.3, definitions of process safety indicators from scientific literature

References	Definitions
Rockwell, 1959; Tarrants, 1963	No definition of process safety indicators, only occupational safety
Martorell et al., 1999	The definition should contain; name, range, information required. The indicator is mathematical, and linked to the information necessary for the evaluation of the indicator
Leeuwen, 2006	Safety Performance Indicators are measurable units indicating processes/activities performances to manage these processes and activities
Sonnemans et al., 2006, 2010; Körver et al., 2008	Repeated disturbances, both technical, as organisational, as on human performance
Hopkins, 2007	Indicators show how process safety risks are managed
Grabowski et al., 2007; Duijm et al., 2008	Building blocks of accidents, conditions, events, preceding unwanted events, and are to some extent capable to predict these events
Erikson, 2009	Indicate the level of management of individual barriers to achieve goals
Dyreborg, 2009	A measure of root causes and safety performance of a production process
Hale, 2009	A measure of a safety level of a system, and if necessary responsible persons taking actions
Harms-Ringdahl. 2009	A measure providing feedback for improvements, if safety is sufficiently accomplished. An observable measure giving insight is a difficult to measure concept as safety
Kjellén, 2009	Predicts future changes in risk levels
Le Coze, 2009	A measure for disturbances, failures in a process system, and for interaction between those involved in safety management
Wreathall, 2009	A proxy for items from underlying safety models.
Knegtering et al., 2009; Zwetsloot, 2009	Lagging indicators, precursors of LOC incidents, leading indicators measure the quality of the management system
Vinnem, 2010	Based upon the prevention of incidents, near-incidents, barrier performances
Øien et al., 2011a	A measure for the status of risk reducing factors
Reiman, 2012	Provides an indication of the present state, or the development of organisations key functions, of processes, and the technical infrastructure of a system
Hassan et al., 2012	Risk based indicators measure the integrity of resources, operational, mechanical, human
Khawaji, 2012	Detection of failures in hazard analysis, design, non-adequate controls, and cause by extreme conditions

The confusion goes even further when relationships are discussed between these two types of indicators (Harms-Ringdahl, 2009). If there is any difference, one would expect a logical connection between the two. This has not been demonstrated yet (Mearns, 2009). Such a relationship is expected from the bowtie metaphor. After all, a scenario left of the central event, continues its way to the right. A number of authors do not distinguish between leading and lagging anymore, because of this ambiguity a more general terminology is used, like key indicator, safety performance indicator, or key performance indicators (Guldenmund and Booster 2005; Saqib and Siddiqi, 2008; Eriksen, 2009; Mearns, 2009; Grote, 2009; Øien et al., 2011a). Even with barriers, there is some confusion. This is evident from the various terms in use, like defence, protection layer, safety critical element, safety function. It is not clear whether these

terms are synonyms or that different authors assign different meanings to the terms (Sklet, 2006). Proposals were suggested to create some order in this confusion. For example, research from the Technical University of Eindhoven in the Netherlands suggests a division in four different types (Körvers, 2004; Körvers and Sonnemans, 2008; Sonnemans et al., 2010):

1) safety-critical deviations from normal procedure - leaks, accidents;
2) monitoring - inspections aimed at human actions, observations, monitoring the effectiveness of safety barriers;
3) safety audits, organisational risk factors, training, safety inspection of equipment;
4) culture index - attitude survey, questionnaire.

Another classification from Pasman and Rogers (2014) makes an explicit reference to 'loss of containment (LOC)'. Concerning the process industry, LOC is elementary. This results in lagging indicators. Leaks are observable, and countable. LOC as lagging indicator emerged first; leading indicators are less easy to define and are of a later date:

1) mechanical integrity - inspections, audits; quality and unresolved action points;
2) settled action points - from process hazard analysis (PHA), from investigation to near misses;
3) training, competence - quality training, test results, number of trained employees.

These formats differ, but have in common that both indicators are related to technology, as well as management and organisational activities. The latter part will be covered in the next section.

Gradually it becomes clear that process safety indicators is a complicated topic (Hassan and Khan, 2012). Failing management factors and thereby failing barriers are scenario-dependent (Zemering and Swuste, 2005; Bellamy, 2009; Dryeborg, 2009; Kjellén, 2009; Le Coze, 2009) and scenarios, appearing in the bowtie metaphor as straight lines, can in reality develop rather capriciously. Serious accidents are never the result of one assignable error or malfunction, but of a pattern of events which have their roots in the technology, the organisational and management domain. It is questionable whether such a pattern can be caught by one or a limited number of indicators (Körver and Sonnemans, 2008; Grote, 2009; Knegtering and Pasman, 2009). Latent failures and conditions from epidemiological models are failures and conditions which are present but which reveal themselves only when they are addressed during an accident scenario (Figure 2.3) (Reason, 1990a; b; Wagenaar et al., 1994).

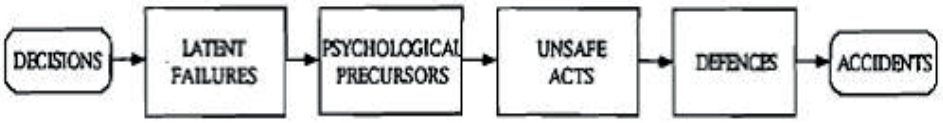

Fig. 2.3, general scheme of an accident scenario (Wagenaar et.al., 1994)

Figure 2.3 is a model for major accidents in the oil industry and it looks like a simplified version of the bowtie metaphor, which includes psychological factors, like the 'psychological precursors' and the 'unsafe acts'. This model has subsequently led to the well-known Swiss cheese metaphor (Figure 2.4).

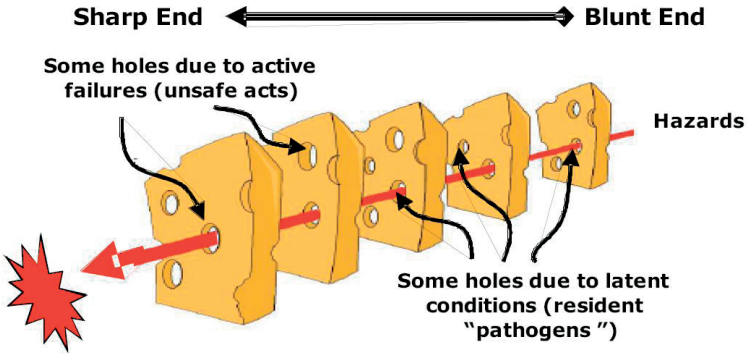

Fig. 2.4, Swiss cheese metaphor (Reason, 1997; Qureshi, 2007)

Latent conditions and errors are detailed in the Tripod theory as the so-called basis risk factors (Groeneweg, 1992). These basic risk factors related both to technology (design, materials), as to management (maintenance policy, procedures, communication, training, conflict management goals, protective equipment), as to the organisation (organisational structure, environmental conditions, order and cleanliness). Logically indicators should provide information about the system elements from Figure 2.3, the holes in cheese slices of Figure 2.4, and on the quality of the basic risk factors. However, both figures also show how complicated it is to distinguish between leading and following indicators. This is only reinforced by system-dynamic accident models. The normal accident theory may lead to indicators of system characteristics, the degree of coupling and complexity. These predict the occurrence of major accidents and thereby leading.

Rasmussen's model (1997), also an example of a system dynamics model, is based on an extensive stakeholder analysis and resulted in his accident analysis method Accimap.

This model shows the relative influence of different groups, information, interaction and conflicts between these groups. Rasmussen emphasises this information and the dynamics of decision making which will affect process safety and that can bring the system into a state where it can get out of his so-called safety envelope (Figure 2.5).

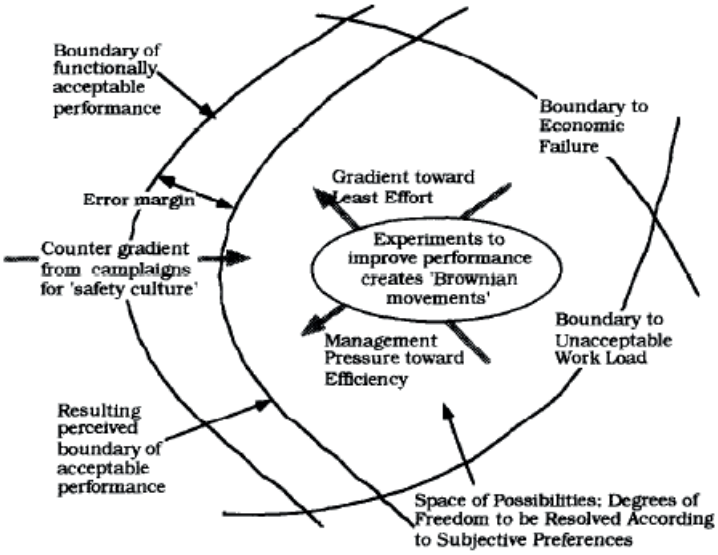

Fig. 2.5, operational boundaries of a safety envelop, 'drift to danger' (Rasmussen. 1997)

This safety envelope is a state in which a system is operating safely. A production process, the ellipse in the centre of Figure 2.5, has a normal variation caused by, for example, physical parameters as temperature and by variations in the quality of raw materials and intermediate products. Rasmussen compared these variations with the Brownian movement of gas molecules. The Brownian motion remains within the boundaries of the safety envelope. Two gradients can bring a production process to the limits of the safety envelope and makes the system unstable; the gradient towards least effort and pressure from management to produce as cost-efficiently as possible. These boundaries, the arcs left and right in the figure are, according to Rasmussen, not universal but company-specific and can be starting points for process safety indicators, providing information about the extent to which boundaries are reached. However, the pace and the dynamics of technological change and market-driven changes to a faster, cheaper and more efficient production, are much greater than the rate of changes of management structures and legislation. This pushes the drift to danger. Therefore, investigation and analysis of serious accidents cannot be separated

from research to decision making, which integrates the knowledge and the context of this decision. This approach provides risk management with an understanding of the dynamics of the safety of processes and the need for stakeholders to determine boundaries and to gain insight through feedback control, when a state of drift to danger will occur (Svedung and Rasmussen, 2002).

Serious accidents are seen as a result of external disturbances in combination with dysfunctional interactions. Thereby safety is defined as a control problem. As with drift to danger, serious accidents will develop from hazards, as safety limits of the system components, when control structures will not function properly, and process models do not match the actual state of the system. The discussion of metaphors, models and theories shows that the formulation of relevant indicators is not an easy one. Table 2.4 provides an overview of process safety indicators, being mentioned in scientific articles discussed.

Table 2.4, process safety indicators from scientific literature

Indicators	References
Process safety	
Alarms, failures, numbers per time period	Martorell '99, Hopkins '09, Bandari '13
Exposure to dangerous substances/activities	Martorell '99, Sklet '06, Kampen '13
Process deviations, number	Sonnemans '06, Körvers '08, Hale '09, Kongvik '10, Øien '11ab, Reiman '12, Bandari '13
State of safety, unwanted	Grabowski '07, Bandari '13
Incidents, number	Körvers '08, Kampen '13
Leakages, number, amount	Vinnem '06, Körvers ´08, Harms '09
Barriers quality	Bellamy '09, Dryeborg '09, Hale '09, Reiman '12, Bandari '13
Fires, explosions, number, costs	Vinnem '06, '10, Bandari '13
Loss of containment, amount, number	Webb '09, Bandari '13
Process design, failures, maintenance, quality control, failures	Harms-Ringdahl '09
Tests, failures	Hopkins '09
Safety system, frequency of activation	Kampen '13, Bandari '13
Inherent safe installations, number	Kampen '13

2.3.3 Indicators for management and organisation

Results of audits and feedback from employees are important information sources for managers to identify signs and indications of accidents (Grabowski 2007; Duijm et al., 2008). Whether these two sources provide enough background for indicators is a question. Similar to process safety, also management and organisational indicators are generally formulated in the scientific literature (Table 2.5).

Table 2.5, management and organisational indicators in scientific literature

Indicators	References
Management and organisation	
Behaviour, unsafe situations, positive feedback	Rockwell 1959, Reiman 2012
Safety management, activities	Martorell 1999, Reiman 2012, Bandari 2013
Safety culture, climate, index	Körvers 2008, Dryeborg 2009, Harms 2009, Reiman 2012
Audits, number performed, settled action points	Basso 2004, Körvers 2008, Kampen 2013, Reiman 2012
Inspections, settled action points	Körvers 2008 Hopkins 2009, Webb 2009, Reiman 2012
Safety observations, number	Körvers 2008, Hale 2009, Kampen 2013, Reiman 2012
Safety procedures, accessibility	Körvers 2008, Kongvik 2010, Bandari 2013
Safety training, programme, frequency	Basso, 2004, Körvers 2008, Webb 2009, Kongvik 2010, Reiman 2012, Kampen 2013, Pasman 2014
Toolbox meetings, frequency, presence	Hale 2009
Safety commissions, settled action points	Harms 2009
Work procedures, correctly followed, transfer of shifts	Basso 2004, Kongvik 2010, Bandari 2013
Safety stops during enhanced risks	Kongvik 2010, Bandari 2013
Human performance meetings, number	Øien 2011b, Reiman 2012
Work permits, transfer, correct performance	Øien 2011b, Webb 2009
Contractor-subcontractor, selection, training	Reiman 2012
Decisions, safety arguments	Reiman 2012
Competence profiles, training	Reiman 2012
Manning, shift size	Reiman 2012
Contingency plan, training	Reiman 2012
Risk assessment during process changes (MoC)	Reiman 2012
Safety analyses, number, trends	Reiman 2012, Pasman 2014
Safety documentation	Reiman 2012
Safety initiatives personnel	Reiman 2012

Some indicators are linked to interventions, as can be expected from management indicators. However, when indicators are quantified there seems hardly any relationship with management quality and thus with safety.

Interestingly, indicators seem to be mainly based on experience from companies or on common sense. Hardly any empirical research was found in the literature, apart from a casuistic study of the Technical University Eindhoven (Körvers, 2004; Sonnemans et al., 2010), and a survey of TNO among members of the Dutch Society of Safety Science - NVVK investigating the member's experience with safety indicators (Kampen et al., 2013). The study of Körvers and colleagues was conducted at three high-hazard industries in the coating sector, the plastic granules sector and the production of pharmaceutical ingredients. In their study, repeated breakdowns and defects in production were coupled with a top 20 of dominant scenarios with safety consequences. Latent factors were examined for these repeated breakdowns, as well as the quality of relevant barriers. The study to these indicators proved to be successful and the research yielded some interesting observations. Process failures were frequently preceded by equipment failure or by other disturbances. Signals were not recognised as a possible early stage of a process accident scenario, if the

immediate consequence was not serious enough. On the other hand, information on non-functional barriers could be known within the company, but was not used from a safety perspective due to a lack of time and lack of effective communication between different departments. Thirdly, it appeared that safety departments of the companies surveyed were hardly involved in the daily production and therefore were not sufficiently aware of the common process hazards and risks. Finally, companies were not aware of the impact of decisions of the top and middle management on barrier quality.

The NVVK survey was conducted among 172 members of the Dutch Society, mainly working in larger process industries. Companies were using in total 15-37 different indicators, which almost entirely were related to occupational safety. Companies with good scores on occupational safety used more complex indicators for the state of their primary process. But at the same time results were hardly used to improve the organisation. Also, no relation was found between indicators and self-reported 'loss of containment' at these companies. The most commonly used indicators were the lost-time accidents, unsettled issues of safety reports, safety training of workers and near-accidents with potentially serious consequences.

2.3.4 Occupational safety and process safety

Many people will intuitively see a difference between occupational safety, with a great variety of types of hazards and process safety, with a focus on 'loss of containment'. The size of the possible consequences plays a role. According to Kjellén (2009), for indicators this difference might be much smaller, seen from a 'hazard-barrier-target' - energy model perspective. However, further research should shed a light on possible overlap between these two types of safety indicators. Companies have a need for simple, understandable and communicable indicators and lost workday as an indicator meets this demand (Table 2.6).

Table 2.6, indicators for occupational safety in the scientific literature

Indicators	References
Occupational safety	
Near accidents, number	Tarrants 1963
Accidents with/without lost days, number	Martorell 1999, Grabowski 2007, Webb 2009, Kampen 2013
Order and cleanliness	Kampen 2013

2.4 PROCESS SAFETY INDICATORS FROM THE PROFESSIONAL LITERATURE

2.4.1 Safety metaphors, models and theories as a basis for process safety indicators

The importance of process safety indicators for the process industry is evident in the list of its definitions (Table 2.7). These definitions fit well with those found in scientific literature (Table 2.3).

Table 2.7, definitions of process safety indicators in the professional literature

Definitions	References
Leading and lagging system guards are a double assurance the risk control system is operating as intended, or giving warnings of problems in development	HSE, 2006
Give results of a risk control system (lagging) or (mal)functioning of critical elements of risk control system (leading).	HSE, 2006
Provide information on outcomes of actions (lagging) or the current situation, affecting future performances (leading).	UK Oil & Gas, 2006
Allow organisations to verify if risk control measures taken are still active	OECD, 2008
Performance indicators quantify objectives set and measure performances, enabling to manage, improve, and being accountable.	Olivier et al., 2010
A standard for measuring the efficiency and performance of process safety	CCPS, 2010
An indicator gives information, effective in improving safety	ANSI/API, 2010
Indicators are standards of performance and effectiveness of the process safety management system, and associated elements and activities are tracked.	CCPS, 2010
Serious safety incidents (lagging) or performance of parts of the safety management system (leading).	CCPS, 2011
Measurement, analysis of incidents in the area of process safety and facilitate benchmarking	Cefic, 2011
Information indicating a company controls its main risks, equipment integrity and the level of safety of the (production)process.	OGP, 2011
Indicators are the measured variables, linked to safety critical measures	EPSC, 2012
Provides information on the safety situation	Bellamy et al., 2012
A key factor for the success of process safety	Bhandari et al., 2013
An indicator is representative to achieve the possibility/capacity of a result suggested	Heuverswyn et al.,2013

Still there are differences. A focus on improving and benchmarking is prominent, while scientific literature speaks about barriers and safety levels. In the professional literature, three metaphors are frequently referred to; Heinrich's pyramid metaphor (ANSI/API RP754 2010; CCPS 2010; OGP 2011), Reason's Swiss cheese metaphor (ANSI / API RP754 2010; CCPS 2010; HSE 2006; OGP 2011; UK Oil & Gas Industry, 2006; Hopkins, 2007), and the bowtie metaphor(CCPS 2010; OGP 2011).

Step change in safety, a publication of the British consortium of companies from the oil and gas (UK Oil and Gas Industry 2006), has modified Shell's Hearts and Minds metaphor (Parker et al., 2006), and relates specific leading indicators to three levels of their 'safety maturity model' (Figure 2.6).

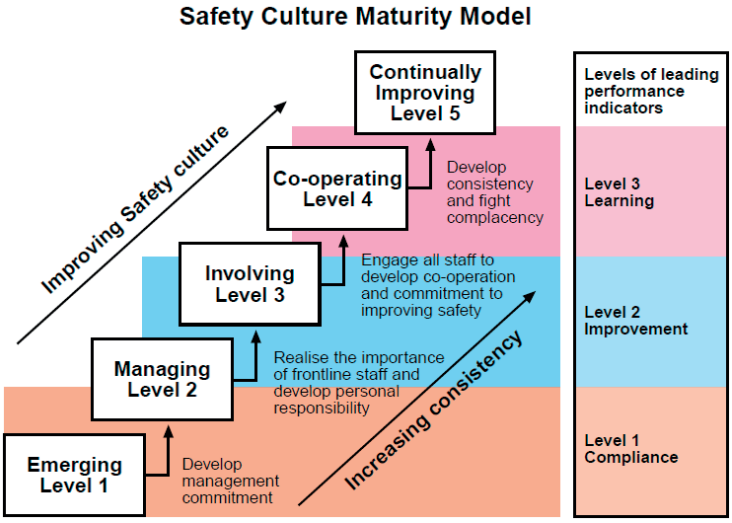

Fig. 2.6, HSE Safety Culture Maturity Model

An initiative of Dutch companies working with large-scale hazardous materials is Veiligheid Voorop (Safety First) (NVO-NCW, 2011). In its documentation the development of process safety indicators is explicitly mentioned, thereby following the coming guidelines of Seveso III. Apart from a scientific focus on process safety indicators, also public authorities (regulators), companies and business organisations support these publications, but stress the importance of experience gained and immediate practical application of results.

2.4.2 Leading and lagging indicators

Prominent organisations on process safety published reports on this topic (HSE, 2006; OECD 2008; ANSI/API, 2010; OGP, 2011; CCPS, 2011; Cefic, 2011; UK Oil and Gas, 2012), and many conferences were organised around this theme by the European Chemical Industry Council and the European Process Safety Centre (Cefic-EPSC, 2012). The BP Texas City refinery disaster served as a catalyst for these reports and conferences. The research team of this major accident (Baker Report, 2007) showed clear deficiencies in process safety management, a conclusion which was equally applicable to other refineries and chemical companies. National and international safety committees and organisations supported this comment, like the British Health and Safety Executive (HSE), the US Chemical Safety and Hazard Investigation Board (CSB). The American Petroleum Industry (API), the Centre for Chemical Process Safety (CCPS) and the International Association of Oil and Gas Producers (OGP) subsequently developed guidelines for key performance indicators (KPIs) to reduce and eliminate process risks (Table 2.8).

Table 2.8, process safety indicators in professional literature

Indicators	References
Process safety	
Alarms, failures, number per time period	OGP 2011, OGP 2008
Exposure dangerous materials/activities	UK Oil & Gas 2006
State of safety, unwanted	OECD 2008
Incidents, number	CCPS 2011
Leakage, number, amount	CCPS 2011, ANSI_API 2010, Cefic 2011
Fires, explosions, number, costs	OGP 2011, HSE 2006, CCPS 2011, ANSI_API 2010, Cefic 2011
Loss of containment, amount, number	OGP 2011, HSE 2006, CCPS 2011, ANSI_API 2010, Cefic 2011
Process design, failures	UK Oil & Gas 2006, OGP 2011, OGP 2008, HSE 2006, OECD
Maintenance, quality control, failures	2008, OGP 2011, OGP 2008, OECD 2008,
Tests, failures	OGP 2011, HSE 2006
Safety system, frequency of activation	OGP 2011, ANSI_API 2010
Installations inherent safe, number	OECD 2008
Process disturbances outside design envelop, number	EPSC 2012, ANSI_API 2010
Safety system, frequency of failure	HSE 2006, ANSI_API 2010
Storage dangerous materials, amounts	OECD 2008

HSE provides guidelines for management and safety experts, based on the practise of the British chemical industry for developing, selecting and implementing process indicators for major process risks, including a road map. Important is the timely discovery of weaknesses (leading) in the risk management system, and not so much failure monitoring (lagging). The process safety management system should first identify major accident scenarios, then barriers are selected for each scenario, the so-called risk control systems (RCS). Finally each critical RCS is linked to lagging, and leading indicators, providing dual assurance. At the end of 2015, high-hazard-high-risk companies should measure their process safety performance, using leading and lagging indicators. This is the strategic goal of the British COMAH (Control of Major Accident Hazards) Competent Authority, which is similar to the Dutch BRZO Competent Authority.

The Organisation for Economic Co-operation and Development (OECD) published the 2008 Guide on Developing Safety Performance Indicators in 2 versions: one for industry and one for public authorities and civic associations. These documents, developed by a group of experts from the public and private sectors, are based on 'best practises' of measuring safety performance. A distinction is made between:

- Result indicators, which are reactive, lagging, and either specify a desired result is achieved but not why, and;
- Activities indicators, proactive, leading, identifying a specific safety performance relative to a benchmark (tolerance level) and can indicate why an outcome is reached.

It is stated that safety performance indicators could indicate if critical elements of safety controls are functioning adequately before catastrophic failure occurs. Both outcome indicators and activity indicators can be linked to the various elements of

the safety management systems in companies, or to various groups concerned (public authorities, aid-giving organisations such as police, fire, etc. and citizen groups).

The American ANSI/API Recommended Practice 754 is particularly aimed at refineries and chemical industry, providing precise definitions and an indicator classification for benchmark purposes. A distinction is made between 4 different types of process safety events (PSEs) which, in order of decreasing severity, are referred to as tier-1 to tier-4, and are linked to different kind of events, and corresponding indicators (Figure 2.7).

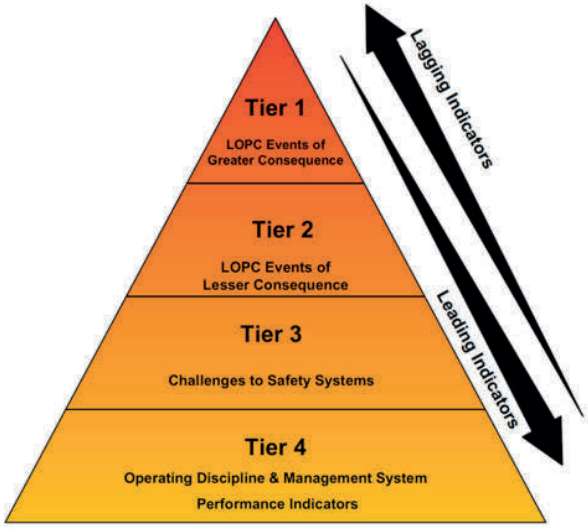

Fig. 2.7, process Safety Indicator Pyramid (ANSI/API 2010)

Tier-2 is defined as a near-miss event, as an indication of a barrier weakness, which can be seen as leading. Statistics show a much higher frequency of Tier-4 events, than tier-1, therefor the different process safety indicators are shown schematically as a pyramid.

The Centre for Chemical Process Safety, gives further details on ANSI/API RP754, including examples of leading indicators and associated quantifiable parameters. Identified risks, accident scenarios and related barriers are the starting point for indicators. The process safety management system is starting point for leading and lagging indicators of the 'risk-based process safety overview' (CCPS, 2014). Again, quantifiable parameters are suggested, coming from a slogan broadly accepted in industry 'you cannot manage what you do not measure'.

The International Association of Oil & Gas Producers OGP issued OGP report no. 456, Recommended Practice on Key Performance Indicators, following a previous OGP report no. 415 on Asset Integrity, and refers to both HSE guidelines and the ANSI/ API RP754. OGP links leading indicator to preventive barriers and lagging indicator to de-escalating barriers. For so-called critical barriers a combination of a leading and a lagging indicator is suggested to test the strength of the barrier. A subsequent indicator could detect barriers defects, as advised by the HSE. However, the distinction between leading and lagging, is, according to the report, not always clear.

Leading indicators in Step Change in Safety of the British Oil and Gas Industry are the result of a comprehensive analysis of current practises in their oil and gas industry. While lagging indicators provide information on the outcome of actions, leading indicators detect a present situation which could have an effect on future results. Depending on the status of safety culture in an organisation, three types of leading indicators are identified: 1) compliance, 2) improving the performance, 3) learning organisation. The choice of the indicator should fit the organisation. Examples of leading indicators for all three levels are given. Step Change in Safety also instils conditions for adequate, effective and usable safety indicators: they need to be accessible and linked to the safety management system in charge, they need to be objective and measurable and lead to control actions. Indicators are only effective when they are part of a continuous learning process of a company. Results from indicators should not stand alone.

Finally, Cefic, the European Chemical Industry Council, issued his Guidance on Process Safety Performance Indicators, for benchmarking purposes, and pays no attention to leading indicators.

Next to the distinction between leading and lagging, other indicator classifications are mentioned in the professional literature. One is based upon the so-called ‘performance pyramid’, including a hierarchy with result-indicators for the outcome of the safety management system as the highest level. At an intermediate level, system-indicators measure the efforts the system, and operational-indicators are defined at the grassroots level which measure concrete achievements in the organisation (Olivier Van Hove, 2010). Also Heuverswyn and Reniers (2012) are using a trichotomy of indicators. Management-indicators show whether conditions are present to achieve desired goals. Process-indicators show whether assumed objectives are feasible, and whether the effort as planned was performed correctly. Finally, result-indicators are proxies for performance, what has been achieved given a pre-set goal.

2.4.3 Indicators for management and organisation

Table 2.9 represents organisational and managerial indicators found in the professional

literature. As with the same item in scientific literature (Table 2.5), and with process indicators from both sources in Table 2.4 and 2.8, the resemblance is striking.

Table 2.9, management and organisation indicators in professional literature

Indicators	References
Management and organisation	
Behaviour, unsafe situations, positive feedback	OECD '08
Safety management activities	UK Oil & Gas '06, OECD '08
safety culture, climate, index	OECD '08
Audits, number performed, settled action points	UK Oil & Gas '06, OECD '08, CCPS '11, ANSI_API '10
Inspections, number performed	HSE '06, UK Oil & Gas '06, CCPS '11, ANSI_API '10
Inspections, settled action points	EPSC '12, OGP '11, CCPS '11, ANSI_API '10
Safety observations, number	UK Oil & Gas '06, OECD '08
Safety procedures, accessibility	OECD '08
Safety training, programme, frequency	OGP '11, OECD '08, CCPS '11
Toolbox meetings, frequency, presence	OGP '11
Work procedures, correctly followed, transfer of shifts	OGP '11, HSE 2006, CCPS '11
Human performance meetings, number	OECD '08
Work permits, transfer, correct performance	UK Oil & Gas '06, OGP '11, OGP '08, OECD '08, CCPS '11, ANSI_API '10
(Sub)contractors, choice, training	OGP '11, OECD '08
Competence profiles, training	UK Oil & Gas '06, OGP '11, OGP '08, HSE '06, OECD '08, CCPS '11, ANSI_API '10
Manning, shift size	OECD '08
Contingency plan, training	OECD '08, ANSI_API '10
Risk assessment during process changes (MoC)	OGP '11, OGP '08, HSE '06, OECD '08, CCPS '11,
Temporarily shutting down safety systems	ANSI_API '10 EPSC '12, CCPS '11
Inspection programme installation	EPSC '12, OGP '11
Safety analyses, number, trends	UK Oil & Gas '06
Safety meetings personnel & management	UK Oil & Gas '06, OGP '11
Safety documentation	OECD '08, SCiS '12
Safety studies, number	UK Oil & Gas '06, OGP '11, OECD '08, ANSI_API '10
Operational procedures, correctness/availability	OGP '11, OGP '08, HSE '06, CCPS '11, ANSI_API '10
Emergency procedures, correctness/availability	HSE '06, OECD '08, CCPS '11, ANSI_API '10
Law offences, deviation of standard	UK Oil & Gas '06, OGP '11, HSE '06, OECD '08
Communication during normal operation and emergencies	HSE '06, OECD '08
External communication and co-operation	OECD '08
Hazard identification and risk analysis	OECD '08
Product safety	OECD '08
Reports/studies of (near) accidents	OECD '08
Safety culture, number/frequency of evaluations	CCPS '11
Safety policy published and communicated	UK Oil & Gas '06
Suggestions for safety improvements, number	UK Oil & Gas '06

2.4.4 Occupational safety and process safety indicators

In literature a clear distinction is made between occupational and process safety. Their origin is different; their scenarios, barriers, and consequences. But recent research shed another light on this matter, showing that minor, more frequent, accidents can provide information about the major or catastrophic accidents. This relationship,

however, is limited to the same risk category (Bellamy, 2015), suggesting that both types of accidents partly follow the same scenario pathway.

2.5 DISCUSSION AND CONCLUSION

Installations in production processes can, for various reasons reach the border of their so-called (safety) design envelop. Based upon their craftsmanship, experienced operators will take action preventing a further development of major accident scenarios. Process safety indicators may act as an additional instrument, showing these changes in risk levels and their relation with the effectiveness of the safety management system in place. But it seems too futuristic yet, to use indicators as a predictive signal for forthcoming major accidents. This reflects the attention on the topic, only the last eight or nine years process safety indicators are a topic in the scientific and professional press. Ten years is not a very long time period and not surprisingly the topic of process safety indicators is still under discussion. It is also reflected in its definitions. The tables show a variety of definitions, both within the scientific and within the professional literature.

The safety metaphors, models, theories as well as the management delivery systems discussed should be a basis for the search for indicators. These metaphors, models, and theories have been developed at different periods in time for different reasons and in different industries, explaining their different conclusions and insights. Both the bowtie, and the Swiss cheese metaphor point in the direction of barriers and of management, or latent factors. In the drift to danger model one of these latent factors refers to the impact of decisions and conflicts that may arise between safety, and other company goals. Decision making is broadly defined and includes both decisions on the scope and efficiency of the production, on maintenance and turn-arounds, as on the quality of outsourcing and the impact of laws and regulations.

The list of definitions shows quite some similarity between the definitions in the scientific and professional literature. Definitions of research groups remain closer to the safety metaphors and models by explicitly referring to (repeated) process disturbances, barrier quality, root causes and precursors of loss of containment. The definitions from the professional literature are closer to regulation requirements, to practical applicability, and to effectiveness of process safety management. Regularly an explicit distinction is made between leading and lagging safety indicators. The American ANSI/API thereby introduced their four-level pyramid. Distinction between the different levels is not very clear and the pyramid seems to be dictated more by legal than by theoretical arguments.

The scientific literature questions a difference between leading and lagging. The more general term of safety indicator is recommended. A final difference between the academic literature and the more practically oriented professional literature is the function of safety indicators. In the professional literature indicators primarily seem to have a descriptive function. They are used to monitor progression over time within a company or to compare results between companies, the so-called benchmark (Grote, 2009; Sedgwick and Stewart, 2010). Differences between indicators for management and organisation in the two literature sources are less marked.

Safety metaphors, models, and theories can guide the formulation of process safety indicators. This review shows a complicated metaphor/model/theory-indicator relationship. But literature seems to agree on a scenario/barriers-indicator relation. A search for process safety indicators may start with a selection of major accident scenarios, say the top-15 or top-20 of the most dominant scenarios selected both by process engineers, plant managers and operators. This selection will be input for a HAZOP type of session, to detect barriers present per scenario, including management supporting systems and management actions related to these systems.

To meet the need for quantification, dominant in industry, numbers of activities, incidents, interventions etc. are counted. Problems with quantification, both for process as for management/organisation indicators have been mentioned several times. Numbers do not contain any information on quality (Hale, 2009; Hudson, 2009; Øien et al, 2011b). More experience with safety indicators is needed (Guastello, 1993; Chaplin and Hale, 1998). A similar argument counts for organisational causes of accidents. With hindsight latent factors, or conditions are clear, but prospectively the relationship with hazards and risks seem relatively vague (Kongsvik 2010; Øien et al 2011a; Bellamy and Sol, 2012; Pasman, 2015).

To conclude, process safety indicators seem to provide insight into the safety of a process or a company. Confirmation, based upon empirical research is necessary. However, it is clear that the 'silver bullet' has not been found yet (Webb, 2009). Safety indicators associated with barriers quality, scenarios and on effects of decision-making appear to be the most obvious ones. Logically, this will make safety indicators, process- and company-specific. The challenge is to define indicators that provide insight into the quality of barriers and development of scenarios. Future international regulations, like Seveso legislation updates, possibly will allow process safety indicators to remain in the spotlight.

2.6 REFERENCES

Allford, L. (2009). Process safety indicators. *Safety Science, 47*(4), 466.

ANSI/API (2010). *Process Safety Performance Indicators for the Refining and Petrochemical Industries*. ANSI/API RP 754, first edition.

Baker report (2007). *The report the B.P. U.S. refineries independent safety review panel*.

Basso, B., Carpegna, C., Dibitonto, C., Gaido, G., Robotto, A., Zonato, C. (2004). Reviewing safety management system by incident investigation and performance indicators. *Journal of Loss Prevention in the Process Industries, 17*, 225-231.

Bellamy, L. (2009). Process safety indicators. *Safety Science, 47*(4), 472-473,

Bellamy, L., Sol, V. (2012). *A literature review on safety performance indicators supporting the control of major hazards*. National Institute for Public health and the Environment, Ministry of Health, Welfare and Sport. RIVM rapport 620089001/2012.

Bellamy, L. (2015). Exploring the relation between major and minor accidents. *Safety Science, 71*, 93-103

Bhandari, S., Azevedo, C. (2013). Implementation of process key performance indicators in a large fertilizer complex. Conference paper, *58th AIChE symposium 'Ammonia plant safety and related facilities' 54*, 269-276, Frankfurt

CCPS (2010). *Guidance for Process Safety Metrics*. AIChE, New Jersey.

CCPS (2011). *Process Safety Leading and Lagging metrics. You don't improve what you don't measure*. AIChE, New York.

CCPS (2014). *Risk Bases Process Safety Overview*. AIChE, New Jersey.

Cefic (2011). *Guidance on Process Safety Performance Indicators*. Brussels.

Cefic-EPSC (2012). *Process safety indicator*, Conference Brussels, http://www.epsc.org/content.aspx?Group=products&Page=pspi_conference.

Chaplin, R., Hale, A. (1998). *An evaluation of the International Safety Rating System (ISRS) as intervention to improve the organisation of safety*. In: Hale A Baram M (Eds.), Safety Management, The Challenge of Change. Pergamon, London.

COMAH (2012). *Process safety performance indicators*.

Dryeborg, J. (2009). The causal relation between lead and lag indicators. *Safety Science, 47*(4), 474-475.

Duijm, N., Fievez, C., Gerbec, M., Hauptmanns, U., Konstsndinidou, M. (2008). Management of health, safety and environment in process industry. *Safety Science, 46*, 908-920.

EPSC European Process Safety Centre (2012). *Safety Critical Measures*, Report nr. 33, Brussels

Eriksen, S. (2009). Performance indicators. *Safety Science, 47*(4), 468.

Grabowski, M., Ayyalasomayajula, P., Merrick, J., Harrald, J., Roberts, K. (2007). Leading indicators in virtual organisations. *Safety Science, 45*, 1013-1043.

Groeneweg, J. (1992). *Controlling the controllable, the management of safety*. Proefschrift Rijksuniversiteit Leiden, DWSO Press, Leiden.

Grote, G. (2009). Response to Andrew Hopkins. *Safety Science, 47*(4), 478.

Guastello, S., (1993). Do we really know our occupational prevention program work? *Safety Science, 16*(3-4), 445-463.

Guillaume, E. (2011). *Identifying and responding to weak signals to improve learning from experiences in high-risk industry*. Proefschrift Technische Universiteit Delft, Boxpress BV, Oirschot.

Guldenmund, F., Booster, P. (2005). The effectiveness of structural measures on safety, a case description (in Dutch). *Journal of applied occupational sciences, 18*(2), 38-44.

Gulijk, C. van, Swuste, P., Zwaard, W. (2015). Heinrich's models. *Journal of Risk Research* (submitted).

Hale, A. (2009). Why safety indicators? *Safety Science, 47*(4), 479-480.

Harms-Ringdahl, L. (2009). Dimensions in safety indicators. *Safety Science, 47*(4), 481-482.

Hassan, J., Khan, F. (2012). Risk based asset integrity indicators. *Journal of Loss Prevention in the Process Industry, 25*(3), 555-554.

Heinrich, H. (1941). *Industrial accident prevention*, 2nd ed. McGraw-Hill Book Company London & New York.

Heuverswyn, K. van, Reniers, G. (2012), *From safety management to performant wellbeing management* (in Dutch), No. 4 die Keure - Business & Economics, Brugge.

Hijmans, E. (1963). *Men, metal, machine* (in Dutch). Kluwer, Deventer.

Hollnagel, E., Woods, D., Leveson, N. (2006). *Resilience Engineering, concepts and precepts*. Ashgate, Aldershot.

Hopkins, A. (2000). *Lessons from Longford, the Esso Gas Plant explosion*. CCH Australia Ltd, Sidney.

Hopkins, A. (2007). *Thinking about Process safety indicators*. Oil and Gas Industry Conference paper 53. Manchester, November.

Hopkins, A. Hale, A. (2009). Process safety indicators. Special issue *Safety Science, 47*(4), 459-510.

Hopkins, A. (2009). Thinking about process safety indicator. *Safety Science, 47*(4), 460-465.

HSE (2006). *Process safety indicators, a step-by-step guide for the chemical and major hazards industries*, HSG

254. The Office of Public Sector Information, Information Policy Team, Kew, Richmond, Surrey.
Hudson, P. (2009). Process indicators; managing safety by numbers. *Safety Science, 47*(4), 483-485.
Johnson, W. (1973). *The Management oversight and risk tree – MORT, including systems developed by the Idaho Operations Office and Aerojet Nuclear Company*. US Atomic Energy Commission, Division of Operational Safety – SAN 821-2/UC-41.
Kampen, J. van, Beek, D. van, Groeneweg, J. (2013). The Value of Safety Indicators. Society of Petroleum Engineers - SPE European HSE Conference and Exhibition 2013. *Health, Safety, Environment and Social Responsibility in the Oil and Gas Exploration and Production Industry*. pp. 109-121.
Khawaji, I. (2012). *Developing system based leading indicators*. Massachusetts Institute of Technology, Boston.
Kidam, K. Hurme, M. (2013). Analysis of equipment failure as contributors to chemical process accidents. *Process Safety & Environmental Protection, 91*, 61-78.
Kjellén, U. (2009). The safety measurement problem revisited. *Safety Science, 47*(4), 486-489.
Kletz, T. (1993). *Lessons from disasters, how organisations have no memory and accidents recur*. UK, Institution of Chemical Engineers.
Knegtering, B. Pasman, H. (2009). Safety of the process industry in the 21st century: a changing need of process safety management for changing industry. *Journal of Loss Prevention in the Process Industries, 22*, 162-168.
Knijff, P. Allford, L. Schmelzer, P. (2013). Process Safety Leading Indicators. A Prespective from Europe. *Process Safety Progress, 32*(4), 332-336.
Kongsvik, T. Almklov, P. Fenstad, J. (2010). Organisational safety indicators: some conceptual considerations and a supplementary qualitative approach. *Safety Science, 48*, 1402-1411.
Körvers, P. (2004). *Accident precursors Pro-active identification of safety risks in the chemical process industry*. Proefschrift Technische Universiteit Eindhoven.
Körvers, P. Sonnemans, P. (2008). Accidents: a discrepancy between indicators and facts! *Safety Science, 46*, 1067-1077.
Le Coze, J. (2009). A taxonomy issue. *Safety Science, 47*(4), 490.
Le Coze, J. (2013). New models for new times. An anti-dualist move. *Safety Science, 59*, 200-218.
Le Coze, J. (2014). *1984-2014, 'normal accidents'; was Perrow right for the wrong reasons?'* Presentation Working on Safety Conference (WIOS2014) Westwood, Scotland September 30th.-October 1st.
Leeuwen, M. van (2006). *De veiligheidsbarometer. The safety barometer, accountability of safety in the gas distribution sector based on safety performance indicators* (in Dutch). Universiteit Twente, Twente.
Leveson, N. (2015). A systems approach to risk management through leading safety indicators. *Reliability Engineering and System Safety, 136*, 17-34.
Martorell, S. Sanchez, A. Munoz, A. Pitarch, J. Serradell, V. Roldam, J. (1999). The use of maintenance indicators to evaluate the effects of maintenance programs on NPP performance and safety. *Reliability Engineering and System Safety, 65*, 85-94.
Mearns, K. (2009). From reactive to proactive – can LPI's deliver? *Safety Science, 47*(4), 491-492.
Nielsen, D. (1971). *The cause/consequence diagram method as a basis for quantitative accident analysis*. Danish Atomic Energy Commission, research Establishment Risø. Rapport Risø-M-1374.
OECD (2008a). *Guidance on developing safety performance indicators related to chemical accident prevention, preparedness and response*. OECD Environment, Health and Safety Publications, Series on Chemical Accidents No. 198 Guidance for industry, Environment Directorate. Paris.
OECD (2008b). *Guidance on developing safety performance indicators related to chemical accident prevention, preparedness and response*. OECD Environment, Health and Safety Publications, Series on Chemical Accidents No. 18 for Public Authorities and Communities/Public, Environment Directorate. Paris.
Øien K Utne I Herrera I (2011a). Building safety indicators I theoretical foundations. *Safety Science, 49*, 148-161.
Øien K Utne I Tinmannsvik R Massaiu S (2011b). Building safety indicators II applications. *Safety Science, 49*, 162-171.
OGP (2008). *Asset Integrity – The key to managing major incident risks*. Report nr 415.
OGP (2011). *Process safety, recommended practice on key performance indicators*. Report nr 456, November, London.
Olivier, P. van, Hove, L. (2010). *The power of indicators* (in Dutch). Intersentia, Antwerpen.
Parker, D. Lawrie, M. Hudson, P. (2006). A framework for understanding the development of organisational safety culture. *Safety Science, 44*(7), 551-562.
Pasman, H. Rogers, W. (2014). How can we use the information provided by process safety performance indicators. *Journal of Loss Prevention in the Process Industries, 30*, 197-206.
Pasman, H. (2015). *Risk Analysis and control for industrial processes gas oil and chemicals*. IChemE Botterworth Heineman, Oxford.
Perrow, C. (1984). *Normal accidents. Living with high-risk technologies*. BasicBooks, US.
Pigeon, N. O'Leary, M. (2000). Man-made disasters: why technology and organisations (sometimes) fail. *Safety Science, 34*, 15-30.
Qureshi, Z. (2007). *A review of accident modelling approaches for complex socio-technical systems*. 12th

Australian Workshop on safety SCS'07.
Rasmussen, J. (1997). Risk management in a dynamic society. *Safety Science, 27*(2-3), 183-213.
Reason, J. (1990a). *Human error*. Cambridge University Press, Cambridge.
Reason, J. (1990b). The contribution of latent human failures to the breakdown of complex systems. *Philosophical Transactions of the Royal Society of London, 327*, 475-484.
Reason, J. (1997). *Managing the risk of organizational accidents*. Ashgate, Aldershot Hampshire.
Reiman, T. Pietikainen, E. (2012). Leading indicators of system safety. *Safety Science, 50*, 1993-2000.
Roberts, K. (1988). Some characteristics of one type of high reliability organization. *Organization Science, 1*(2), 160-176.
Rochlin, G. (1986). High reliability organisations and technical change. Some ethical problems and dilemma. *IEEE Technology and Society Magazine*, September; 3rd-9th.
Rockwell, T. (1959). Safety Performance measurement. *Journal of Industrial Engineering, 10*(1), 12-16.
Rolt, L. (1955). *Red for Danger: A History of Railway Accidents and Railway Safety*. The Bodley Head, London.
Saqib, N. Siddiqi, M. (2008). Aggregation of safety performance indicators to higher-level indicators. *Reliability Engineering and System Safety, 93*, 307-315.
Sedgwick and Stewart, 2010, *Experience with developing process safety KPI's within Scottish Power*. Retrieved from https://www.energyinst.org/filegrab/?ref=653&f=4.Sedgwick&Stewart.pdf.
Sklet, S. (2006). Safety barriers, definitions, classifications, and performance. *Journal of Loss Prevention in the Process Industries, 19*, 494-506.
Sonnemans, P. Körvers, P. (2006). Accidents in the chemical industry: are they foreseeable? *Journal of Loss Prevention in the Process Industries, 19*, 1-12.
Sonnemans, P. Körvers, P. Pasman, H. (2010). Accidents in normal operation - Can you see them coming? *Journal of Loss Prevention in the Process Industry, 23*, 351-366.
Svedung, I. Rasmussen, J. (2002). Graphic presentation of accident scenarios mapping system structure. *Safety Science, 44*(5), 397-417.
Swuste, P. Gulijk, C. van, Zwaard, W. (2010). Safety metaphors and theories a review of the occupational safety literature of the US UK and the Netherlands, till the first part of the 20th century. *Safety Science, 48*, 1000-1018.
Swuste, P. Gulijk, C. van, Zwaard, W. Oostendorp, Y. (2014). Occupational safety theories, models and metaphors in the three decades since WO II, in the United States, Britain and the Netherlands: a literature review. *Safety Science, 62,* 16-27.
Swuste, P. Gulijk, C. van, Zwaard, W. Oostendorp, Y. (2015). Developments in the safety science domain, in the field of general and in safety management between the 1970s and 1979, the year of the near disaster on Three Mile Island, a literature review. *Safety Science* (in press).
Tarrants, W. (1963). *An evaluation of the critical incident technique as a method for identifying industrial accident causal factors*. Doctoral dissertation, New York University, New York.
Tarrants, W. (1970). A definition of the safety measurement problem. *Journal of Safety Research, 2*(3), 106-108
Turner, B. (1976). The organisational and inter-organisational development of disasters. *Administrative Science Quarterly, 21*(3), 378-397.
Turner, B. (1978). *Man-made disasters*. Butterworth-Heinemann Oxford.
UK Oil and Gas Industry (2012). *Step Change in safety, leading performance indicators, guidance for effective use*. Aberdeen.
VNO-NCW, (2011). *Safety First, 10 action points for safety. VNO-NVW, Den Haag (in Dutch).*
Visser, J. (1995). Managing safety in the oil industry. The way ahead. Proceedings of Loss Prevention and Safety Promotion in the Process Industries, Antwerp, Belgium, June 6-9, 1995.
Vinnem, J. Aven, T. Husebo, T. Seljelid, J. Tveit, O. (2006). Major hazard risk indicators for monitoring of trends in the Norwegian offshore petroleum sector. *Reliability Engineering and System Safety, 91*, 778-791.
Vinnem, J. (2010). Risk indicators for major hazards on off shore installations. *Safety Science, 48*, 770-787.
Wagenaar, W. Groeneweg, J. Hudson, P. Reason, J. (1994). Promoting safety in the oil industry. *Ergonomics, 37*(12), 1999-2013.
Webb, P. (2009). Process safety indicators: a contribution to the debate. *Safety Science, 47*(4), 502-507.
Weick, K. (1987). Organisational culture as a source of high reliability. California. *Man Review, 29*(2), 112-127.
Wijk, L. van (1977). The accident process, a system model (in Dutch). *De Veiligheid, 53*(10), 433-436.
Wildavsky, A. (1988). *Searching for Safety*. Transaction Publishers, London.
Winsemius, W. (1951). *The psychology of accidents*. Discourses of the Institute of Preventive Medicine (in Dutch). Kroese, Leiden.
Wreathall, J. (2009). Leading? Lagging? Whatever! *Safety Science, 47*(4), 493-494.
Zemering, C. Swuste, P. (2005). The scenario audit (in Dutch). *Journal of applied Occupational Sciences, 18*(4), 79-88.
Zwetsloot, G. (2009). Prospects and limitations of process safety performance indicators. *Safety Science, 47*(4), 495-497.

3

DETERMINING A REALISTIC RANKING OF THE MOST DANGEROUS PROCESS EQUIPMENT OF THE AMMONIA PRODUCTION PROCESS: A PRACTICAL APPROACH[3]

3 The Chapter is based on the paper: Schmitz, P., Reniers, G. & Swuste, P. (2021). Determining a realistic ranking of the most dangerous process equipment of the ammonia production process: A practical approach. *Journal of Loss Prevention in the Process Industries, 70*, 104395. https://doi.org/10.1016/j.jlp.2021.104395, and was formatted and edited for this thesis.

ABSTRACT

This chapter investigates how the most dangerous process equipment can be determined by calculating their effects resulting from a loss of containment using DNV GL's Phast™ dispersion model. To do so, flammable and toxic effects from a release from the main equipment of an ammonia plant have been calculated. Such an encompassing approach, which can be carried out for an entire plant, is innovative and has never been conducted before. By using this model, it has been demonstrated that the effects arising from an event of failure are the largest in process equipment containing pressurised synthesis gas and 'warm' liquid ammonia, meaning the ammonia buffer tanks, ammonia product pumps, and the ammonia separator. Most importantly, this document substantiates that it is possible to rank the most hazardous process equipment of the ammonia production process based on an adverse health impact on humans using the calculated effect distance as a starting point for a chance of death of at least 95%. The results from the effect calculations can be used for risk mapping of an entire chemical plant or be employed and applied in a layer of protection analysis (LOPA) to establish risk mitigation measures.

3.1 INTRODUCTION

In the chemical industry, major hazard incidents may lead to severe damage and casualties, and sometimes even to the bankruptcy of a company. It is therefore of utmost importance to focus on this type of (process safety related) incidents so to prevent them. Crisislab's investigation, as referred to in section 1.2.1, concluded that there is a lack of anticipation of "early warnings". This is not unknown in the chemical industry: Hopkins (2000) already arrived at similar conclusions in his report on the Esso incident in Longford (Australia), whereas Baker's report (2007) of the BP incident in Texas (USA) was a wake-up call for the global chemical/process safety community. This chapter contains the results of the first phase of this research, and looks for the (selection of) worst case accidents. It answers the following research question:

> *Which process equipment has the largest adverse health impact on humans in the event of failure?*

The associated sub-questions to be investigated are:
1) What are the intrinsic hazards of the ammonia production process?
2) Where in the ammonia production process can an event of failure occur?
3) What adverse health impact can the hazards have on humans in the event of failure?
4) How can the adverse health impact on humans be measured?

This chapter only deals with effects and their calculations, and aims to indicate the most dangerous equipment of the ammonia production process. The likelihood of scenarios which may lead to such effects, is dealt with in the next chapter (Schmitz et al., 2020).

3.1.1 Definitions

Since a hazard can materialise itself through a scenario to an effect and subsequently to all kinds of consequences, a link is made to bowties. Bowties are user-friendly for mapping scenarios (Chevreau et al., 2006; De Ruijter and Guldenmund, 2016), and illustrate the relationship between hazard, effect and consequence.

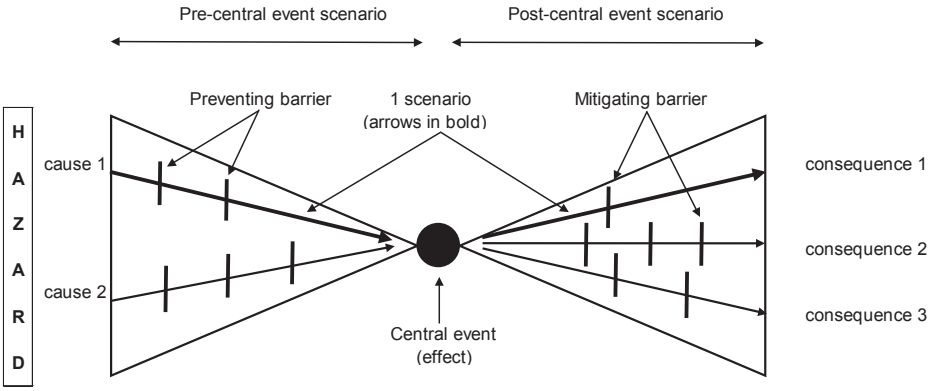

Fig. 3.1, the bowtie model

Figure 3.1 shows the bowtie metaphor and indicates a scenario comprising of two parts, meaning a pre-central event scenario which may take days, weeks, months or even longer to develop, and a post-central event scenario which may unroll quickly into the ultimate consequences: casualties, injuries, damage and/or loss of production (Swuste et al., 2016).

The central event is in the middle of the bowtie and is in a (petro)chemical installation often characterised by an undesired and uncontrolled release of a hazardous substance and/or energy. As it were, a situation arises with an uncontrollable hazard. Hazard is the intrinsic ability or potentiality to cause material damage, casualties and/or injuries. Cockshott (2005) describes hazard as a condition that could potentially lead to injury, and/or damage to property or to the environment. He defines a central event as the initial consequence which involves the release of a hazard. In this thesis Cockshott's initial consequence is freely translated as effect, meaning that the effect is manifested in the central event and can be defined as the primary result of the release of the hazard.

Table 3.1 shows the relationship between the hazard, effect and consequence to humans. For example, the release of a flammable gas can lead to a jet or flash fire which heat radiation or flame contact may result in severe burns or even fatality. Although some physical properties such as pressure and temperature may be considered as intrinsic hazards, their influence is indirect through the released substances. More pressure leads, for example, to a higher release flow and hence to a larger effect. Consequences have only been considered for humans, and not for the installation or the environment. In contrast to the installation and the environment, humans experience both the effects of a flammable and a toxic release.

Table 3.1, relation between hazard, effect and consequence to humans

Left-hand side of the bowtie	Central event	Right-hand side of the bowtie
The ammonia production process has the following intrinsic hazards:	At a loss of containment, the intrinsic hazards may lead to one of the following effects:	The effects may result in one of the following adverse health consequences on humans:
(Over)heated steam, flammable & toxic substances	Heat radiation or flame contact Overpressure Toxic concentration	Burns Internal injury Poisoning

3.1.2 The ammonia production process

The ammonia process uses natural gas, steam, and air as raw materials. The process, shown in Figure 3.2, consists of two main parts: 1. the steam reforming, the method for producing hydrogen from natural gas, and 2. the ammonia synthesis loop. The steam reforming is followed by the shift conversion, carbon dioxide removal and methanation steps and is operated at pressures of 25 to 35 bar. The hydrogen (H_2) is then combined with nitrogen to produce ammonia (NH_3) via the Haber-Bosch process in the synthesis reactor. The numbers in brackets in the text below refer to the process units of Figure 3.2.

Process units 1 to 7 are referred to as the steam reforming, the shift conversion, carbon dioxide removal and methanation. The incoming natural gas largely consists of methane (CH_4), but also contains small amounts of sulphur. This is undesirable and sulphur is therefore converted to H_2S and absorbed with the aid of hydrogen and a catalyst (1). In the reformer (2) the desulphurised natural gas is largely converted to CO, CO_2 and hydrogen (H_2) using steam and a catalyst at 825 °C and 35 bar. Air is supplied to the secondary reformer (3), through which nitrogen (N_2) is introduced into the process, which is needed as the second component to make ammonia. The oxygen from the air reacts with some H_2 and increases the secondary reformer's temperature to over 1000 °C, enabling to crack the remaining methane. The CO formed in the cracking process is converted to CO_2 and H_2 in two serial reactors (4 and 5) using steam. To remove the CO_2 from the gas mixture, the process gas is passed through a (physical) scrubber unit (6). The last residues of CO and CO_2 (not converted or washed out) are converted into methane in the methanation (7) using a catalyst and H_2.

The ammonia synthesis loop consists of the process units 8 to 12. In this part of the ammonia production process, the process gas mainly consists of hydrogen and nitrogen, in a ratio of 3 to 1. The synthesis gas is compressed (8) to the synthesis pressure after which the residues of water are removed by adsorption in the molecular sieves (8a). The reaction to ammonia is according the Haber-Bosch process and takes place in the synthesis reactor (9) in the presence of a catalyst at approx. 200 bar and 515 °C. Since there is insufficient heat in the process in a start-up situation, the start-up heater (9a) is temporarily used to bring the synthesis gas mixture up to its reaction

temperature. The ammonia formed is successively cooled (10) and separated in the ammonia separator (11) from the unreacted and inert gases, which are returned to the compressor (8). The liquid ammonia from the ammonia separator (11) is reduced in pressure from 200 bar to approx. 18 bar before entering the expansion vessel (12). The gases released during the ammonia expansion are sent to the waste gas recovery, which is located elsewhere and outside the scope of this study. From the ammonia expansion vessel, the liquid ammonia serves as a coolant (10a) before being sent to the buffer tanks (13) and the ammonia grid (14). Finally, the ammonia is either stored (15) at atmospheric conditions or immediately delivered to the site users (not indicated).

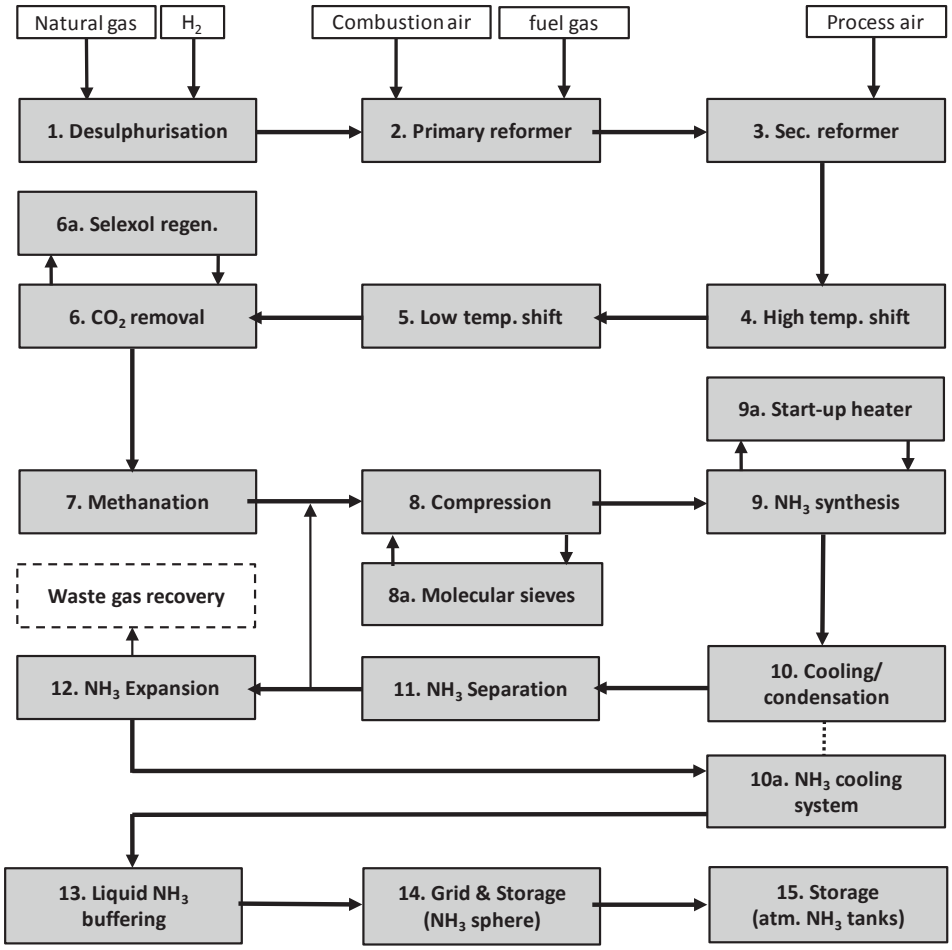

Fig. 3.2, overview of the ammonia production process

3.2 METHODOLOGY

In this chapter various indices have been investigated, most of which have been developed to quickly identify the most significant hazards (in terms of effect) of a (petro)chemical installation. Perhaps the most commonly used is the Dow Fire & Explosion index (AIChE, 1994a), which calculates an exposure area based on substance, process and installation data from which property damage can be determined. Dow's Chemical Exposure index (AIChE, 1994b), on the other hand, calculates the effect distances due to an airborne amount of a toxic substance and is a simple method for determining relative, acute toxicity hazards in adjacent plants and communities (Marshall and Mundt, 1995). This index is also used for drawing up emergency plans (Mannan, 2004). The Mond index is very similar to Dow's Fire & Explosion index, but is more detailed (Tyler, 1985; Andreasen and Rasmussen, 1990). Unfortunately, the Mond index does not have a separate rating for toxicity. Several indices have been developed for hazard identification, evaluation and inherently safe design purposes: SWeHI, HIRA (FEDI and TDI) and I2SI (Khan and Abassi, 1998; Khan et al., 2001; Khan et al., 2003; Khan and Amyotte, 2004). During the Aramis project a method was also designed for the selection of dangerous equipment (Delvosalle et al., 2006) based on process parameters and substance data. The method developed by Tugnoli and Cozzani (2007) is based on commercial software models and takes into account thermal radiation, overpressure and toxic concentration.

All these indices report a relative risk index on a somewhat arbitrary scale. The numerical index results cannot be compared directly to each other, although each index provides guidance on the meaning of the numbers it generates (Hendershot, 1997). In this study, the effects have been calculated using the Phast™ software program, which uses standard dispersion models and has an extensive substance database. Phast™ can calculate thermal radiation, concentrations like upper and lower explosion limits, overpressure and toxic concentrations of individual components but also of mixtures, under the predominantly prevailing weather conditions.

This research has been performed following four steps, which are described in the sections below:

1) Selecting the main process equipment;
2) Collecting the associated process data;
3) Drawing up the starting points;
4) Calculating the effects using Phast™.

3.2.1 Step 1: Selecting the main process equipment

The hazards of the ammonia production process are very diverse in nature. The natural gas, the cracked gas from the steam reforming and the synthesis gas pose a fire and an explosion hazard. Ammonia, and several other substances in the process, such as CO and CO_2, are toxic. In addition, the ammonia production process produces steam at all kinds of pressures and temperatures, which not only entails a (physical) explosion risk but also a risk of burns in the event of a release.

An ammonia plant consists of many process equipment (vessels, reactors, heat exchangers, etc.) and pipes. In order to estimate where the hazards of the ammonia process are located and how these hazards relate to each other, the ammonia production process has been divided into smaller parts than the process units indicated in Figure 3.2. In this research 64 process equipment have been selected to be significant and representative for the ammonia production process. The pipework is excluded because its effects can be traced back to the process equipment connected to it.

The ammonia production process is connected to a grid which exports the produced ammonia to the site users and the two atmospheric storage tanks. The boundaries of the ammonia production process to be investigated are limited from the imported natural gas to the export of the produced ammonia into the grid. The grid as well as the atmospheric storage tanks and loading facilities are outside the scope of this research, indicated as process unit 14 and 15 in Figure 3.2 respectively.

3.2.2 Step 2: Collecting the necessary process data

Clearly, process pressures, temperatures and substances are influencial parameters for determining the effect radii. In addition, the height of the release is of influence as is the contained quantity, where ammonia is concerned. The total release depends not only on the (automated) controls of the ammonia production process, but also on the response time of the control room operators. This particularly affects in case of ammonia where the source duration strongly determines the effect radius. The issue of the response time was presented to several control room operators and from the interviews it appeared that in the event of an operational abnormality, they first try and keep the ammonia production process running rather than focussing on the possibility of a calamity. This is understandable because a shutdown of the ammonia production process may entail a disturbance of the ammonia supply to the site users. Only when the control room operators see an emerging risk, they will shut down the ammonia production process as quickly as possible, taking it to a predefined, safe state. In consultation with the control room operators the response time has been set at 5 minutes, assuming the safeguarding system does not automatically intervene prematurely. In the worst case it takes 5 minutes before the main pumps

and compressors are being stopped, the ammonia process has been isolated into so-called containment systems and is being depressurised using the flares.

In Dow's Chemical Exposure Index Guide (AIChE, 1994b), the release time of toxic scenarios is set at 5 minutes. The Dutch guideline for risk calculations, Bevi (RIVM, 2015) and the purple book (VROM, 2005b) use different response times for the calculation of quantitative risk assessments, and distinguish between different containment systems. The containment system closest to the situation of the ammonia plants is a semi-automatic containment system, meaning that a leak is automatically detected and reported in a continuously staffed control room, and where the control room operator activates the shutdown system after validation by pushing a button. The response time of a semi-automatic containment system is 10 minutes. This length of time is not considered realistic and as indicated above the response time to manually activate the shutdown system has been determined at 5 minutes. As the response time is only relevant in case of ammonia and given the large size of such a release, this will inevitably lead to rapid detection from the controlled process and from local observations (odour, noise) by the control room and field operators respectively. Hence, little time is needed to validate such an event.

By isolating the ammonia production process there is no more flow of liquid and gas between the containment systems. However, this is still possible between the process equipment within one containment system. In general, gases can move freely through a containment system whereas liquids can not, as most liquid flows are controlled by valves or pumps.

3.2.3 Step 3: Drawing up the starting points

To guarantee that data is handled in the same way and that accepted criteria are used as an input of the dispersion calculations, a few starting points have been formulated. As indicated in section 3.1.1 only consequences on humans have been considered whereas consequential damage and production outage have been ignored. The toxic concentration, heat radiation, flame contact and overpressure scenarios have been calculated at a height of 1 metre as most employees present in the plant are at ground level (RIVM, 2015; Tugnoli and Cozzani, 2007). The synthesis gas and ammonia compressors are in a building at a height of 8 metres. Since there is a reasonable chance of operators and mechanics being present at a height of 8 metres, the calculations assume that these compressors are located on ground level and in the open air.

The calculated effects are shown as radii within which there is a chance of death of at least 95% which is much higher than the 1% chance of Tugnoli and Cozzani (2007), and the chance of 50% by Khan and Abassi (1998), and Khan et al. (2001). The largest

distance from the source is used as a measure of the size of the effect. In this way, the effects of the different process equipment as a result of an uncontrolled release can be compared with each other, whether it concerns a heat radiation, a flame contact, a toxic cloud or an overpressure scenario.

For the calculations of the 64 main process equipment of the ammonia production process, a free outflow has been assumed through a round 50 mm hole located at the bottom of the equipment. This diameter size is an accepted practise in the chemical industry and based on an average diameter of flanges and pipe fittings welded to equipment for piping, valves and instrumentation. In addition, the direction of the outflow has been taken horizontally (RIVM, 2015).

For the liquid filled vessels, the degree of filling is in accordance with normal operation and set at 50%. As gases can move freely through an isolated containment system, all gaseous components of an isolated containment system will flow out. In contrast, liquid flows inside a containment system need to be assessed case-by-case to establish the subsequent delivery from adjacent equipment because liquid flows are controlled by valves and pumps. Since the hole is at the bottom, the liquid inside a process equipment will flow out completely.

In the event of a calamity, the ammonia production process is taken to a safe state, either automatically by the safeguarding system or manually by the operating staff, meaning that several predefined valves are closed so that the containment systems are isolated from each other. Seven containment systems have been defined with reference to the process units of Figure 3.2: 1 to 5; 6 and 6a; 7; 8 and 8a; 9 to 11 (without 10a); 10a and 12; and 13.

A probit relationship shows the relationship between the concentration of a substance, the exposure time and the effect on humans. A probit relationship for a toxic substance can be used for any combination of concentration and exposure time to estimate the percentage of people who decease from exposure to the substance. For the toxic effects of ammonia, the probit relationship $Pr = -16.21 + \ln(\int C^2 \times dt)$ has been used, where C is the concentration in parts per million (ppm) and t is the exposure time in minutes (RIVM, 2015). The exposure time for the persons present in the affected area is equal to the duration of the release, unless there is significant pool evaporation. In such a case, the additional exposure time has been estimated using the dynamic exposure images of Phast™. The concentration can be calculated based on the total exposure time using the above probit relationship. The concentration being entered for the calculation of the toxic radii is based on a chance of death of 95%, assuming no chance of escape from the toxic cloud in the affected area.

Figure 3.3 shows the consequences from a continuous release of a flammable gas. A direct ignition leads to a jet fire, whereas a delayed ignition leads to a flash fire or an explosion (RIVM, 2015). For heat radiation in case of a jet fire, the following probit relationship has been assumed: Pr = -36.38 + 2.56 ln(∫$Q^{4/3}$ x dt), where Q is the heat radiation in W/m^2 and t the exposure time in seconds (RIVM, 2015). The radii of 35 kW/m^2 have been calculated for heat radiation due to jet fires. An exposure time of 20 seconds within the 35 kW/m^2 radius will inevitably lead to death, assuming 20 seconds will not be enough time to escape from the affected area.

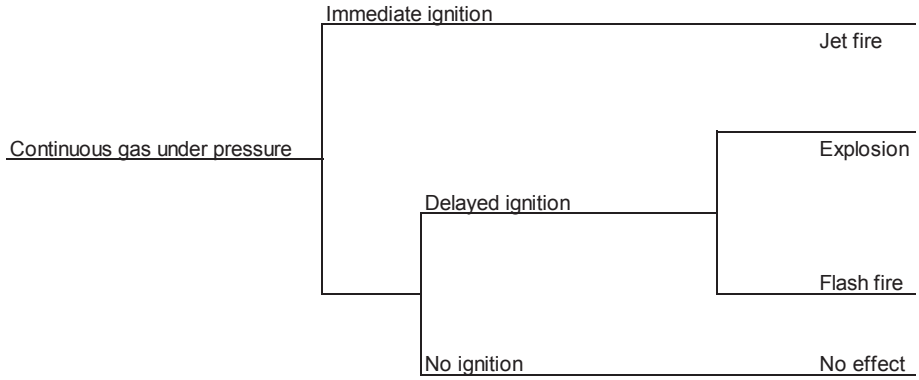

Fig. 3.3, event tree for continuous release of a flammable gas (RIVM, 2015)

The main body parts that can be directly damaged by a pressure wave resulting from a blast or an explosion are the ears and lungs (HSE, s.d.). In addition, explosions can also be associated with other injuries caused by projectiles and flying objects, physical displacement or inhalation of hot and toxic gases (Owers et al., 2011; Zuckerman, 1940; Mannan, 2004; VROM, 2005a). The chance of injuries from the latter group increases proportionally as one is closer to the explosion (Dussault et al., 2014). For overpressure-related personal injury, the HSE uses the probit relationship: Y = 5.13 + 1.37 ln(P), where P is the overpressure in bar (HSE, s.d.). The probit relationship shows that exposure to an overpressure of 0.9 bar results in a 50% chance of death. Mannan (2004) refers to Eisenberg et al., who determined a 50% chance of death at 1.4 bar overpressure based on serious lung bleeding. APPEA (HSE, s.d.) applies 0.7 bar as 100% fatal for both indoor locations and unprotected structures, whereas the Dutch guideline for risk calculations (RIVM, 2015) puts the site-specific risk at 1 for an overpressure higher than 0.3 bar. Owers et al. (2011) state that the chance of death is 50% at 9 barg, but this would only concern primary effects, meaning the interaction from the blast wave with the body. In fact, much higher pressure levels (up to tens of

bars) are reported to which people can still be exposed, where it is assumed that not the overpressure but other explosion effects usually result in a much higher chance of death (HSE, s.d.; Zipf and Cashdollar, s.d.; Mannan, 2004; VROM, 2005a). Lethality only occurs with high overpressures and long duration of the pressure wave (VROM, 2005a). It must be concluded that the values reported in the literature differ considerably from each other and that it is not always clear which explosion effects and which injuries have been included in the chance of death. For this research it is assumed that an overpressure of 0.9 bar from an explosion results in a chance of death more than 95%. Besides the direct consequences for the ears and lungs, other injuries have also been considered. Finally, it should be noted that the actual overpressure exerted on humans by the blast wave, due to reflection and circulation, may be greater than the calculated overpressure (VROM, 2005a).

When calculating the pressure effects resulting from an explosion, the growth and displacement of the cloud, as well as the moment of ignition, have been considered carefully. The latter is set in Phast™ in such a way that the resulting pressure wave reaches a maximum distance from the point of release. The distance from the overpressure radius to the point of release has been taken as a measure of the magnitude of the overpressure effect. It is assumed there is no chance of escape from the affected area in case of an explosion.

A release of a continuous pressurised gas may also lead to a flash fire, meaning a rapid combustion without significant overpressures. A flash fire can only occur when the explosive cloud is not confined nor hindered by obstacles. Persons within the ignited cloud will be seriously burned by direct flame contact. In most cases, the size of the burned skin surface is so large that those exposed will decease. As an estimate of the extent of personal injury from a flash fire, it seems reasonable to assume that all persons within the cloud at the time of ignition will be fatally affected. Due to the short exposure time, the extent of personal injury outside the cloud will be relatively small. The lower explosion limit defines the size of the explosive cloud and is used as a measure of the effect (VROM, 2005a).

Flash fires are particularly dangerous in confined areas, as even a relatively small fire can consume enough oxygen and produce enough smoke to cause death of the persons present. But as the flash fires will occur in the open, asphyxiation and smoke inhalation have not been considered.

In the containment system 9 to 11 and excluding 10a (see Figure 3.2) the composition of the substances can be both flammable and toxic. The flammable and toxic gases can move freely through the containment system, which leads to different effects in the

event of an equipment failure. For the calculation of the jet fire, flash fire and explosion effects, a gas composition is assumed as it is present in the equipment during normal operation. Exposure to a heat radiation, flame contact and an overpressure is already fatal when the release is of a short duration. This is different for exposure to ammonia as only longer durations prove to be fatal. Therefore, the entire gas mass (of 8,500 kg) and the release duration do play a prominent role in the calculation of the effects of a toxic ammonia release. The duration of the release determines the exposure time and thus the ammonia concentration for a chance of death of at least 95%. In view of the longer release duration, the gas composition of the total containment system has been averaged in order to make a better estimate of the flow rate of the release and hence the release duration and exposure time.

In the containment system 10a and 12 (see Figure 3.2) there is a subsequent supply of liquid ammonia from other equipment in the containment system. If the release rate shows a cascading variation, each variation is calculated considering its release rate and duration. The calculated effect radii are then placed in time to determine the maximum effect distance.

3.2.4 Step 4: Calculating the effects using Phast™

Phast™ version 7.21 has been used for the dispersion calculations. The calculation model can be used to analyse and quantify situations in which potential consequences may occur to people, the environment and installations (DNV GL, 2014). The calculations assume that the process equipment are located in a free space without being surrounded by other equipment. Next to process data and substance properties, weather conditions and wind speed are influential. The calculations are based on the average weather conditions as recorded in the weather service database of Maastricht Aachen airport. The most common weather type is D (“pasquill stability D, neutral little sun and high wind or overcast/windy night”) with a wind speed of 5 m/s. The average temperature is assumed to be 10 °C.

3.3 RESULTS

A selection of the 64 most relevant process equipment of the ammonia production process is shown in Tables 3.2 and 3.3. The selection is based on expert opinion, and an average cross-section of an ammonia plant comprising the most recognisable equipment has been considered. Table 3.2 contains input data such as the process pressure and temperature and the height at which the content is being released. It also lists the most relevant substances of the gas composition, and the mass of the gaseous and liquid ammonia. And finally, for some of the process equipment, the

subsequent supply of ammonia from other process equipment of the containment system is recorded.

Table 3.3 shows the calculated effect distances, which are the horizontal distances from the source to the effect radius at a height of one metre. Table 3.3 also lists the calculated release rates and their duration. The release durations leading to heat radiation, flame contact and overpressure effects are much longer than 20 seconds and have not been calculated in more detail. The exposure time inevitably leads to a chance of death of at least 95% in case of a jet fire of 35 kW/m^2. In case of an (unignited) gas cloud the duration is long enough to become stable and to reach its maximum size before it is ignited in a delayed time. The last column records the concentrations of ammonia that correspond to the exposure time. If there is a varying release rate due to a subsequent delivery, both the concentration of the first and of the total release duration are given.

Figure 3.4 shows the 35 kW/m^2 radius of the synthesis reactor (step 9 in Figure 3.2) as a top view at 1 metre height. The point of release is in the middle of the Y-axis. The synthesis reactor has a pressure of 200 bar and a temperature of 450 °C in normal operation. The gas consists of hydrogen and nitrogen in a ratio of 3 to 1 with approximately 9.5% methane. The release rate is 31.3 kg/s, which results in a horizontal jet fire when immediately ignited. The maximum distance of the 35 kW/m^2 radius at 1 metre height from the point of release is 55 metres. Figure 3.5 shows the course of the heat radiation from the point of the release as a side view at 1 metre height. The heat radiation is more than 35 kW/m^2 between 16 and 55 metres. The maximum heat radiation is over 100 kW/m^2 in the centre of the horizontal jet fire.

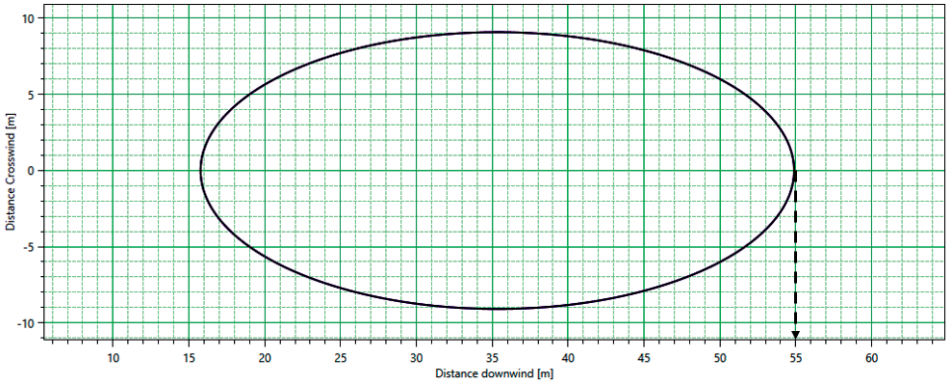

Fig. 3.4, top view at 1 metre height of the 35 kW/m^2 radius of the synthesis reactor as a function of the distance from the point of release

Table 3.2, input data for the Phast™ calculations

Process unit	Equipment (TS – Tube Side, SS – Shell Side)	Central event	Pressure (bar g)	Temp. (°C)	Height (m)	Composition (mol %)							Mass gaseous NH_3 (kg)	Mass liquid NH_3 (kg)	Subsequent supply (kg/h)
						CH_4	CO_2	CO	H_2	N_2	H_2O	NH_3			
1	Desulphurisation	Jetfire/expl/fl.fire	38	320	3	83.8	1.4	0	3.5	4	0				
2	Reformer (TS)	Jetfire/expl/fl.fire	38	800	3	11.9	3.6	2.8	21.2	0.8	59.1				
3	Secondary reformer	Jetfire/expl/fl.fire	37	950	3	2.7	4.9	7.1	32.5	14.6	37.1				
3	Waste gas heat boiler	Jetfire/expl/fl.fire	37	620	4	0.2	4.9	10.1	35.2	14.2	37.1				
4	High temperature shift	Jetfire/expl/fl.fire	35	360	3	0.2	8.0	6.1	38.3	14.2	34.0				
5	Low temperature shift	Jetfire/expl/fl.fire	33.5	240	3	0.2	12.0	1.1	42.3	14.2	30.0				
6	CO_2 absorber	Jetfire/expl/fl.fire	31.7	-1	4.5	0.2	10.1	0.3	67.1	22.0	0				
6	Separator downstream CO_2 absorber	Jetfire/expl/fl.fire	31	-1	1	0.3	0.1	0.3	74.6	24.4	0				
7	Methanation	Jetfire/expl/fl.fire	30	270	4	0.5	0.1	0.1	74.2	24.5	0.3				
7	Synthesis gas cooler (SS)	Jetfire/expl/fl.fire	30	30	2	0.7	0	0	73.9	24.6	0.5				
8	Synthesis gas compressor	Jetfire/expl/fl.fire	200	40	1	0.7	0	0	73.9	24.6	0.5				
8a	Molecular sieves	Jetfire/expl/fl.fire	72	5	3	0.7	0	0	73.9	24.6	0.5				
9	Syngas heat exchanger (TS)	Jetfire/expl/fl.fire	200	31	3	8.9			63.7	21.2		1.3			
9	Syngas heat exchanger (TS)	Tox. cloud	200	31	3	9.5			57.5	21.5		8.5	8500		
9	Synthesis reactor	Jetfire/expl/fl.fire	200	450	1	9.5			57.5	21.5		8.5			
9	Synthesis reactor	Tox. cloud	200	450	1	9.5			57.5	21.5		8.5	8500		
10	Synloop waste heat boiler (TS)	Jetfire/expl/fl.fire	200	300	1.5	10.1			51.6	17.3		15.5			
10	Synloop waste heat boiler (TS)	Tox. cloud	200	300	1.5	9.5			57.5	21.5		8.5	8500		
10	Syngas heat exchanger (SS)	Jetfire/expl/fl.fire	200	175	3	10.1			51.6	17.3		15.5			
10	Syngas heat exchanger (SS)	Tox. cloud	200	175	3	9.5			57.5	21.5		8.5	8500		
10	NH_3 converter effluent chiller (TS)	Jetfire/expl/fl.fire	200	-25	3	11.3			58.0	19.0		5.7			
10	NH_3 converter effluent chiller (TS)	Tox. cloud	200	-25	3	9.5			57.5	21.5		8.5	8500		
11	Ammonia separator	Jetfire/expl/fl.fire	200	-25	1	11.8			60.4	19.9		1.7			
11	Ammonia separator	Tox. cloud	200	-25	1	9.5			57.5	21.5		8.5	8500	1500	
12	Ammonia expansion vessel	Jetfire/expl/fl.fire	18	-22	5	23.5			42.3	15.8		11.1			
12	Ammonia expansion vessel	Tox. Cloud	18	-22	5	23.5			42.3	15.8		11.1		2300	68000
10a	NH_3 converter effluent chiller A (SS)	Tox. cloud	5.2	10	3									5650	68000

Table 3.2, input data for the Phast™ calculations

Process unit	Equipment (TS – Tube Side, SS – Shell Side)	Central event	Pressure (bar g)	Temp. (°C)	Height (m)	Composition (mol %)							Mass gaseous NH_3 (kg)	Mass liquid NH_3 (kg)	Subsequent supply (kg/h)
						CH_4	CO_2	CO	H_2	N_2	H_2O	NH_3			
10a	NH_3 converter effluent chiller B (SS)	Tox. cloud	2.3	-7	3									4600	0
10a	NH_3 converter effluent chiller C (SS)	Tox. cloud	0.8	-21	3									4200	0
10a	NH_3 converter effluent chiller D (SS)	Tox. cloud	0.1	-32	3									2200	0
10a	Ammonia compressor	Tox. cloud	9.3	105	1										50000
10a	Ammonia condenser	Tox. cloud	9	25	9									5	50000
10a	Ammonia collection vessel	Tox. cloud	9	25	5									2200	50000
10a	Ammonia product pumps	Tox. cloud	17	10	1									3700	68000
13	Ammonia buffertanks	Tox. cloud	16	10	1.5									32200	0

Table 3.3, output data from Phast™

Process unit	Equipment (TS – Tube Side, SS – Shell Side)	Central event	Effect radius (m)	Flow rate (kg/s)	Source duration (s)	Concentration at chance of death ≥ 95% (ppm)
1	Desulphurisation	Jetfire/expl/fl.fire	32/8/0	8.16	>20	
2	Reformer (TS)	Jetfire/expl/fl.fire	0/0/0	6.42	>20	
3	Secondary reformer	Jetfire/expl/fl.fire	0/0/0	6.39	>20	
3	Waste gas heat boiler	Jetfire/expl/fl.fire	0/0/0	6.41	>20	
4	High temperature shift	Jetfire/expl/fl.fire	0/0/0	7.23	>20	
5	Low temperature shift	Jetfire/expl/fl.fire	0/0/0	7.70	>20	
6	CO_2 absorber	Jetfire/expl/fl.fire	0/12/0	8.79	>20	
6	Separator downstream CO_2 absorber	Jetfire/expl/fl.fire	30/19/35	7.21	>20	
7	Methanation	Jetfire/expl/fl.fire	0/7/0	4.95	>20	
7	Synthesis gas cooler (SS)	Jetfire/expl/fl.fire	22/13/20	6.62	>20	
8	Synthesis gas compressor	Jetfire/expl/fl.fire	61/49/71	41.3	>20	
8a	Molecular sieves	Jetfire/expl/fl.fire	34/19/21	16.3	>20	
9	Syngas heat exchanger (TS)	Jetfire/expl/fl.fire	61/37/49	47.8	>20	
9	Syngas heat exchanger (TS)	Tox. cloud	2	49.6	171	53000
9	Synthesis reactor	Jetfire/expl/fl.fire	55/26/38	31.3	>20	
9	Synthesis reactor	Tox. cloud	2	31.3	271	41100
10	Synloop waste heat boiler (TS)	Jetfire/expl/fl.fire	57/26/37	37	>20	
10	Synloop waste heat boiler (TS)	Tox. cloud	2	37	230	46000
10	Syngas heat exchanger (SS)	Jetfire/expl/fl.fire	57/20/21	42	>20	
10	Syngas heat exchanger (SS)	Tox. cloud	2	40	212	49000
10	NH_3 converter effluent chiller (TS)	Jetfire/expl/fl.fire	66/38/52	57	>20	
10	NH_3 converter effluent chiller (TS)	Tox. cloud	2	57	148	58000
11	Ammonia separator	Jetfire/expl/fl.fire	68/55/86	55.9	>20	
11	Ammonia separator	Tox. cloud	34	218-56.4	7-157	270000-57000
12	Ammonia expansion vessel	Jetfire/expl/fl.fire	0/7/0	4.1	>20	
12	Ammonia expansion vessel	Tox. Cloud	34	65-19	50-300	101000-41000
10a	NH_3 converter effluent chiller A (SS)	Tox. cloud	84	33.8	336	38800
10a	NH_3 converter effluent chiller B (SS)	Tox. cloud	51	22.9	200	50000
10a	NH_3 converter effluent chiller C (SS)	Tox. cloud	41	13.7	307	41000
10a	NH_3 converter effluent chiller D (SS)	Tox. cloud	14	4.9	449	33600
10a	Ammonia compressor	Tox. cloud	11	2.8	300	41000
10a	Ammonia condenser	Tox. cloud	0	13.9	300	41000
10a	Ammonia collection vessel	Tox. cloud	27	43.8-13.9	74-300	83000-41000
10a	Ammonia product pumps	Tox. cloud	128	61	300	41000
13	Ammonia buffertanks	Tox. cloud	156	59	542	30500

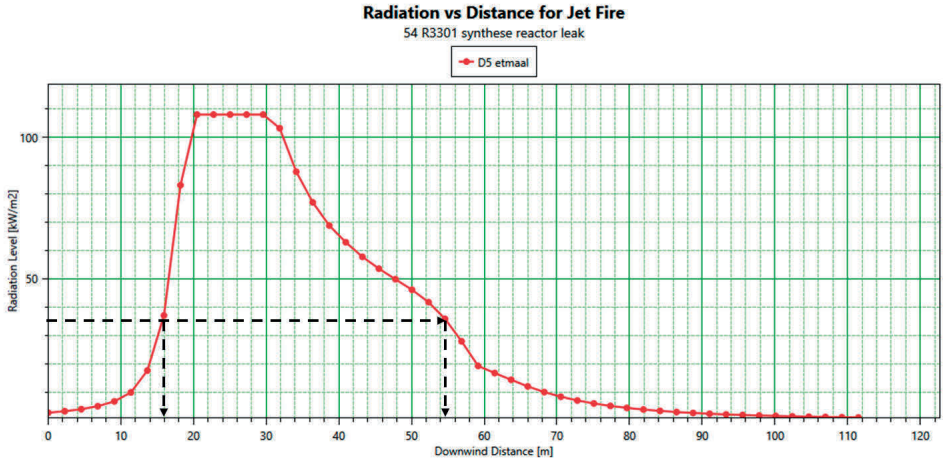

Fig. 3.5, side view at 1 metre height of the heat radiation of the synthesis reactor as a function of the distance from the point of release

Figure 3.6 shows a side view of the gas cloud released from the separator downstream the CO_2 absorber (step 6 of Figure 3.2). The size of the gas cloud is limited by its lower explosion limit of 53,200 ppm which is assumed to be the size of the flash fire. The maximum distance to the source is just over 35 metres.

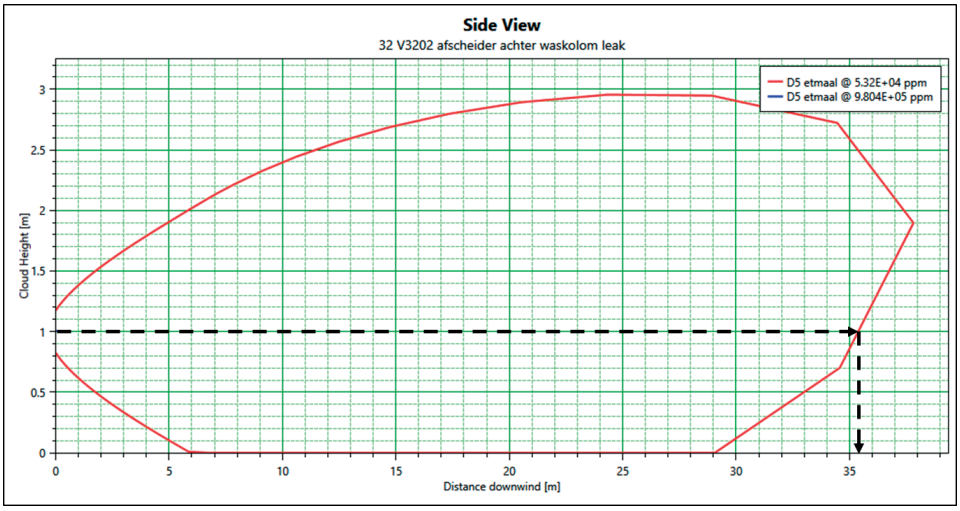

Fig. 3.6, side view of the flammable gas cloud of the separator downstream the CO_2 absorber as a function of the distance from the point of release

A gas release at the molecular sieves (step 8a of Figure 3.2) can also lead to a jet fire, a flash fire or an explosion due to respectively an immediate or delayed ignition. Figure 3.7 shows the 0.9 bar overpressure radius at ground level with a maximum distance of 19 metres from the point of release, with the ignition source in the middle of the explosion at 15 metres from the point of release. The effect radius at 1 metre height has been calculated assuming the explosion to be spherical and its centre at the height of release. The moment of ignition is set in Phast™ as delayed, meaning the explosive cloud is ignited after 11 seconds after its first release when it has stabilised within its explosive limits. This delayed explosion scenario is assumed to be worst case.

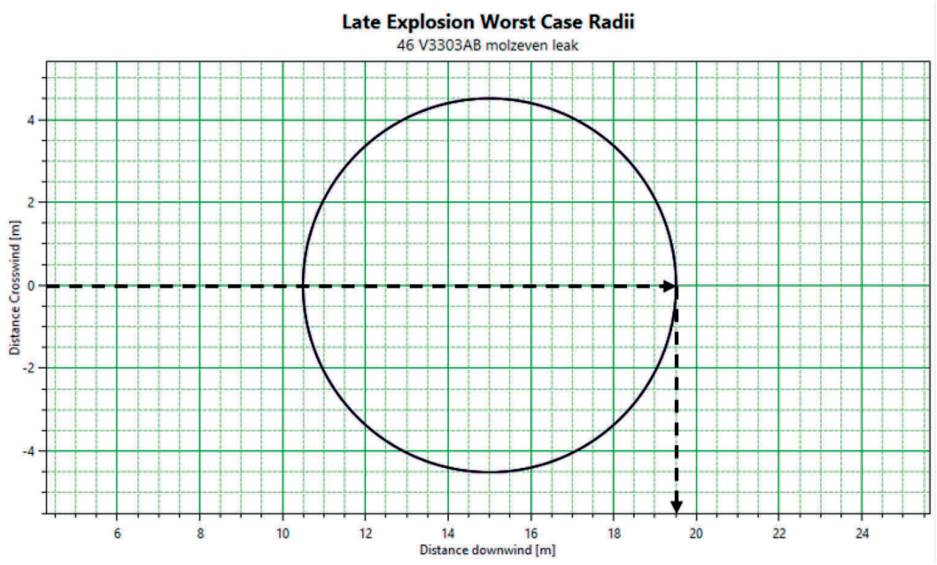

Fig. 3.7, top view of the 0.9 bar overpressure radius at ground level of the molecular sieves as a function of the distance from the point of release

Figure 3.8 shows a side view of a toxic cloud released from the (shell of the) ammonia converter effluent chiller A (step 10 of Figure 3.2). The chiller's shell side contains 5650 kg of saturated ammonia at 10 °C at an equilibrium pressure of 5.2 bar gauge, which is released at the bottom of the equipment at a height of 3 metres. There will also be a subsequent delivery of 68 tons/hr ammonia for 300 seconds, meaning the control room response time. The total amount of ammonia is released at a flow rate of 33.8 kg/s for 336 seconds. No pool is formed so the exposure time is equal to the release duration. For a 95% chance of death, the ammonia concentration at an exposure time of 336 seconds is 38,800 ppm. The effect radius at 1 metre height for this concentration is 84 metres. The 38,800 ppm radius stabilises after 9 seconds and continues until the chiller has emptied after 336 seconds.

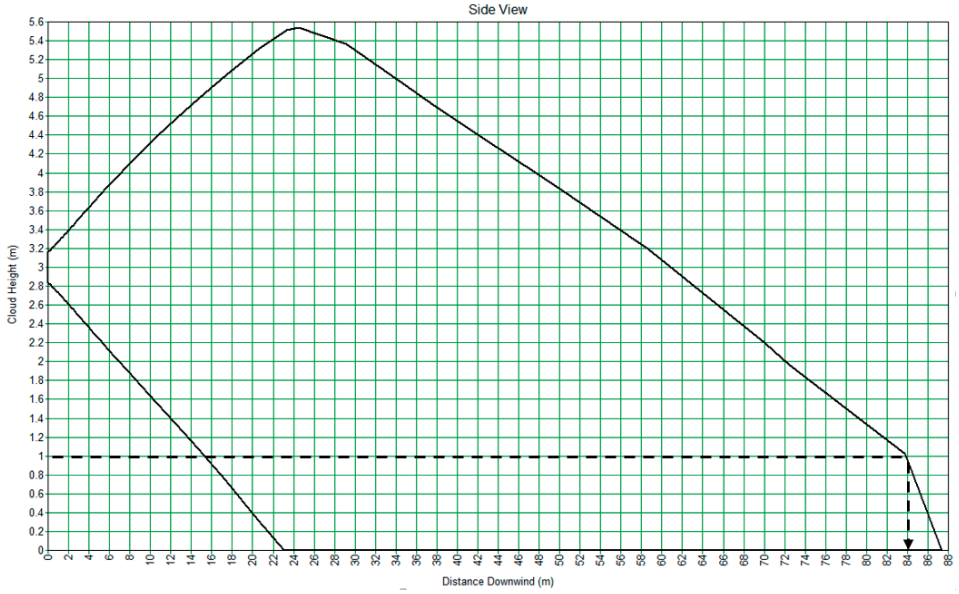

Fig. 3.8, side view of 38,800 ppm ammonia radius of the ammonia convertor effluent chiller A (shell side) as a function of the distance from the point of release

Figure 3.9 shows the calculated effects in a bar graph in which the main equipment is put in the order of the ammonia production process. The numbers behind the equipment correspond to the process units in Figure 3.2. The largest effects of the ammonia production process due to the release of flammable gases are to be expected in the process part with the highest pressures: from compression to ammonia separation. The largest toxic effects regarding the release of ammonia can be found at the ammonia product pumps and the buffer tanks.

It should be noted that where process equipment does not show any effect, it does not mean that there are no effects. However, the effects do not meet the criterion whereby the chance of death is at least 95% at a height of 1 metre.

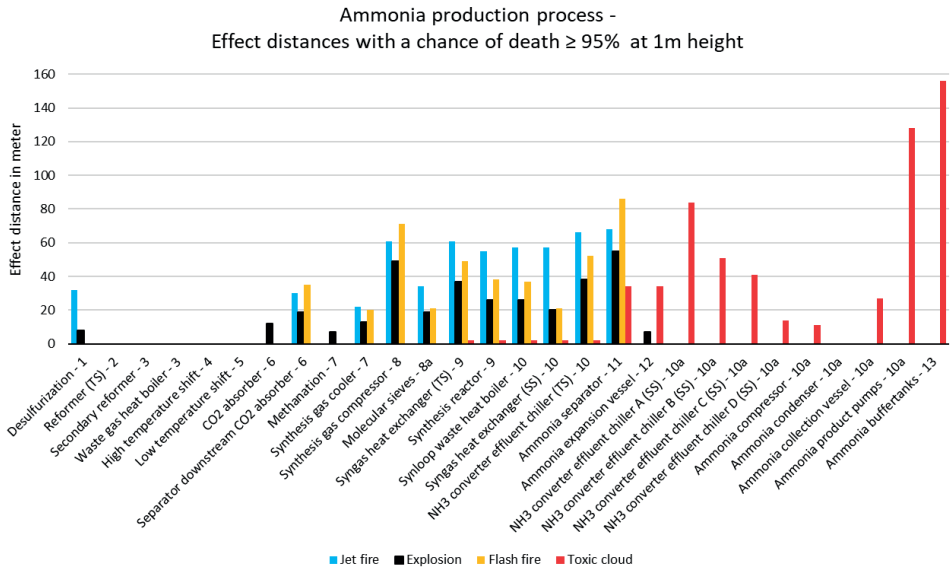

Fig. 3.9, overview of the effect distances for the main equipment of the ammonia production process with a chance of death of at least 95%

3.4. DISCUSSION

In the toxic scenarios, the release duration largely determines the size of the effect. The release duration for those scenarios with a subsequent delivery of ammonia from another process equipment in their containment system (process units 10a and 12, see Figure 3.2), is depending on the response time of the control room operator to shut down the plant. In consultation with control room operators, a response time of 5 minutes has been chosen, based on rapid detection, both from process data and from local observations (odour, noise) in combination with a simple intervention. A longer reaction time of for example 10 minutes, would increase the toxic radii somewhat, but would not significantly change the overall conclusion.

The effects have been calculated with a chance of death of at least 95% and this is much higher than was found in other papers and guidelines. Due to the choice of such a high chance of death, all persons in the effect radius will not be able to flee or avoid the hazard and will, regardless of their physical condition, be immediately affected and will most certainly decease. The probit relationship of ammonia shows an asymptotic approximation of the concentration to one million ppm with an increasing chance of death. The choice of 95% chance of death is arbitrary to the extent that a greater chance leads to too high concentrations and too small effect radii. The toxic effects could therefore be underestimated.

The overpressure of 0.9 bar at which it is very likely to decease from the blast pressure could be questioned as standards, guidelines and scientific studies reveal a large variety of values. However, where the HSE (s.d.) probit relationship establishes a chance of death of 50% for 0.9 bar based on primary effects (lung damage), a more than 95% chance of death considering the secondary, tertiary and even quaternary effects appears to be justified. Even more because there is a possibility that in a confined process installation the actual overpressure exerted on people is higher than the calculated overpressure due to reflection and turbulences.

The Phast™ dispersion model stems from the same supplier as Safeti: DNV GL. In the Netherlands, effect calculations, and in particular quantitive risk assessments (QRAs), are prescribed with Safeti-NL, a version of Safeti adapted for the Netherlands, for granting an environmental permit. Calculations with Phast™ and Safeti-NL will hardly differ from each other. Phast™ is slightly more flexible in use, meaning it has freely selectable weather types and heights of exposure, and a larger database of (acute toxic) substances. In that respect, the choice for Phast™ seemed to be a better choice than the choice for Safeti-NL. But, like all models, the Phast™ calculation model has several limitations that must be considered. Some of meaning are mentioned below:

- Any structures, buildings, and the like are not included in the calculations. This is not possible in Phast™ unless these data are entered manually.
- The hazards of most mixtures are determined by the individual components, meaning that the absorption of ammonia by moisture in the outside air is not considered.
- Phast™ can calculate with changing compositions, but only as a step disturbance and not according to a (predefined) curve. This is especially relevant for toxic effects with longer exposure times where the released gas' composition changes. To overcome this, toxic effects were calculated using average compositions of the released gas.
- Phast™ calculates dispersions as if equipment is located in a free space. So, caution is appropriate when equipment is located indoor or in confined spaces.
- When used in batch plants, attention should be paid to the choice of process conditions as they may vary.

Flammable, explosive and toxic clouds progress in a specific direction, meaning they are determined by the location of the release (jet fires) and by the prevailing wind (toxic clouds). This is different for flash fires and explosions: both the flames and the overpressure radius develop in all directions from the centre of the explosion. Depending on the situation, flash fires and explosions may cover a larger area, which potentially makes them more dangerous than the other two. However, this

phenomenon has not been considered as the distance has been chosen as a measure of the size of the effect.

Regarding flash fire effects it is assumed that everyone in the flammable cloud will decease. This assumption is somewhat conservative as field operators and mechanics wear protective clothing made of fire-retardant materials, which significantly reduce or prevent thermal injury in the body areas that are covered by the fire-retardant material. In the overpressure and heat radiation scenarios no account has been taken of secondary effects by domino scenarios although they may be possible (Reniers and Cozzani, 2013). Secondary effects can be determined in a next step using Phast™ by calculating overpressure and heat radiation levels at which consequential damage may occur to adjacent process equipment. Secondary effects should then be attributed to the initially failed process equipment. Depending on the situation it could well be that the chance of death may be substantially lower from domino scenarios as they take some time to develop, meaning that the chance of escaping from the affected area is much larger. It is expected that these calculations will most likely not substantially contribute to the results of this research.

It can be deduced from Figure 3.9 that:

- The largest effect distances are attributable to ammonia;
- The effects of heat radiation, flame contact and overpressure are approximately the same;
- The heat radiation and overpressure effects up to and including the CO_2 absorber (step 6 of Figure 3.2) are less than 35 kW/m^2 and 0.9 bar respectively at ground level. The inert gases present (CO_2, N_2 and water) absorb so much energy that they significantly reduce the effects;
- Process pressure is decisive regarding the overpressure, flame contact and heat radiation effects;
- The hold-up of saturated ammonia and the subsequent delivery contribute to the release duration, and thus to the effect radii;
- The higher the temperature of the saturated ammonia, the larger the effect radii.

3.5 CONCLUSIONS

In this chapter, flammable and toxic effects from a release from the main equipment of an ammonia plant have been calculated. Such an encompassing approach, which can be carried out for an entire plant, is innovative and has never been conducted before. The calculations show that the ammonia production process comprises several intrinsic hazards related to the presence of steam, flammable gas and ammonia. A release

of a hazardous substance can give rise to burns, internal injury or poisoning from exposure to heat radiation, flames, overpressure or toxic concentration respectively. In the front end of the ammonia production process loss of containment scenarios may lead to heat radiation from jet fires, flame contact from flash fires or to overpressure from explosions due to the presence of flammable components. In the back end there is also ammonia present which release may lead to high toxic concentration levels resulting in poisoning. Releases of steam have not been considered as their effects are much smaller than those from jet or flash fires. The largest adverse health impact on humans in the event of failure can be expected from the compression to the ammonia separation (exposure to heat radiation, flame contact and overpressure) and from the ammonia product pumps and the buffer tanks (exposure to a toxic ammonia concentration). In general, it can be concluded that pressure, temperature and mass are of meaning in that when they increase, the effects and hence the adverse health impact on humans become larger.

Effects have been calculated for a chance of death of at least 95%. This results in effect radii from which maximum distances from the point of release can be determined. By taking the maximum distance as a (relative) measure, the effects of a release of both flammable and toxic substances can be compared. If the central event cannot be avoided, there is a 1 to 1 relationship between the central event and the consequences of burns, internal injury, and poisoning resulting in death. The method in this chapter enables to measure the adverse health impact on humans from a release of hazardous substances from any process equipment. Hence, this chapter provides a relative ranking of equipment and does not claim to provide absolute results, but it leads to an understanding of the relative position of equipment with respect to their dangerousness.

The effect calculation results can be used for risk mapping of an entire chemical plant or be employed and applied in a layer of protection analysis (LOPA) to establish risk mitigation measures. The results from this research provided new insights for OCI Nitrogen into the current method of equipment classification and the investment in preventive measures. A path forward for future process safety research can be the link of the equipment ranking results with barrier management and as such, further optimisation of safety investments.

3.6 REFERENCES

American Institute of Chemical Engineers (AIChE). (1994a). *Dow's Fire and Explosion Index Hazard Classification Guide* (seventh edition). New York, US: American Institute of Chemical Engineers.

American Institute of Chemical Engineers (AIChE). (1994b). *Dow's Chemical Exposure Index Guide* (first edition). New York, US: American Institute of Chemical Engineers.

Andreasen, P., & Rasmussen, B. (1990). Comparison of methods of hazard identification at plant level. *Journal of Loss Prevention in the Process Industries, 3*, 339–344.

Baker report. (2007). *The report of the BP U.S. refineries independent safety review panel*. Retrieved from https://www.csb.gov/bp-america-refinery-explosion/.

Chevreau, F., Wybo, J., & Cauchois, D. (2006). Organising learning processes on risks by using the bow-tie representation. *Journal of Hazardous Materials, 130*, 276–283. https://doi.org/10.1016/j.jhazmat.2005.07.018.

Cockshott, J.E. (2005). Probability Bow-Ties – A Transparant Risk Management Tool. *Process Safety and Environmental Protection, 83*(B4), 307–316. https://doi.org/10.1205/psep.04380.

Delvosalle, C., Fievez, C., Pipart, A., & Debray, B. (2006). ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries. *Journal of Hazardous Materials, 130*, 200–219. https://doi.org/10.1016/j.jhazmat.2005.07.005.

DNV GL. (2014). Retrieved from www.dnvgl.com>Images>Phast-flier_tcm8-56726.

Dussault, M.C., Smith, M., & Osselton, D., 2014. Blast Injury and the Human Skeleton: An Important Emerging Aspect of Conflict-Related Trauma. *Journal of Forensic Sciences, 59*(3), 606–612. https://doi.org/10.1111/1556-4029.12361.

Helsloot, I., Scholtens, A. & Vlagsma, J. (2016). *Toeval of structureel incidentalisme? Negen incidenten uit 2015 bij Chemelot nader beschouwd*. Retrieved from
http://crisislab.nl/wordpress/wp-content/uploads/2016-06-07-rapport-Chemelot-def.pdf.

Hendershot, D.C. (1997). Measuring Inherent Safety, Health and Environmental Characteristics Early in Process Development. *Process Safety Progress, 16*(2), 78–79.

Hopkins, A. (2000). *Lessons from Longford, the Esso Gas Plant explosion*. Sidney, Australia: CCH.

Health and Safety Executive (HSE). (s.d.). *Methods for approximation and determination of human vulnerability for offshore major accident hazard assessment*. Retrieved from https://www.hse.gov.uk/foi/internalops/hid_circs/technical_osd/spc_tech_osd_30/spctecosd30.pdf.

Khan, F.I., & Abbasi, S.A. (1998). Multivariate Hazard Identification and Ranking System. *Process Safety Progress, 17*(3), 157–170.

Khan, F.I., Husain, T., & Abbasi, S.A. (2001). SAFETY WEIGHTED HAZARD INDEX (SWeHI), A New, User-friendly Tool for Swift yet Comprehensive Hazard Identification and Safety Evaluation in Chemical Process Industries. *Trans IChemE, 79*(B), 65–80.

Khan, F.I., Sadiq, R., & Amyotte, P.R. (2003). Evaluation of Available Indices for Inherently Safer Design Options. *Process Safety Progress, 22*(3), 83–97.

Khan, F.I., & Amyotte, P.R. (2004). Integrated Inherent Safety Index (I2SI): A Tool for Inherent Safety Evaluation. *Process Safety Progress, 23*(2), 136–148. https://doi.org/10.1002/prs.10015.

Mannan, S. (2004). *Lees' Loss Prevention in the Process Industries*. Amsterdam, the Netherlands: Elsevier.

Marshall, J.T., & Mundt, A. (1995). Dow's Chemical Exposure Index Guide. *Process Safety Progress, 14*(3), 163–170.

Owers, C., Morgan, J.L., & Garner, J.P. (2011). Abdominal trauma in primary blast injury. *British Journal of Surgery, 98*, 168–179. https://doi.org/10.1002/bjs.7268.

Reniers, G., & Cozzani, V. (2013). *Domino effects in the Process Industries*. Amsterdam, the Netherlands: Elsevier.

Rijksdienst voor Volksgezondheid en Milieu (RIVM). (2015). *Handleiding Risicoberekeningen Bevi (version 3.3)*. Retrieved from https://www.rivm.nl/documenten/handleiding-risicoberekeningen-bevi-v33.

Ruijter, A. de, & Guldenmund, F. (2016). The bowtie method: A review. *Safety Science, 88*, 211–218. http://dx.doi.org/10.1016/j.ssci.2016.03.001.

Schmitz, P., Swuste, P., Reniers, G., & Nunen van, K. (2020). Mechanical integrity of process installations: barrier alarm management based on bowties. *Process Safety and Environmental Protection, 138*, 139–147. https://doi.org/10.1016/j.psep.2020.03.009.

Swuste, P., Theunissen, J., Schmitz, P., Reniers, G., & Blokland, P. (2016). Process safety indicators, a review of literature. *Journal of Loss Prevention in the Process Industries, 40*, 162–173. http://dx.doi.org/10.1016/j.jlp.2015.12.020.

Tugnoli, A., & Cozzani, V. (2007). A Consequence Based Approach to the Quantitative Assessment of Inherent Safety. *AIChE Journal, 53*(12), 3171–3182. http://dx.doi.org/10.1002/aic.11315.

Tyler, B.J. (1985). Using the Mond Index to Measure Inherent Hazards. *Plant/Operations Progress, 4*(3), 172–175.

Ministerie van Verkeer en Waterstaat (VROM). (2005a). *Publicatie reeks gevaarlijke stoffen 1. Deel 2A: Effecten van explosie op personen*. Retrieved from https://content.publicatiereeksgevaarlijkestoffen.nl/documents/PGS1/PGS1-2005-v0.1-deel-2a.pdf.

Ministerie van Verkeer en Waterstaat (VROM). (2005b). *Publication Series on Dangerous Substances (PGS 3). Guidelines for quantitative risk assessment*. Retrieved from https://content.publicatiereeksgevaarlijkestoffen.nl/documents/PGS3/PGS3-1999-v0.1-quantitative-risk-assessment.pdf.

Zipf, R.K., & Cashdollar K.L. (s.d). *Effects of blast pressure on structures on the human body*. Retrieved from https://www.cdc.gov/niosh/docket/archive/pdfs/niosh-125/125-explosionsandrefugechambers.pdf.

Zuckerman, S. (1940). Experimental study of blast injuries to the lungs. *The Lancet*, 219–224.

4

MECHANICAL INTEGRITY OF PROCESS INSTALLATIONS: BARRIER ALARM MANAGEMENT BASED ON BOWTIES[4]

4 The Chapter is based on the paper: Schmitz, P., Swuste, P., Reniers, G. & Nunen van, K. (2020). Mechanical integrity of process installations: Barrier alarm management based on bowties. *Process Safety and Environmental Protection, 138*, 139–147. https://doi.org/10.1016/j.psep.2020.03.009, and was formatted and edited for this thesis.

ABSTRACT

This chapter focusses on the development of a method to monitor accident processes in the chemical industry mainly caused by mechanical integrity of static equipment like vessels, tanks and heat exchangers. A significant part of the mechanical integrity failure scenarios originates from material degradation and corrosion mechanisms which may develop over a relatively long-time period, possibly taking months, years or even longer. Mechanical failure scenarios from two process units have been worked out and visualised using a bowtie. This chapter shows that the monitoring of early warnings can provide information about the current development of mechanical failure scenarios. In addition, early warnings can be used to initiate inspections if there is a likelihood that the mechanical failure scenario has been activated. Considering the shift from breakdown maintenance to preventive and predictive maintenance and risk-based inspection (RBI), inspections based on early warnings could also be a new step in the field of maintenance efficiency.

4.1 INTRODUCTION

OCI Nitrogen has experienced several process safety incidents at its two ammonia plants at the Chemelot site in Geleen, the Netherlands. In most of the incidents process equipment started leaking which was discovered at an early stage i.e. before break. According to an internal investigation, these incidents were mainly caused by an incorrect choice of process equipment or piping material and unforeseen mechanical failure scenarios. The scenarios were not identified in previously conducted safety studies, nor were the related phenomena looked at during regular inspections. These "leak before break" incidents were always unforeseen and occurred without any warning signal. Due to these incidents, the ammonia plant at issue had to shut down unscheduled.

This chapter describes a method for hazard identification as first step in risk control of process installations. The method specifically looks at investigating mechanical failure scenarios that can affect the integrity of static process units of ammonia plants leading to major and catastrophic failures. The method is based on an existing mechanical integrity assessment of one of OCI Nitrogen's ammonia plants (Schmitz et al., 2019). Ageing is not explicitly investigated in this sub-study, even though the ammonia plants of OCI Nitrogen are relatively old compared to the number of years for which they were originally designed. Despite ageing is a topic in literature (HSE, 2010; OVV, 2018; SZW, 2016; TNO, 2015), there are two arguments why this sub-study was not focussed on ageing as such. Firstly, ageing is not directly related to chronological age" (COMAH, 2010; HSE, 2006; CCPS, 2018). Secondly, mechanical failure scenarios, such as corrosion, erosion or fatigue, develop over time, and this aspect will automatically come forward. This chapter is only focussing on mechanical failure scenarios and not so much on ageing. Although these scenarios develop over time and are strongly related to ageing, ageing is a much wider concept.

Kletz, Perrow and Turner showed from the late 1970 onwards that major accident processes often started from less noticeable events, which were later called early warnings (Turner, 1978; Perrow, 1984; Kletz, 1988). It was the Turner who postulates this Incubation Theory, showing various organisational failures leading to major accidents. Incubation referred to mechanisms in organisations which denied hazards and risks. In the late 1980s, Reason used the metaphor of resident pathogens for the denial of early warnings. These pathogens were later visualised as holes in barriers in his well-known Swiss Cheese metaphor (Reason, 1987, 1997). The origin of these holes lied in the decision-making processes of the so-called blunt-end managers and the impact of these decisions on front-line operators. For the first time the Tripod model made the concept of latent factors operational with the Basic Risk Factors (Groeneweg, 1992).

And thirty years after the publication of Turner, the early warnings were part of the so-called Management Delivery Systems of the Bowtie metaphor. These delivery systems were necessary actions of management to ensure the presence and to monitor the quality of barriers (Guillaume, 2011; Guldenmund et al., 2006). Early warnings are investigated empirically in this chapter and gain an important place in the current understanding of complex accident processes.

Although most mechanical failures may develop slowly, it is preferable to detect them as early as possible. The early detection of a hazard can be done by a sensor as part of a barrier. Dokas et al. (2013) use the term early warning as a synonym for leading process safety indicator. They can be seen as an observable collection of data which can indicate the faults and threats of a system in a timely manner. Knegtering and Pasman (2013), Øien et al. (2011a, 2011b) and Vinnem (2010) directly link these early warnings to indicators. Based on this, the barrier's quality determines to what extent scenarios can be detected early and influenced by taking timely actions so to stop the occurrence and development of (material degradation and corrosion) scenarios.

In this chapter a connection is made between incident scenarios and (preventive) barriers. From these barriers early warnings can be derived serving as indicators. A well selected group of indicators can provide information about the current likelihood of accident processes. The method is explained based on two examples i.e. a steam superheater and a start-up heater, two important process units in the ammonia production. The following research question is formulated:

> *How can major process safety incidents caused by mechanical failure of static process units be anticipated and prevented at OCI Nitrogen's ammonia plants?*

Mechanical integrity can be defined as the management of critical process equipment to ensure it is designed and installed correctly and that it is operated and maintained properly (API, 2019). A deficiency in mechanical integrity and ageing of equipment is often a major cause of incidents in the industry. This is also the case on the Chemelot site: approximately 50% of the "loss of containment" incidents at Chemelot were due to deficiencies in mechanical integrity in the period 2011 – 2015 (Hoedemakers, 2016). Some of the scenarios were not identified and some were identified but assessed not to be realistic. Hoedemakers (2016) investigated the technical causes based on 89 mechanical integrity incidents and has identified five categories:

1) Corrosion under insulation;
2) Contact with aggressive chemicals;

3) Vibrations that are continuously present in a working plant;
4) Extreme process conditions including frequent starting / stopping and heating / cooling of the plant;
5) Mechanical stress in the material.

Based on this, Hoedemakers has identified four major causes for mechanical failure:

1) External conditions, such as the weather, the environment and (plant) emissions;
2) Internal process conditions due to (aggressive) chemicals;
3) Maintenance activities, for example, assembly under stress or wrong material selection;
4) Process conditions like vibrations, pressure peaks, extreme temperatures, rapid temperature changes.

Professional literature provides all kinds of guidelines with programmes for asset management, asset integrity or risk management, whether or not aimed at preventing ageing of (process) installations (DNV, 1996; HSE, 2006, 2007, 2010; IAEA, 2017; OGP, 2008). Risk-based inspection (RBI) is an example of this. Scientific literature is more model-based and provides proposals for risk-based asset integrity indicators (Hassan and Khan, 2012), condition monitoring (Utne et al., 2012) or an integrity operating window (Lagad and Zaman, 2015) which can foresee increased risks and thus promote timely action.

4.2 INDUSTRIAL CHALLENGE

A complete RBI programme provides a consistent methodology for assessing the optimum combination of methods and frequencies of inspection. By analysing each available inspection method, estimating its relative effectiveness in reducing failure probability and including the costs, an optimisation programme can be developed (API, 2016). However, an RBI programme does not consider process disturbances adequately which may significantly increase the risks associated with mechanical failures. In large chemical installations like an ammonia plant, process upsets, unscheduled shutdowns and extreme internal and external conditions may cause accelerated material degradation or increased corrosion rates. They may require instant monitoring or inspection upon detection.

RBI is a suitable systematic programme in which an inspection programme is established beforehand based on a risk assessment. But deficiencies in mechanical integrity, especially in plants which are at or over their lifespan, may need immediate

detection and follow-up. It's therefore of vital importance to map these scenarios and discover how they can be detected and managed at an early stage. This chapter provides guidance for mapping scenarios into bowties, implementing early warnings and using barrier alarm management on scenario level.

4.3 METHODOLOGY

Bowties are appropriate and user-friendly for the mapping of scenarios (Chevreau et al., 2006; de Ruijter and Guldenmund, 2016). They have not only been applied in major hazard scenarios but also in occupational safety scenarios (Bellamy et al., 2007). The bowtie is a metaphor for an accident process and shows the initiating event of a scenario, one or more hazards, the consequences and the barriers that can stop the scenario from happening (Swuste et al., 2016). Comparing the simple, sequential design of bowties with the "Swiss cheese model" by Reason (1990), bowties may have multiple scenarios leading to the central event. The holes in the Swiss cheese correspond to the flaws in the organisational aspects in the bowtie, shown as "management delivery systems" below. They should initiate management actions to guarantee the barriers' quality (Swuste et al., 2019).

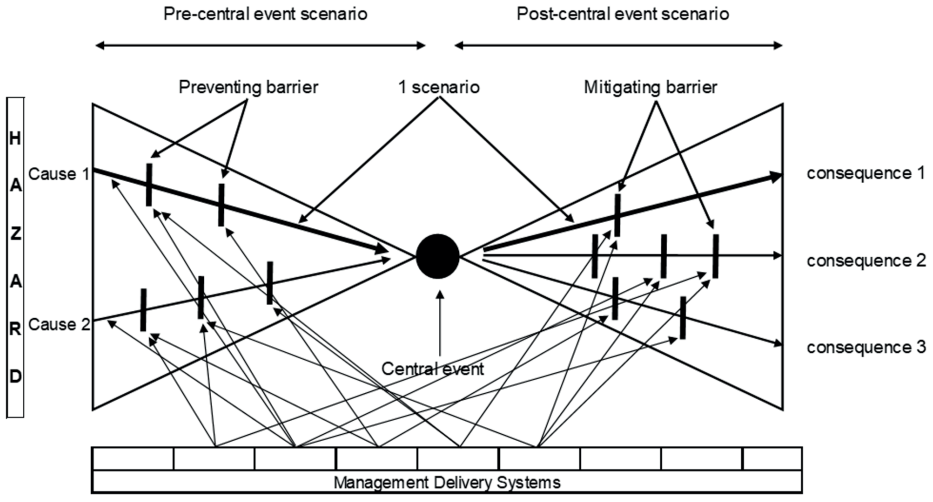

Fig. 4.1, bowtie metaphor

Figure 4.1 shows an example of a bowtie with the so-called central event at the centre of the bowtie. This central event in (petro)chemical installations is often characterised by an undesirable and uncontrolled release of a hazardous substance and/or energy

from the plant. As a result, one or more hazards become uncontrollable. A hazard has the intrinsic ability to cause material damage, casualties and injuries and consists of the substance and energy of a process unit. According to Cockshott (2005) it is "a condition that could potentially lead to injury, damage to property or the environment". He defines a central event as "the initial consequence which includes the release of a hazard". An ammonia plant contains inflammable gases such as hydrogen and natural gas, toxic ammonia in gas and liquid form and steam at very high pressures and temperatures.

A barrier can be defined as anything that can prevent a cause from developing into a consequence, including preventing the cause itself (Bellamy et al., 2007). Safety barriers can be physical and/or non-physical means to prevent, control or reduce undesired events or accidents (Sklet, 2006). If these barriers are broken or not present, a scenario may develop into a central event, or the central event may lead to undesired consequences.

What do barriers look like? And how do they intervene into a scenario and a central event? Guldenmund et al. (2006) nominate 11 different types of barriers, both preventive and protective (or mitigating). Most barriers fulfil more than one task: the detection of the hazard, the diagnosis of the scenario and the actions to prevent the scenario from developing. Hollnagel (2008) has a slightly different approach and distinguishes barriers according to their function, according to what they do, and defines four barrier systems: physical (buildings, fences), functional (alarms, interlocks, interface), symbolic (rules, tasks, procedures) and incorporeal (safety culture). Vinnem (2010) uses technical and operational barrier elements to include the presence of influencing organisational factors. A similar distinction is made by Bellamy et al. (2007). Here a difference is made between primary barriers and the support of barriers. Primary barriers are directly involved in the causal chain, while the support of barriers will influence the primary barrier quality.

Guldenmund et al. (2006) divided barriers into three elements, meaning detection by a sensor, diagnosis and action. All three barrier elements are supported by management delivery systems as shown in Figure 4.2. This bowtie is an adapted version of the original bowtie metaphor. The barrier elements are drawn in series for simplicity reasons. The first barrier element is a sensor which can diagnose the hazard. It needs regular maintenance and inspection to fulfil its function. Both the Maintenance department and the department for testing of safety critical equipment (SCE) work according predefined procedures. The second barrier element is for logic solving or decision purposes whereas the third element relates to an automated (system) or manual action. In the example of Figure 4.2 the second barrier element is implemented as a

standard operating procedure (SOP) to follow-up on an alarm. The standard operation procedures of the plant are kept up to date and stored in a datafile. The third barrier element is an action carried out by an operator who is trained by the plant instructors. In this case the first barrier element is technical and the other two are non-technical. They are drawn with a thinner line to indicate their lower reliability. The management delivery systems supporting the primary barriers are also considered to be non-technical as their way of working is based on work processes and procedures.

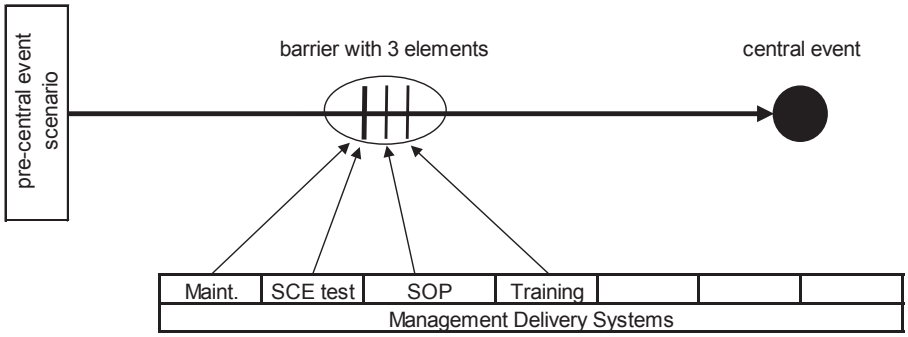

Fig. 4.2, relation of management delivery systems and barriers
(Maint.: maintenance; SCE: safety critical equipment; SOP: standard operating procedure)

Primary barriers may consist of both technical and non-technical barrier elements, with non-technical ones being regarded as work processes and procedures in which manual handling or decision making is predominant. Secondary or supporting barriers as part of the management delivery systems are non-technical in nature. In the elaborated examples below only the primary barriers are considered for further assessment.

Hoedemakers' investigation (2016) on major causes of mechanical failure incidents was aimed at the left-hand side of the bowtie. Three out of four major causes from his research have been considered in the below described method. Scenarios from maintenance activities have been excluded as they are hard to define and managed via other work processes.

The research was conducted on an ammonia plant of OCI Nitrogen, and focussed on scenarios related to mechanical integrity, like material degradation and corrosion of the main static equipment. A multi-disciplinary team assessed the construction and material choice, understood the mechanical failure scenarios, and explained the deviations in the operation of the various process units (such as start-up and

shutdown). In the team, expertise was present on the (chemical) process, construction and used materials of the process units, material degradation and corrosion, and the performance of inspections. Also, incidents occurred at OCI Nitrogen and other ammonia manufacturers were investigated to obtain likelihoods of the different mechanical failure scenarios. In addition, the start-up and shutdown of process units, and operational management were extensively discussed with the control room operators. These discussions gave insight in various process deviations.

Figure 4.3 shows the flow chart that was used to assess the process units, which have been selected in a preliminary sub-study (Schmitz et al., 2018) as described in chapter 3. The flow chart aims to include mechanical failure scenarios for both normal and deviating operational modes such as starting and stopping but also, for example, catalyst reductions.

In step 4 of Figure 4.3 the likelihood of the failure mechanism is divided into four groups:

- Very probable. The mechanical failure scenario has already occurred in the concerned process unit (mostly without major or catastrophic failure);
- Probable. The mechanical failure scenario has not occurred yet, but it seems probable based on the current conditions or in case of a minor deviation from current operation. External casuistry can also indicate the likelihood of the failure mechanism;
- Improbable. The mechanical failure scenario will probably not occur but cannot be excluded. The failure mechanism will only occur in case of major (process) deviations;
- Very improbable. The mechanical failure scenario will not occur and is excluded from further consideration.

An early warning detection (steps 5 and 5a) provides an indication whether a mechanical failure scenario will occur. The combination of an early warning detection and a high-quality monitoring (step 6) functions as a full barrier if there is a proper procedure in place which includes follow-up analysis to investigate the potential threat.

In step 7, a criticality calculation is used to assess whether additional barriers are required, or existing barriers need improvement. The criticality C is determined by the likelihood L of the mechanical failure scenario, the quality D of the detection and monitoring of the mechanical failure scenario, and the reliability B of the barriers using the formula: $C = L \times D \times B$. Table 4.1 shows the numerical values for L, D, and B against their descriptions, which are qualitative and not quantitative. The qualitative descriptions can be justified because it is a concept.

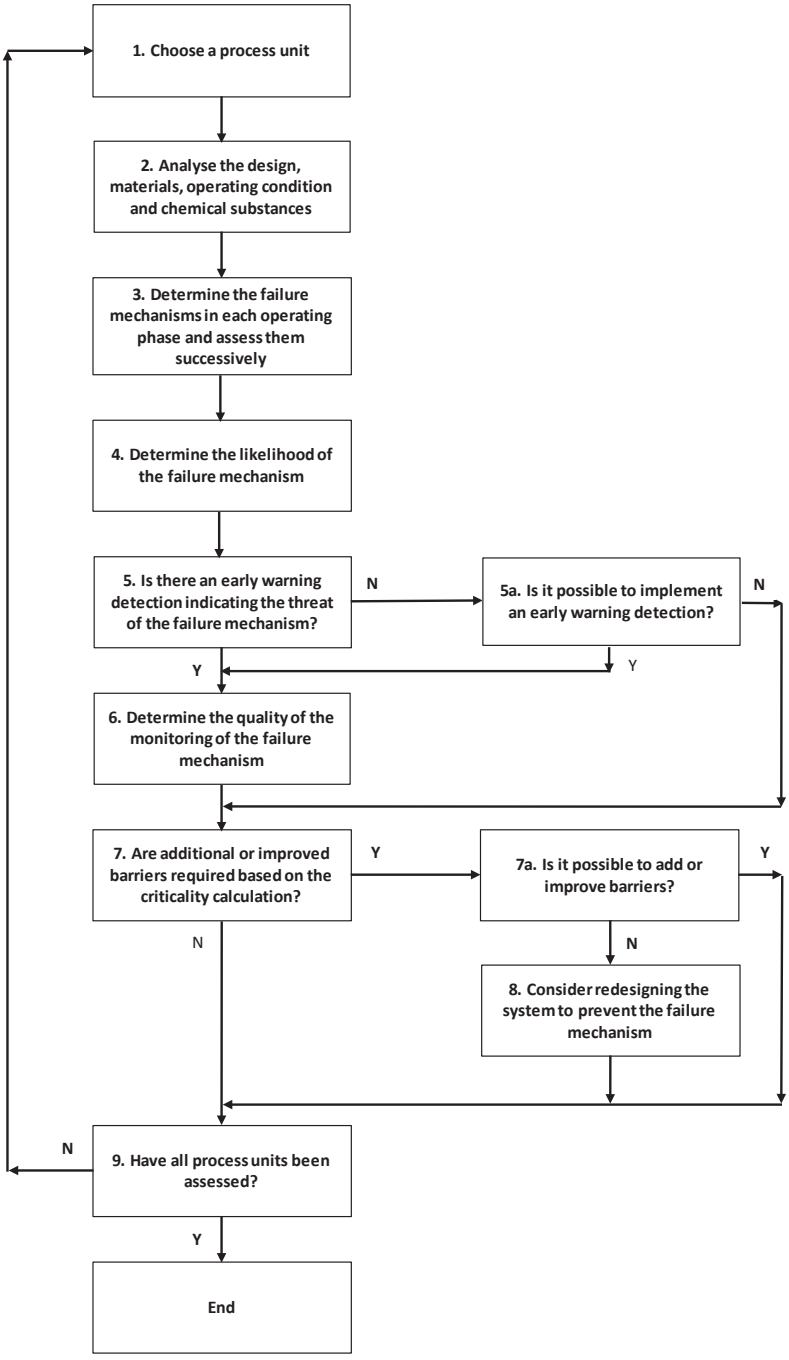

Fig. 4.3, process unit assessment flow chart

Table 4.1 – Numerical value of likelihood of the mechanical failure scenario (L), quality of detection and monitoring of the mechanical failure scenario (D) and reliability of barriers (B)

	1	2	3	4
L	Very improbable	Improbable	Probable	Very probable
D	Very good	Good	Reasonable	Unreasonable or not present
B	Very good	Good	Reasonable	Unreasonable or not present

The criticality is a number between 1 and 64. Based on examples and case studies it was determined that (very) probable scenarios at least need two good independent protection layers (IPL's) to consider them as sufficiently safe. This comes down to a criticality of 16 or lower. The criticality of a very probable failure scenario (L = 4) safeguarded by two good barriers (B =2) equals 16 (L x B_1 x B_2 = 4 x 2 x 2). When protected even better, meaning one very good and one good barrier, the criticality equals 8 (4 x 1 x 2). The threshold of 16 may seem somewhat conservative as most companies would opt for the ALARP principle (as low as reasonably practicable) in their risk assessment.

Table 4.2 is a non-exhaustive list with examples of the quality (in the sense of reliability) of barriers and detections applied at OCI Nitrogen. The table provides direction for barriers and detections that are already in place or which can be implemented. It is the team's responsibility to determine the quality, and reliability of barriers and detections. This should be assessed on a case-by-case basis.

If the mechanical failure scenario does not have enough barriers and the implementation of additional barriers is not possible, a redesign should be considered in accordance with step 8 of Figure 4.3. A redesign could be accomplished by a different material choice, a change in process conditions or altered start-up or shutdown procedures in order to prevent a major or catastrophic failure of the process unit caused by the assessed mechanical failure scenario.

Table 4.2 – Qualitative indication of barriers and detections

Quality of the barrier or detection	Value of D or B	Examples
Very good	1	• Covered with sheet steel (cladding, a uniform binding of a protective metal cover) • Distribution pipe to prevent erosion caused by intruding gas • SIL2 instrumental protection
Good	2	• Covered with sheet steel (lining, a local binding of a protective metal cover) • Covered with heat-resistant stone and/or plaster (refractory) • SIL 1 instrumental protection • Safety critical work instruction or procedure, procedural safeguards, alarm with management attention
Reasonable	3	• Coating, preservation • Non-SIL instrumental protection • Normal work instruction or procedure, alarm with operator attention
Unreasonable or none	4	

Finally, a bowtie is set up showing the initiating event in the left part and the preventive barriers, which should prevent the occurrence of a loss of containment and/or energy in the central event.

4.4 DATA COLLECTION AND ANALYSIS

Two scenarios of an ammonia process unit were examined and schematically shown as the left part of the bowtie (Figures 4.5 and 4.7). The presence and quality of barriers and early warnings (detection) was assessed, and it was determined whether improvements were necessary.

4.4.1 Scenario 1, start-up heater, thermal fatigue

During start-up, the start-up heater is used to heat synthesis gas, a mixture of hydrogen and nitrogen in a ratio of 3:1, from approx. 270 °C to approx. 400 °C. The process flow for the start-up heater and synthesis reactor is shown schematically in Figure 4.4. The synthesis gas is provided by the synthesis gas compressor and has a pressure of approx. 200 bar. When the supply to the start-up heater (via valve MEV3001) is opened, the temperature in the supply line to the start-up heater rises quickly due to the hot synthesis gas at 270 °C. When there is enough flow, the start-up heater is ignited to further heat the synthesis gas until the synthesis reaction is activated. When the synthesis reactor is generating enough heat from its reaction to heat up the supplied gas, the burner in the start-up heater will be switched off and the start-up heater taken out of line by closing valve MEV3001.

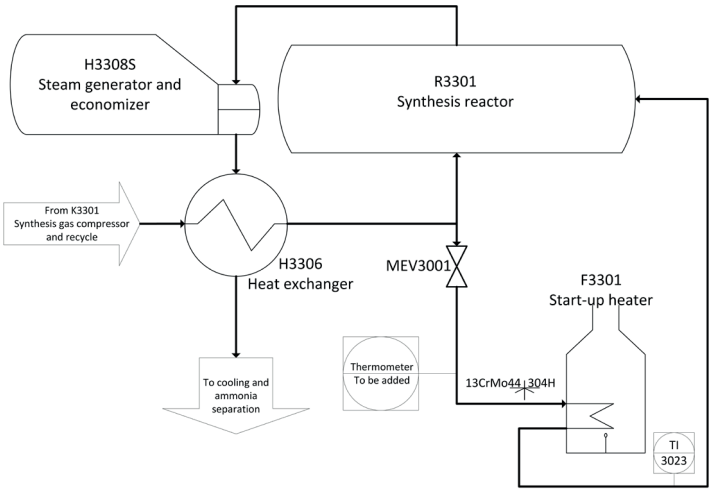

Fig. 4.4, start-up heater and synthesis reactor

The supply line of the start-up heater is made of Cr-Mo steel (13CrMo44), whereas the coils are made of austenitic steel (304H). This means that there is a dissimilar welding joint (also known as black & white welding joint) in the transition of the supply line to the inlet header. This welding joint is not designed for high levels of stress caused by large temperature gradients, also known as thermal fatigue, i.e. fatigue involving cyclic, plastic deformation and eventually cracking. A trend of the temperature of the outlet of the start-up heater (TI3023) shows that during start-up, temperature rises at a rate of approx. 200 °C/h for the first half hour after opening of the supply valve and then levels off. The temperature of the dissimilar welding joint experiences quite a similar temperature gradient in this operating phase. This creates unacceptable material stresses in the mentioned welding joint.

The inlet and outlet header, made of the same material as the coils (304H), contain little cracks which are, among other things, associated with thermal fatigue and are due to the design. There is external casuistry, but this is not related to the welding joint described above.

In the current situation:

- The work instruction only mentions a temperature rise for the synthesis reactor of 50 °C per hour. It does not mention anything about the start-up heater, the supply and discharge pipes or headers;
- There is no temperature point in the supply of the start-up heater located at the welding joint;
- Supply valve MEV3001 cannot be operated from the control room. This makes it difficult to control the heating up of the supply and discharge pipes and headers;
- Cracks at the dissimilar welding joint of the supply line have not been detected so far. Due to the present high temperature gradients the mechanical failure scenario is classified as probable (step 4 of the flow chart).

Given the fact that there is no early warning in the current situation, it is checked, in accordance with step 5a of the flow chart, whether it can be implemented. This seems possible by installing a temperature point in the supply line of the start-up heater, which generates an alarm when the temperature rises over 50 °C (122 F) per hour. Based on this alarm, a fitness for service (FFS) analysis should be initiated (according to the procedure). If deemed necessary, an inspection may determine whether a repair is necessary. If the procedure receives management attention in accordance with Table 4.2, the procedure may be classified as good (step 6). In order to receive this classification, the procedure should be described and included in the safety management system and have a certain degree of management involvement during its use. The alarm will not only be visible in the control room but could also be sent to

those responsible for integrity and asset management. In addition, this alarm could be discussed in the daily operation meeting.

In step 7, the criticality must be determined to check whether additional or improved barriers are needed. It is assumed that, in the current situation, there is no barrier in the mechanical failure scenario of thermal fatigue (so B=4). With a probable mechanical failure scenario (L=3) and good detection/monitoring (i.e. a temperature gradient alarm) (D=2), the criticality equals 24 (C = L x D x B = 3 x 2 x 4). As the criticality is higher than the threshold of 16, the scenario is currently insufficiently safeguarded and requires additional barriers (step 7a). To lower the criticality this (probable) scenario should be provided with an additional good barrier on top of the proposed detection/monitoring (which is classified as good). This can be achieved by controlling supply valve MEV3001. Although automatic control is preferred, MEV3001 can also be manually operated from the field in accordance with the instructions of the operator in the control room (as indicated in Figure 4.5). To achieve a good barrier, the current operating instruction should be classified as safety critical. This provides the scenario with two good barriers (a temperature gradient alarm and a safety critical procedure for controlling MEV3001), which means that the criticality of the scenario is sufficiently low (C = L x D x B = 3 x 2 x 2 = 12).

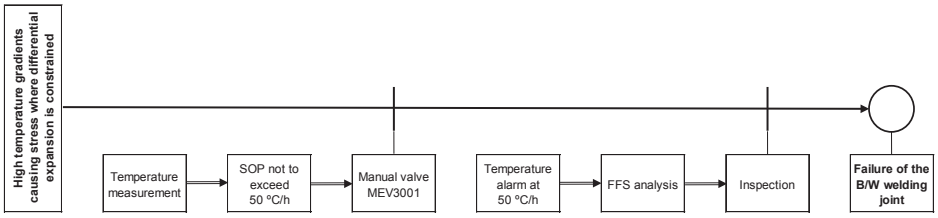

Fig. 4.5, left part of the bowtie of thermal fatigue in the start-up heater
(SOP: standard operating procedure; FFS: fitness for service; B/W: black & white)

Figure 4.5 shows a bowtie for the scenario with the new and independent barriers, which work out as a 1-out-of-2 system. Both barriers are (mostly) non-technical and based on an instruction or procedure. The individual barriers are constructed as a 3-out-of-3 system, in other words: all three elements must work in order to ensure the availability of the barrier.

As a result of this sub-study, the safeguarding system of the above scenario will be improved to prevent thermal fatigue. Several temperature measurements up and downstream the start-up heater are being installed to allow the start-up heater to heat up more slowly, and a draft standard operating procedure has been drawn up that

guarantees to stay within the integrity operating window.

4.4.2 Scenario 2, steam superheater, creep and Nelson hydrogen attack

In the steam superheater, high pressure steam of 125 bar is superheated by means of hot process gas, which consists of about 35% hydrogen. The process gas decreases from 600 °C to 475 °C. Figure 4.6 shows the flow of the process gas which is led upwards via the internal heat exchanger and returns along the wall after which it exits on the right-hand side. The process gas that leaves the internal heat exchanger at the top passes the internal brickwork (refractory) that protects the outer wall against a too high temperature. Two time-related mechanical failure scenarios have been identified, which can cause the steam superheater to fail catastrophically, i.e. a sudden, unstoppable, total loss of the containment. In the case of damaged refractory, the outer wall can be exposed to excessive heat for a prolonged period of time which may lead to creep (slow plastic deformation under the influence of stress and temperature) and Nelson hydrogen attack (diffusion of H-atoms into the metal which react with carbides to methane and whereby the larger, trapped methane may cause cracks when exceeding the yield limit). A major damage of the internal refractory exposes a large part of the wall to hot process gas, which can cause the wall to weaken and rapidly lead to failure of the steam superheater. Since a major damage is always preceded by small, hard-to-see defects, the scenario is focussed on the latter.

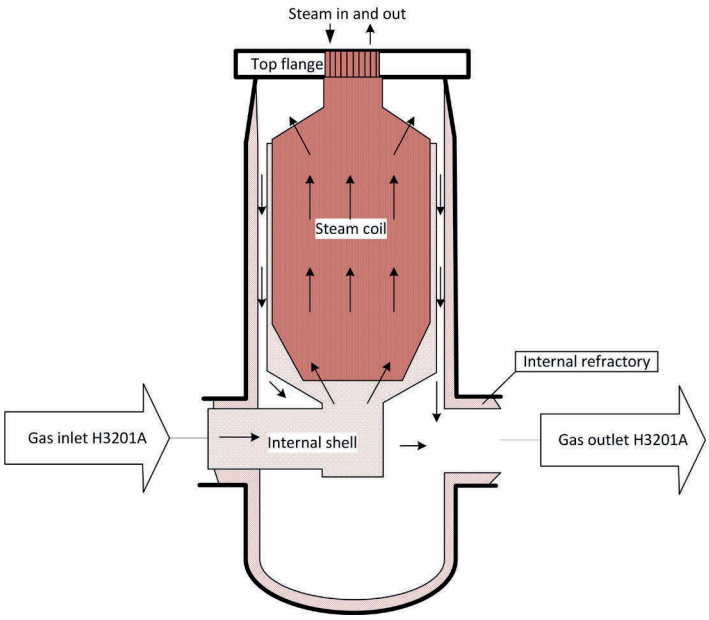

Fig. 4.6, steam superheater

In contrast to the upstream waste heat boiler, few incidents at other ammonia producers have been reported regarding this equipment. Singh et al. (2003) report internal pipe leakages as a result of under deposit corrosion due to phosphate deposits. Given the construction, however, it is not possible for a leak of steam to affect the refractory. Own casuistry shows that although minor defects have been detected in the refractory, this has not led to a local overheating of the wall. Larger damage to the wall that can lead to hot spots, however, cannot be ruled out. Based on experiences with other equipment provided with refractory this scenario is estimated to be probable (L=3).

In case of refractory defects, hot spots can occur on the outside of the wall. Although they can be observed visually during an operator round, they can easily be overlooked. The quality of the current detection and monitoring of the mechanical failure scenario is classified as poor (D=4). The internal refractory is inspected every four years during a turn-around. As indicated above, only minor defects have been found. This barrier is therefore qualified as good (B=2). In the current situation, the criticality C (L x D x B) is equal to 24 (3 x 4 x 2). Therefore, the scenario must be provided with additional or improved barriers.

The heater can be provided with indicator paint on the outside, which discolours on the hot spot due to the higher surface temperature where the internal refractory is no longer intact. Indicator paint reduces the chance that hot spots are overlooked. In addition, the outer wall can be provided with several temperature measurements that alarm at a high temperature. In case of a discoloured indicator paint and / or one or more temperature alarms, the wall can be examined with an IR camera in order to determine whether a fitness for service (FFS) analysis should be carried out. This should then indicate whether an inspection is necessary. The inspection should reveal the need for replacement or repair. If this procedure receives management attention, the quality of the detection and monitoring of the mechanical failure scenario (D) can be regarded as good in accordance with equivalent procedures within the company. The procedure should not only be included in the safety management system but also contain management involvement when in use. In addition, the temperature alarms should not only raise an alarm in the control room but also be passed on to those who are responsible for the integrity and asset management. The criticality in the improved situation equals 12 (C = L x D x B = 3 x 2 x 2) which makes the scenario sufficiently safe. No additional barriers are required if the detection and monitoring are implemented as proposed above.

Figure 4.7 shows the bowtie of the scenario with the newly implemented detection and monitoring. Together with the internal refractory, this forms a 1-out-of-2 system, i.e. the scenario is provided with two independent barriers connected in series. The

existing internal refractory is a technical barrier, whereas the proposed detection and monitoring of the mechanical failure scenario is a non-technical, procedural barrier. The latter consists of a detection via the indicator paint, temperature alarms and IR measurement after which a procedure with management attention should ensure monitoring of the mechanical failure scenario in the form of an FFS analysis and inspection. The temperature alarms can be seen as an early warning regarding the mechanical failure scenario creep and Nelson hydrogen attack.

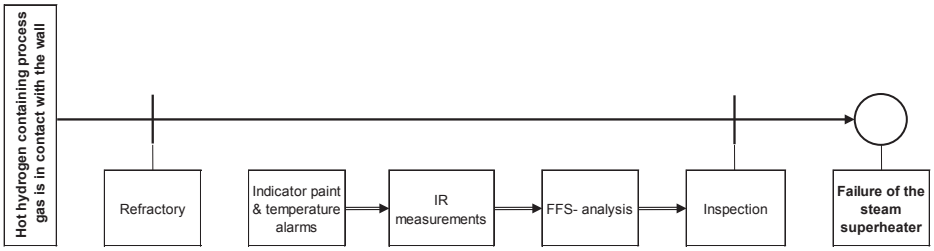

Fig. 4.7, left part of the bowtie regarding creep and Nelson hydrogen attack of the steam superheater (IR: infrared; FFS: fitness for service)

As a result of this sub-study, the steam superheater has been equipped with 5 temperature alarms indicating a too high wall temperature. In addition, the wall temperature is measured on a weekly basis using IR. In the coming turnaround, the relevant parts will be provided with indicator paint.

4.5. DISCUSSION

This sub-study on mechanical failure scenarios has the following important results:

1) Important, missing information about design, material choice and inspection methods, but also potential incidents have been revealed;
2) Additional scenarios have been found by, in contrast with previous assessments, looking at all operational modes;
3) Part of the mechanical failure scenarios have now been judged as probable because the quality of the barriers has been taken into account;
4) RBI may not always lead to the timely execution of all necessary inspections;
5) Bowties clearly show the early warnings of a developing accident scenario.

Poor design, incorrect assembly or repair and incomplete or inadequate inspections have not been considered. The time dependency of mechanical failure scenarios is not included either. However, the operation of the plant outside the operating window

was looked at intensively, especially in start-up and shut-down situations. Many mechanical failure scenarios are susceptible to these deviating operations, which are often not considered in the design. The expected (mechanical) lifespan will be considerably shortened when the process is operated outside the operating window, which is referred to as the integrity operating window by Lagad and Zaman (2015). As the definition of Dokas et al. (2013) shows, early warnings can be used to draw up such an integrity operating window.

The elaborated examples show how mechanical failure scenarios, like material degradations, relate to ageing as they take place over time. Early warnings and barriers (both technical barriers and non-technical, procedural barriers) have been added and improved the scenarios as they can stop the development. Ageing as such is a much wider concept and has not been considered as this chapter focussed on mechanical failure scenarios only.

Increased temperatures and temperature gradients have proven to be important input parameters for the assessment. Some of the critical mechanical failure scenarios like creep, thermal fatigue and Nelson hydrogen attack are related to them. These scenarios may become probable during start-up and shut down when the process is strongly deviating from normal operating conditions.

Inspections represent an integral part of the condition monitoring of process equipment (Utne et al., 2012). The bowties show that they can be carried out when initiated by early warnings. These process indicators reveal that the mechanical failure scenario concerned may take place. Then a fitness for service analysis provides detailed information for closer inspections. If such an inspection is considered urgent and cannot be performed during operation, the installation must be shut down. The speed at which and the extent to which the mechanical failure scenario is taking place, depends on several factors which can be hard to oversee. A further elaborated consideration is not included in this sub-study.

Two examples have been used to show how mechanical failure scenarios can be detected. Some mechanical failure scenarios can be monitored during operation and some need to be monitored during regular or interim inspections. The quality of the inspection has a significant impact on the reliability of the results. The results of the inspections determine to what extent the mechanical failure scenario has already developed. Not only the quality of the inspections can be used as process indicators (Hassan and Khan, 2012), but also the result of the inspections. Inspections can be regarded as barriers, if they are executed timely and properly.

4.6 CONCLUSIONS

The main question raised in this chapter is how major process safety incidents caused by mechanical failure of static process units can be anticipated and prevented at OCI Nitrogen's ammonia plants.

In response, the primary focus is on (very) probable scenarios, which either have occurred at OCI, or are known from the international literature on accidents at ammonia plants. These scenarios are visualised by bowties. The risk-based approach developed in this study provides information on the number and quality of necessary barriers to stop the impact of these scenarios.

The existing detectors at temperature, pressure and flow, show whether enough information is present to follow the development of these scenarios. Early warnings can be implemented which may serve as an indicator, showing the development of the scenario. How these indicators relate to the likelihood of the central event will be discussed in more detail in the next chapter.

The method used in this sub-study is somewhat reminiscent of the model for risk-based inspections (RBI): inspections are carried out when it appears necessary based on a risk assessment. However, this is only partly true. The difference is that in this method inspections are not necessary until there is a demonstrable likelihood that the failure mechanism and thus the scenario is taking place. On the contrary, RBI is a systematic method in which an inspection programme is established beforehand based on a risk assessment (API, 2016). In the light of the shift from breakdown maintenance to preventive and predictive maintenance and RBI, inspections based on early warnings could be a new step in the field of maintenance efficiency.

The method in this chapter is based on barrier management of alarms, at scenario level. Further research is needed to also design indicators at other levels that can provide advance information on major accident processes, starting with the management delivery system as the next higher aggregation level.

4.7 REFERENCES

American Petroleum Institute (API). (2016). *Risk-Based Inspection*. API RP 580, third ed. Washington, US: API Publishing Services.

American Petroleum Institute (API). (2019). *Mechanical integrity: Fixed equipment standards & recommended practices*. API Publishing Services, Washington DC. Retrieved from https://www.api.org/oil-and-natural-gas/health-and-safety/refinery-and-plant-safety/process-safety/process-safety-standards/mechanical-integrity-standards.

Bellamy, L.J., Ale, B.J.M., Geyer, T.A.W., Goossens, L.H.J., Hale, A.R., Oh, J., Mud, M., Bloemhof, A., Papazoglou, I.A., & Whiston, J.Y. (2007). Storybuilder – A tool for the analysis of accident reports. *Reliability Engineering and System Safety, 92*, 735-744. http://dx.doi.org/10.1016/j.ress.2006.02.010.

Centre for Chemical Process Safety (CCPS). (2018). *Dealing with aging process facilities and infrastructure*. New York, US: AIChE.

Chevreau, F., Wybo, J., & Cauchois, D. (2006). Organizing learning processes on risks by using the bow-tie representation. *Journal of Hazardous Materials, 130*, 276-283. http://dx.doi.org/10.1016/j.jhazmat.2005.07.018.

Cockshot, J.E. (2005). Probability Bow-Ties – A Transparant Risk Management Tool. *Process Safety and Environmental Protection, 83*(B4), 307-316. http://dx.doi.org/10.1205/psep.04380.

COMAH. (2010). Ageing Plant Operational Delivery Guide. Retrieved from https://www.yumpu.com/en/document/view/16634806/competent-authority-ageing-plant-operational-delivery-guide-hse.

Dokas, M., Feehan, J., & Syed, I. (2013). EWaSAP: An early warning sign identification approach based on a systemic hazard analysis. *Safety Science, 58*, 11-26. http://dx.doi.org/10.1016/j.ssci.2013.03.013.

DNV. (1996). *Risk management of ageing process plants*. DNV Research Report 96-2001.

Groeneweg, J. (1992). *Controlling the controllable, the management of safety*. Leiden, The Netherlands: DSWO Press.

Guillaume, E. (2011). *Identifying and responding to weak signals to improve learning from experiences in high-risk industry* (Doctoral's thesis). Retrieved from https://repository.tudelft.nl/islandora/object/uuid:f455e8a0-cce5-4a36-8a98-f83371dc2a2a.

Guldenmund, F., Hale, A., Goossens, L., Betten, J., & Duijn, N. (2006). The development of an audit technique to assess the quality of safety barrier management. *Journal of Hazardous Materials, 130*, 234-241. http://dx.doi.org/10.1016/j.jhazmat.2005.07.011.

Hassan, J., & Khan, F. (2012). Risk-based asset integrity indicators. *Journal of Loss Prevention in the Process Industries, 25*, 544-554. http://dx.doi.org/10.1016/j.jlp.2011.12.011.

Hoedemakers, G. (2016). *Mechanische integriteitsrisico's in chemische procesinstallaties: Hoe houden we de tijger in zijn kooi?* (Master's thesis).

HSE. (2006). *Plant ageing*. RR509. Retrieved from http://www.hse.gov.uk/research/rrhtm/rr509.htm.

HSE. (2007). *Key Programme 3. Asset Integrity Programme*. Retrieved from http://www.hse.gov.uk/offshore/kp3.pdf.

HSE. (2010). *Managing Ageing Plant, A Summary Guide*. Retrieved from https://www.academia.edu/33500484/Managing_Ageing_Plant_A_Summary_Guide_HSE_Books_Health_and_Safety_Executive.

IAEA. (2017). *Handbook on Ageing Management for Nuclear Power Plants*. Safety Guide No. NP-T-3.24. Retrieved from https://www-pub.iaea.org/MTCD/Publications/PDF/P1738_web.pdf.

Kletz, T. (1988). On the need to publish more case histories. *Plant/Operation Progress, 7*, 145-147.

Knegtering, B., & Pasman, H. (2013). The safety barometer. How safe is my plant today? Is instantaneously measuring safety level utopia or realizable? *Journal of Loss Prevention in the Process Industries, 26, 821-829*. http://dx.doi.org/10.1016/j.jlp.2013.02.012.

Lagad, V., & Zaman, V. (2015). Utilizing Integrity Operating Windows (IOWs) for enhanced plant reliability & safety. *Journal of Loss Prevention in the Process Industries, 35*, 352-356. http://dx.doi.org/10.1016/j.jlp.2014.10.008.

OGP. (2008). *Asset integrity – the key to managing major incident risks*. Report No. 415. Retrieved from https://www.scribd.com/document/391778284/OGP-Report-415-Asset-integrity-the-key-to-managing-major-incident-risks-December-2008-pdf.

Øien, K., Utne, I., & Herrera, I. (2011a). Building safety indicators I theoretical foundations. *Safety Science, 49*, 148-161. http://dx.doi.org/10.1016/j.ssci.2010.05.012.

Øien, K., Utne, I., Tinmannsvik, R., & Massaiu, S. (2011b). Building safety indicators II applications. *Safety Science 49*, 162-171. http://dx.doi.org/10.1016/j.ssci.2010.05.015.

Onderzoeksraad Voor Veiligheid (OVV). (2018). *Chemie in samenwerking – Veiligheid op het industriecomplex Chemelot*. Retrieved from https://www.onderzoeksraad.nl/nl/page/4707/chemie-in-samenwerking---veiligheid-op-het-industriecomplex-chemelot.

Perrow, C. (1984). *Normal accidents. Living with high-risk technologies*. New York, US: Basic Books.

Reason, J. (1987). The Chernobyl errors. *Bulletin of the British Psychological Society, 40*, 201-206.
Reason, J. (1990). *Human error*. Cambridge, UK: University Press.
Reason, J. (1997). *Managing the risks of organizational accidents*. Abingdon, UK: Taylor & Francis.
Ruijter, A. de, & Guldenmund, F. (2016). The bowtie method: A review. *Safety Science, 88*, 211-218. http://dx.doi.org/10.1016/j.ssci.2016.03.001.
Schmitz, P., Swuste, P., Theunissen, J., Reniers, G., Decramer, G., & Uijterlinde, P. (2018). Een aanpak voor het bepalen van een realistische ranking van de gevaarlijkste procesonderdelen van het ammoniakproductieproces. *Tijdschrift voor toegepaste Arbowetenschap, 2018*(2), 42-56.
Schmitz, P., Swuste, P., Reniers, G., & Van Nunen, K. (2019). Mechanical Integrity of Process Installations: an Assessment Based on Bow-Ties. *Chemical Engineering Transactions, 77*, 97-102. http://dx.doi.org/10.3303/CET1977017.
Singh, J., Varma, S.L., & Patel, B.M. (2003). Failures in Secondary Waste Heat Boilers. *AIChE Technical Manual 2003, Safety in ammonia plants and related facilities symposium, 44*, 109-116.
Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries, 19*, 494-506. http://dx.doi.org/10.1016/j.jlp.2005.12.004.
Swuste, P., Theunissen, J., Schmitz, P., Reniers, G., & Blokland, P. (2016). Process safety indicators, a review of literature. *Journal of Loss Prevention in the Process Industries, 40*, 162-173. http://dx.doi.org/10.1016/j.jlp.2015.12.020.
Swuste, P., van Gulijk, C., Zwaard, W., Lemkowitz, S., Oostendorp, Y., & Groeneweg, J. (2019). *Van veiligheid naar veiligheidskunde*. Alphen aan den Rijn, The Netherlands: B + B Vakmedianet.
SZW. (2016). *Ageing bij Brzo-bedrijven*.
TNO. (2015). *Literatuuronderzoek naar veroudering van installaties*. Retrieved from https://publications.tno.nl/publication/34626341/jB13ci/TNO-2015-R10878.pdf.
Turner, B. (1978). *Man-made disasters*. Oxford, UK: Butterworth-Heinemann.
Utne, I.B., Brurok, T., & Rødseth, H. (2012). A structured approach to improved condition monitoring. *Journal of Loss Prevention in the Process Industries, 25*, 478-488. http://dx.doi.org/10.1016/j.jlp.2011.12.004.
Vinnem, J.E. (2010). Risk indicators for major hazards on offshore installations. *Safety Science, 48*, 770-787. http://dx.doi.org/10.1016/j.ssci.2010.02.015.

5

PREDICTING MAJOR ACCIDENTS IN THE PROCESS INDUSTRY BASED ON THE BARRIER STATUS AT SCENARIO LEVEL: A PRACTICAL APPROACH[5]

5 The Chapter is based on the paper: Schmitz, P., Swuste, P., Reniers, G. & Nunen van, K. (2021). Predicting major accidents in the process industry based on the barrier status at scenario level: a practical approach. *Journal of Loss Prevention in the Process Industries, 71*, 104519. https://doi.org/10.1016/j.jlp.2021.104519, and was formatted and edited for this thesis.

ABSTRACT

This chapter investigates the development of (leading) indicators regarding the process safety performance of OCI Nitrogen's ammonia production process. The question is answered whether indicators can be derived from the barrier system status to provide information about the development and likelihood of the major accident processes in the ammonia production process.

The accident processes are visualised as scenarios in bowties, with the focus on the status of the preventive barriers on the left-hand side of the bowtie. Both the quality – expressed in reliability/availability and effectiveness – and the activation of the barrier system give an indication of the development of the accident scenarios and the likelihood of the central event. This likelihood is calculated as a loss of risk reduction compared to the original design. The calculation results in an indicator called "preventive barrier indicator", which should initiate further action. Based on an example, it is demonstrated which actions should be taken and what their urgency is.

5.1 INTRODUCTION

The aim of this chapter is to identify indicators which provide information about the major hazard accident scenarios of OCI Nitrogen's ammonia production processes. The former two chapters focussed on the 'ranking' of the most dangerous process parts of the ammonia production process (Schmitz et al., 2018) and the main static installation parts of the ammonia production process related to mechanical failure mechanisms (Schmitz et al., 2019a; b; 2020). The purpose of the previous two chapters is to select the most likely, hazardous scenarios of the ammonia production process as front-end loading for this chapter. This chapter describes the results concerning (preventive barrier) indicators, which aim to recognise and stop the development of scenarios at an early stage. The research question associated with this sub-research is:

> *Can indicators be derived – based on the status of the barrier system – that provide information on the development and likelihood of major accident processes in the ammonia production process?*

The associated sub-questions to be investigated are:
1) What is a barrier system?
2) How can the status of a barrier system be determined?
3) What is an indicator?
4) What are criteria for indicators?
5) What is the relationship between indicators and accident processes?

Accident processes that originate from working conditions are excluded in this sub-study. This chapter is exclusively concerned with potential incidents related to process safety and, in addition, only those that are major or catastrophic.

This chapter starts with definitions of indicators from the literature, followed by the barrier concept from the bowtie metaphor. Here quality aspects of barriers, barrier systems and their status are discussed, which are used to develop the preventive barrier indicator concept. This concept is applied to one of the major hazard scenarios of an essential equipment of the ammonia production, the loss of cooling of the post reformer.

5.1.1 Indicators

Process safety indicators have been the focus of many studies, but little empirical research has been published on it, as observed by Swuste et al. (2016). In contrast, many (petro) chemical companies measure their process safety performance and HSE (2006), CCPS (2011), Cefic (2011, 2016), OGP (2011) and ANSI/API (2010) have

set up guidelines to monitor process safety based on indicators. A distinction is often made between 'leading' and 'lagging' indicators. Where the former are proxies to hazards, barriers, scenarios and management factors, the latter provide information on the central, loss of containment or loss of control event and its consequences. The scientific literature questions this distinction (Swuste et al., 2016).

Leading indicators should provide information before an incident occurs and indicate the extent to which one deviates from an ideal situation. They can be considered as an early warning (Dokas et al., 2013; Knegtering and Pasman, 2013; Øien et al., 2011a, b; Vinnem, 2010). (Leading) indicators should monitor the level of safety, decide where and which action is necessary, and motivate operators to actually take the necessary action (Hale, 2009). In a guideline of the HSE (2006), leading indicators are a form of active monitoring aimed at a few critical parts of the risk management system. They should encourage the most important actions or activities to be carried out as intended.

This chapter emphasises the leading indicators and focusses on the barriers on the left-hand side of the bowtie. They should be defined to provide insight into the quality of the barriers and the development of scenarios (Swuste et al., 2016). To measure the safety level, the barrier quality and the scenarios must be actively monitored. This means that monitoring must be done continuously and at "real time".

5.1.2 Barriers

The bowtie model forms the basis of this chapter. The bowtie is a suitable model to visually map the course of accident scenarios (from cause to effect) and enables to include preventive and mitigating barriers (Schmitz et al., 2019a, 2019b). In the central event, a dangerous substance and/or energy is released in an uncontrolled manner and a state of uncontrollable hazard arises. Preventive barriers, as shown in Figure 5.1 on the left-hand side of the bowtie, should stop the accident processes at an early stage and avoid the central event from happening.

A barrier is anything that prevents causes from developing into consequences, including preventing the cause itself (Bellamy et al., 2007). If barriers are broken or not present, a scenario can develop into a central event, or the central event can develop into unwanted consequences.

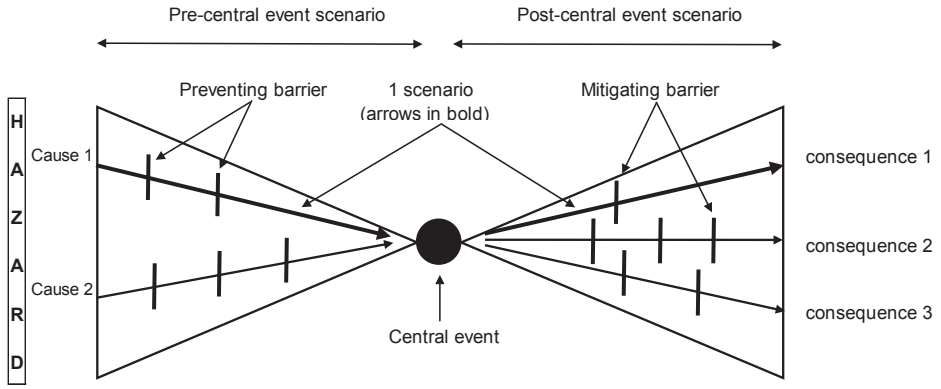

Fig. 5.1, the bow-tie model (Schmitz et al., 2019b)

Barriers can be classified in different ways: Sklet (2006) distinguishes between physical and non-physical, while Hollnagel (2008) classifies them according to function or purpose and Vinnem (2010) opts for technical and operational barrier elements. Barriers are usually made up of three elements: a sensor, a decision maker and a final element or action taker, referred to by Guldenmund, Hale, Goossens, Betten and Duijm as detect, diagnose and act as main barrier tasks (Guldenmund et al., 2006). A barrier only works if all three elements are functioning. In this sense, a barrier can be regarded as a 3-out of-3 system.

A barrier system is the set of existing barriers that must prevent causes from developing into consequences. The barrier system in this chapter is limited to the existing preventive barriers (on the left-hand side of the bowtie), which should prevent causes from developing into the central event of the accident process. To achieve this, the (preventive) barrier system must be in place and be of good quality. Different parameters indicate something about the quality of barriers. According to Sklet (2006), Vinnem (2010) and Badredine et al. (2014), the quality of barriers is determined by:

- Effectiveness (functionality, capacity): the ability of a barrier to perform its necessary function correctly;
- Reliability: the likelihood that a barrier will be able to perform its necessary function, given the aforementioned conditions, for a specified period of time;
- Availability: the chance that a barrier will function at any point in time;
- Costs: the costs of keeping the barrier functional, reliable and available;
- Robustness: the ability to continue to function in the event of (extreme) environmental influences, such as an incident;
- Response time: the time from activation of the barrier to the execution of the

intended function;
- "Trigger": the event or condition that activates the barrier.

The above parameters characterise the quality of a barrier. They are "qualifiers", requirements that a high-quality barrier must meet. The quality of barriers might decrease because of use, wear, pollution, degradation, damage or defects. In order to measure the likelihood that a scenario will develop into a central event, it is necessary to monitor the decline in quality of the barriers. This monitoring can be done by selecting relevant parameters capable of mapping the lowering in barrier quality. This means that these parameters must be sensitive to change, something that several authors emphasize as an important criterion (Hale, 2009; Vinnem, 2010; Sinelnikov et al., 2015). The quality parameters, effectiveness, reliability and availability are the only ones that vary sufficiently over time and can present the possible deterioration in quality of a barrier. In line with Sklet's (2006) approach, this chapter considers reliability and availability under one heading. Where effectiveness is a barrier's ability to perform its necessary function correctly, reliability/availability means the likelihood that a barrier will function at any point in time. Sklet outlines the difference using an emergency shutdown (ESD) system as an example. Internal leakage of an ESD valve reduces effectiveness while not affecting reliability/availability. A barrier must be both reliable/available and effective to stop the development of an accident scenario.

Reliability/availability and effectiveness have been selected in this chapter to monitor the quality of a barrier or barrier system. This is in line with the views of Landucci, Argenti, Tugnoli and Cozzani, who also assess the performance of barriers based on availability and effectiveness (Landucci et al., 2015). By monitoring these parameters, an image of the quality status of a barrier or barrier system can be given, which can be translated into a likelihood of an accident scenario as explained in section 5.2.2.

Preventive and corrective maintenance, inspection and test programmes, and management and administrative aspects influence the reliability/availability and effectiveness of technical barrier systems (Vinnem et al., 2006). Within the (petro) chemical industry it is required to maintain, inspect and test barriers according to a predefined schedule. Not (properly) or not timely executing such a programme can affect both the reliability/availability and the effectiveness of a barrier. This chapter assumes that the maintenance, inspection and testing of a barrier is of good quality and that the barrier is reliable/available and effective after maintenance. In addition, testing should meet the specific conditions of the plant as much as possible. Lees (in Mannan, 2005) indicates that a barrier may have been approved in a workshop but may not function properly in the actual installation.

Besides the influence of maintenance, inspection and testing, there are additional aspects that can affect reliability/availability and effectiveness. A barrier may be not reliable/available and/or not effective for various reasons: due to a defect or by a (deliberate) inactivation. A defective barrier will not function when there is a demand and/or will not perform the intended function correctly and is therefore by definition not reliable/available and/or not effective. SIL (safety integrity level) qualified instrumental barriers contain a degree of self-diagnosis in their design as some of the defects are automatically detected and reported. Type B instruments are preferably used in SIL-qualified safety loops for their high diagnostic coverage as they are based on (programmable) electronic technology. Because of these diagnostics, errors can be detected that would otherwise remain latent (Houtermans, 2014). Mechanical safety barriers, on the other hand, usually do not have such degree of self-diagnostics. A defective mechanical safety device is only noticed at its next inspection or test or when an incident occurs which the mechanical safety device should have prevented.
A barrier that has been deliberately inactivated is not reliable/available. This is done, for example, for performing maintenance, an inspection or a test. For instrumental safeguards, this is often indicated by the term "overriding". "Overriding" can be done in different ways, but in all cases an overridden barrier no longer performs its function.
In summary, the parameters reliability/availability and effectiveness provide a picture of the quality of a barrier. The following has been assumed:

- Maintenance, inspection and testing of a barrier is of good quality;
- A barrier that is put into operation after maintenance, inspection and testing is reliable/available and effective;
- Delayed maintenance, inspection and testing affects reliability/availability and effectiveness to some extent;
- A barrier that is overridden or defective is not reliable/available and/or not effective and therefore no longer able to stop the development of an accident scenario.

To increase readability, the barrier qualification 'reliable/available and/or effective' is replaced by 'trustworthy' from here. This also counts for 'not reliable/available and/or not effective' and 'possibly not reliable/available and/or not effective', which is replaced by 'not trustworthy' and 'possibly not trustworthy', respectively. A barrier is trustworthy when it is maintained, inspected and/or tested as scheduled, and not trustworthy when it is inactivated or defective. In the area in between there may be reasons to assume that the barrier is possibly not trustworthy due to lagging or lacking maintenance, inspection and/or testing, or otherwise.

5.2 METHODOLOGY

5.2.1 Preventive barrier indicator

Based on the above quality parameters reliability/availability and effectiveness, a barrier can be (1) trustworthy, (2) possibly not trustworthy or (3) not trustworthy. The barrier status in this case indicates that (1) the barrier is working as designed, (2) may not be working or (3) is not working at all. In this way, the barrier status provides information about the likelihood that the scenario can develop into a central event.

In addition to trustworthy, possibly not trustworthy, and not trustworthy, a barrier can also be 'actived' or 'not activated'. In this chapter it is assumed that an activated barrier not only acts at a demand (reliable/available), but also performs the predefined function within the required response time (effective). If an available/reliable barrier is activated, but proves to be ineffective, the scenario will develop further. In the event of an activated barrier, which is not only available/reliable, but also effective, the development of the accident scenario has stopped, but attention is required because the scenario has been initiated. Table 5.1 shows the possible (preventive) barrier statuses and links them to symbols. These symbols are used as abbreviations in this chapter.

Table 5.1, possible barrier statuses and associated symbols

Barrier status		Barrier symbol
Trustworthy and not activated		V
Possibly not trustworthy	Not maintained, inspected or tested on time	?
Not trustworthy	Overridden or defective	Θ
Trustworthy and activated		!

Trustworthy barriers will, when a scenario is initiated, be activated and stop the scenario before the central event occurs. The scenario has developed up to the activated barrier(s) and no further. Based on the activated barrier(s), the position can be determined in which the scenario is currently located. The position in the scenario indicates the remaining barriers that protect against the central event. The status of the remaining barriers – based on their quality parameters reliability/availability and effectiveness – can provide information about the likelihood that the scenario could have developed into the central event.

5.2.2 Relative risk reduction

In section 5.1.2 it was concluded that improper or not timely implementation of the maintenance, inspection and test programme can adversely affect the trustworthiness of a barrier. Assuming that the maintenance, inspection and test programme is

performed to a high standard, this raises two questions: What is not timely, and to what extent is the trustworthiness adversely affected?

Here we use a common and generally accepted equation from the IEC (2016) of the unavailability of a barrier as a function of time: $U(t) = 1 - e^{-\lambda t}$, where λ is the barrier failure frequency and t is any moment in time. In this thesis, U(t) is assumed to be the opposite of trustworthiness, meaning reliability/availability and effectiveness. U(t) is a dimensionless number between 0 and 1, sometimes shown as a percentage between 0 and 100. From this equation it can be deduced that the unavailability is 0 when t equals 0. That is what can be expected, meaning a barrier is 100% trustworthy when the barrier is new. The equation also shows that U(t) increases as time progresses. If a barrier is never maintained, inspected and tested, and the time t runs to infinity, U(t) will go to 1. In other words, the barrier will fail with 100% certainty when it is needed (not reliable/available) and/or the barrier will not (correctly) perform its necessary function (not effective). Therefore, to ensure the trustworthiness of a barrier, a barrier should be checked at regular intervals, that is maintained, inspected and tested. The time interval with which the maintenance, inspection and test are to be performed, can be calculated as indicated in the formula in order to achieve the trustworthiness required according to the design.

The risk reduction RR that can be achieved with the barrier is the reciprocal value of U(t), meaning RR equals $(1 - e^{-\lambda t})^{-1}$. As the risk reduction is mostly given as a 10-, 100- or 1000-fold reduction, this chapter uses the Briggs logarithm, the mathematical function that has the exponent as a result. The risk reduction expressed in logarithm is abbreviated as RRL, where the RRL is equal to $^{10}\log(1 - e^{-\lambda t})^{-1}$.

In this thesis the time interval in between each maintenance, inspection and test is defined as T, meaning the barrier is maintained, inspected and tested at T, 2T, 3T, etc. In this way, the maximum unavailability U(t) of the barrier is in accordance with the design and is equal to $1 - e^{-\lambda T}$. The minimum risk reduction RR of the barrier equals $(1 - e^{-\lambda T})^{-1}$ and the minimum RRL $^{10}\log(1 - e^{-\lambda T})^{-1}$. The barrier can be qualified as trustworthy. If a barrier is checked later than the required period T, the RR will decrease and may not meet the RR required for the barrier. Table 5.2 shows the effect of postponement of maintenance, inspection and testing on the risk reduction RR and the risk reduction expressed in logarithm RRL. Three different values of U(t), meaning 0.1, 0.01 and 0.001, are included in Table 5.2 for various time intervals. An unavailability of 0.1 means that in average, the barrier is not working in 10% of the demands. In addition, an unavailability of 0.01 and 0.001 implies that the barrier is not trustworthy in 1%, respectively 0.1% of the demands. Table 5.2 shows that if, for example, the check is postponed by half a period to 1.5T, U(t) increases by a factor of 1.5 to resp. 0.15, 0.015 and 0.0015 and the RR decreases by 33%.

For this chapter, it is assumed that a barrier may not be trustworthy if the RR has decreased by 50% or more from the required design value. Table 5.2 shows that this is the case if a barrier has not been checked (maintained, inspected and tested) for more than a doubled period of T, that is from 2T upwards.

Table 5.2, the influence of the time interval on U(t), RR and RRL

Time interval T	$U(t) = 1 - e^{-\lambda t}$	$RR = (1 - e^{-\lambda t})^{-1}$	$RRL = {}^{10}\log(1 - e^{-\lambda t})^{-1}$
T	0.1 / 0.01 / 0.001	10 / 100 / 1000	1 / 2 / 3
1.5T	0.15 / 0.015 / 0.0015	6.67 / 66.7 / 667	0.82 / 1.82 / 2.82
2T	0.19 / 0.019 / 0.0019	5.25 / 52.5 / 525	0.72 / 1.72 / 2.72
2.12T	0.20 / 0.020 / 0.0020	5.01 / 50.1 / 501	0.70 / 1.70 / 2.70
3T	0.27 / 0.027 / 0.0027	3.69 / 36.9 / 369	0.57 / 1.57 / 2.57
3.66T	0.32 / 0.032 / 0.0032	3.16 / 31.6 / 316	0.50 / 1.50 / 2.50
6.58T	0.50 / 0.050 / 0.0050	2.00 / 20.0 / 200	0.30 / 1.30 / 2.30
No check	1	1	0

Summarising, using Table 5.2 implies that:

- Unavailability is expressed as $U(t) = 1 - e^{-\lambda t}$;
- The failure rate λ is assumed constant, meaning at the low horizontal part of the bathtub;
- The equation of U(t) should be interpreted in such a way that trustworthiness is reduced when time progresses. However, it may well be that the barrier or barrier system keeps its designed risk reduction. The equation only shows that the *chance* of unavailability becomes bigger;
- Trustworthiness and risk reduction are the opposite of unavailability;
- The required risk reduction can only be achieved when the barrier is maintained, inspected and tested at regular intervals T;
- The use of Briggs logarithm simplifies the calculation of multiple barriers;
- A barrier that has not been maintained, inspected and tested for more than 2T, may not be trustworthy as its RR has decreased by 50% or more from the required design value.

The status of the barrier system can be used to determine the likelihood of the central event against which the barriers should prevent. The status of the barrier system is therefore suitable to derive an indicator. The indicator, referred to as "preventive barrier indicator", shows the likelihood of the central event. It has been developed based on the RRL of the barrier system as a ratio to the designed or required value. The preventive barrier indicator is the quotient of the current RRL and the required RRL. This is also called relative risk reduction expressed in a logarithm: RRRL. $RRRL(t) = [RRL(t) / RRL_{required}] \times 100\%$.

Table 5.3 shows the outcome of the preventive barrier indicator representing the likelihood of the central event in four colours: green (very unlikely), yellow (not unlikely), orange (likely) and red (very likely). As the colour shifts from green to red, the likelihood of the central event increases. The boundaries are evenly distributed in this chapter and are set at 0%, 25%, 50%, 75% and 100%. For each of these classifications, management must determine how to respond and by whom. This is beyond the scope of this thesis.

Table 5.3, the colour of the preventive barrier indicator related to the RRRL

	100%	75%	50%	25%	0%
RRRL		RRRL>75%	50%< RRRL ≤75%	25%<RRRL≤50%	RRRL≤25%
Prev. barrier indicator		green	yellow	orange	red

The preventive barrier indicator, RRRL, can be determined not only from the trustworthiness of the barrier system, but also from its activation. If the barrier system has been activated, it is possible to determine how many barriers still protect against the central event. The calculation of the RRRL can be applied in the same way here: RRRL(t) = [RRL(t) / $RRL_{required}$] x 100%, where RRL(t) is the risk reduction expressed in Briggs logarithm of the (remaining) barrier system to the central event. The RRRL shows the current risk reduction compared to what it should be according to design and has thus become a (relative) measure for the loss of quality of the barrier system. The preventive barrier indicator shows:

- The quality or trustworthiness of the (preventive) barrier system taken from its quality parameters, and;
- The development of the (left-hand side of the) accident scenario through the activated barrier(s).

Three scenarios have been worked out below with a barrier system of a total RRL of resp. 1, 2 and 3. The barrier system is always located on the left-hand side of the bowtie and consists of preventive barriers. In the first example as shown in Figure 5.2, a scenario is protected by a barrier system with an RRL of 1.

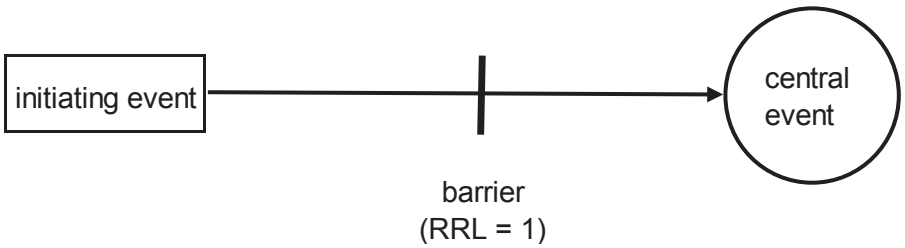

Fig. 5.2, a scenario protected by one barrier with an RRL of 1

Table 5.4 shows the preventive barrier indicator related to the barrier status. With a possibly not trustworthy barrier, the RR has decreased from 10 to 5. The RRL is 0.70, resulting in an RRRL of 70%, as a result of which the preventive barrier indicator turns yellow. If the barrier is not trustworthy, the preventive barrier indicator turns red because the RRRL has reduced to 0%. If the barrier is trustworthy and activated and the scenario does not develop any further, the RRL equals 1 and the RRRL equals 100%. After all, the barrier worked on demand and has proven to be effective. The preventive barrier indicator turns green. Since the scenario has been initiated, it seems evident that targeted action should be taken. This is visualised by placing two exclamation marks in the green field to indicate that the scenario is developing, and that attention is required.

Table 5.4, preventive barrier indicator of a barrier system consisting of one barrier with an RRL of 1

Barrier	RRL	RRRL	Prev. barrier indicator
V	1	100%	Green
?	0.70	70%	Yellow
Θ	0	0%	Red
!	1	100%	!Green!

In Figure 5.3, a scenario is protected by a barrier system comprising two independent barriers with an RRL of 1 each. The RRL of the barrier system is the sum of each of the RRLs (RRL = RRL1 + RRL2 = 1 + 1 = 2). Table 5.5 shows what the preventive barrier indicator is in relation to the status of the barriers. If one of the barriers is possibly not trustworthy, the RRL has been reduced from 2 to 1.70 (RRL = 0.70 + 1). The RRRL is equal to 85% ((1.70 / 2) x 100%). In this case, the preventive barrier indicator is green. If both barriers are possibly not trustworthy, the RRL has been reduced to 1.40 (RRL = 0.70 + 0.70) and the preventive barrier indicator turns yellow (RRRL = (1.40 / 2) x 100% = 70%). If one of the barriers is not trustworthy, the RRL is reduced from 2 to 1 (RRL = 0 + 1) and the RRRL is 50% ((1/2) x 100%). The preventive barrier indicator turns orange. If both barriers are not trustworthy, the preventive barrier indicator turns red.

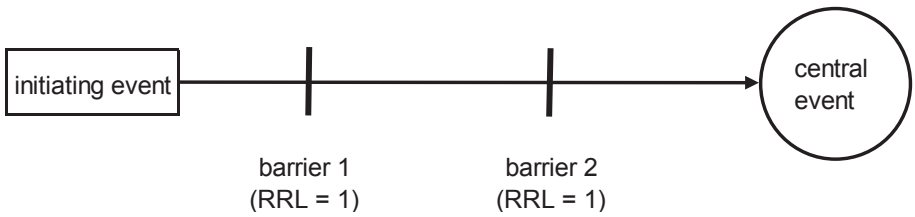

Fig. 5.3, a scenario protected by two independent barriers with an RRL of 1 each

Table 5.5, preventive barrier indicator of a barrier system consisting of two barriers with an RRL of 1 each

Barrier 1	Barrier 2	RRL	RRRL	Prev. barrier indicator
V	V	2	100%	Green
V	?	1.70	85%	Green
V	Θ	1	50%	Orange
?	V	1.70	85%	Green
?	?	1.40	70%	Yellow
?	Θ	0.70	35%	Orange
Θ	V	1	50%	Orange
Θ	?	0.70	35%	Orange
Θ	Θ	0	0%	Red
Θ	!	1	50%	!Orange!
!	V	2	100%	!Green!
!	?	1.70	85%	!Green!
!	Θ	1	50%	!Orange!

Table 5.5 also shows how the preventive barrier indicator colours when one of the barriers is being activated. When activating barrier 1, the RRL is at least 1 (RRL = 1 + RRL2). The preventive barrier indicator changes depending on the status of the second barrier. When activating barrier 2, the RRL of the barrier system is equal to 1. Barrier 2 can only be activated if the first barrier is not trustworthy as the scenario developed up to the second barrier. The RRRL has been reduced to 50% ((1/2) x 100%) and the preventive barrier indicator turns orange.

The third example is elaborated in Figure 5.4 and shows a scenario with a barrier system consisting of two barriers: one with an RRL of 1 and one with an RRL of 2. This example represents for instance a high-pressure scenario, which is equipped with a SIL 1 qualified, instrumental safeguard and a (mechanical) safety valve.

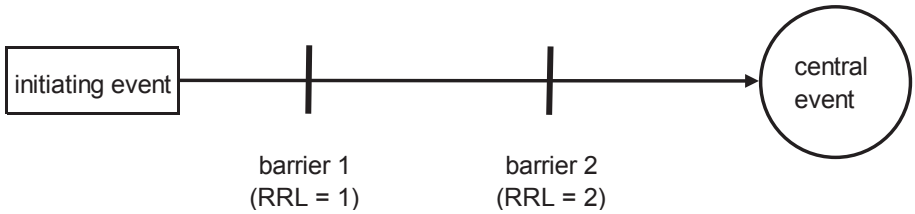

Fig. 5.4, a scenario protected by two independent barriers with an RRL of 1 resp. 2

Table 5.6 shows the RRL, the RRRL and the preventive barrier indicator related to the status of the two barriers. The same reasoning can be followed as in the second example with the two identical barriers. However, the two barriers differ in designed RRLs, which results in different RRRLs and preventive barrier indicator colours.

Table 5.6, preventive barrier indicator of a barrier system consisting of two barriers with an RRL of 1 resp. 2

Barrier 1	Barrier 2	RRL	RRRL	Prev. barrier indicator
V	V	3	100%	Green
V	?	2.70	90%	Green
V	Θ	1	33%	Orange
?	V	2.70	90%	Green
?	?	2.40	80%	Green
?	Θ	0.70	23%	Red
Θ	V	2	67%	Yellow
Θ	?	1.70	57%	Yellow
Θ	Θ	0	0%	Red
Θ	!	2	67%	!Yellow!
!	V	3	100%	!Green!
!	?	2.70	90%	!Green!
!	Θ	1	33%	!Orange!

5.2.3 Special cases

5.2.3.1 M-out of-n barrier systems

M-out of-n barrier systems are widely used in the process industry. Due to the multiple implementation, they have a high trustworthiness and are ideally suited for use in case of high-risk scenarios. An m-out of-n barrier system consists of n serial, identical barriers where the sensors share the same set value and where the same final elements are controlled. An m-out of-n barrier system is activated when at least m barriers are activated. The most common designs are the 1-out of-2, 1-out of-3, 2-out of-3, and 2-out of-4 system.

M-out-of-n barrier systems require special attention since their status may be difficult to determine. When m equals 1, the m-out of-n or 1-out of-n system can be drawn in the bowtie as n serial barriers from which the status can be readily established. As these barriers have the same setting, there are only limited combinations when they are activated, meaning that a barrier is either trustworthy and activated or not trustworthy. But when m doesn't equal 1, it gets more complicated to establish the barrier system's status. To overcome this, some basic rules have been drawn up below based on the status of their single barriers:

- An m-out of-n barrier system is activated if at least m barriers are activated, because that is the prerequisite for activating the m-out of-n barrier system;
- An m-out of-n barrier system which is not trustworthy has at least as many "not trustworthy" barriers that the system cannot be activated. An m-out-n barrier system is not trustworthy if at least (n-m + 1) barriers are "not trustworthy". One "not trustworthy" barrier can be substituted by two "possibly not trustworthy" barriers;
- If there is a demand on an m-out of-n barrier system which is possibly not trustworthy, at least one of the barriers needed to activate the barrier system, should have the status of "possibly not trustworthy", meaning that at least one of the barriers has not been timely maintained, tested or inspected. An m-out of-n

barrier system is "possibly not trustworthy" if at least (n-m + 1) barriers are "possibly not trustworthy". Each pair of "possibly not trustworthy" barriers can be substituted by one barrier which is "not trustworthy".

Table 5.7 shows when a 2-out of-3 and a 2-out of-4 system are possibly not trustworthy, not trustworthy or trustworthy and activated based on the status of the individual barriers.

Table 5.7, worked examples of a 2-out of-3 and 2-out of-4 barrier system

Status van an m-out of-n system	2-out of-3 system	2-out of-4 system
Trustworthy and not activated	All combinations which are not mentioned below	All combinations which are not mentioned below
Possibly not trustworthy	At least two barriers are possibly not trustworthy, or One barrier is not trustworthy	At least three barriers are possibly not trustworthy, or At least one barrier is possibly not trustworthy, and one barrier is not trustworthy, or Two barriers are not trustworthy
Not trustworthy	At least two barriers are not trustworthy, or One barrier is not trustworthy, and two barriers are possibly not trustworthy	At least three barriers are not trustworthy, or Two barriers are not trustworthy, and two barriers are possibly not trustworthy
Trustworthy and activated	At least two barriers have been activated	At least two barriers have been activated

5.2.3.2 Dormant controls

A dormant control, also called passive control, is a device that only starts to control from a certain process value onwards. A dormant control is regarded as an instrumental safeguard, like a pressure blow-off control that opens when the pressure of the process increases and exceeds a safe value. The control valve will be opened to a position to regain the desired process value. A dormant control is aimed at stopping the development of the scenario and can be considered a barrier. In Table 5.8, a symbol is linked to the status of a dormant control in a similar way as is done in Table 5.1.

Table 5.8, dormant control indicator

Dormant control status		Symbol
Trustworthy and not activated		V
Possibly not trustworthy	Not maintained, inspected or tested on time	?
Not trustworthy	On manual mode or defective	Θ
Trustworthy and activated		!

5.2.3.3 Over-safeguarded scenarios

In occasional cases scenarios may be "over-safeguarded", meaning they are provided with a better barrier system than required by a risk assessment. If all barriers are included, the installed RR will be larger than the required RR. Depending on the status of the barrier system, the RRRL may be larger than 100%. Table 5.3, which shows the colour of the preventive barrier indicator in relation to the RRRL, remains valid in such a case.

5.2.3.4 SIL a qualified SIFs

In the process industry instrumental safeguards are used which do not have a SIL qualification as described in IEC 61511 (IEC, 2016). Four SIL levels are specified in this European standard, with SIL 4 as the highest and SIL 1 as the lowest level. However, "SIL a" qualified SIFs (Safety Instrumented Function) are often also part of a barrier system, but do not meet a SIL level as defined by IEC 61511. According to this standard, SIL a qualified SIFs are not subject to any special safety requirements. In this chapter it is assumed that a SIF with a SIL a qualification has an RRL of (minimum) 0.5. This means, for example, that two independent serial SIL a SIFs have a total RRL of 1 and can be equated to one SIL 1 SIF. A SIL a SIF which is possibly not trustworthy has an RRL equal to 0.2.

5.3 CASE STUDY

5.3.1 The ammonia process

The ammonia process uses natural gas as a raw material to which steam and air are supplied. The process consists of two main parts: the cracking process and the synthesis. In the cracking process, the incoming natural gas is stripped of sulphur and then largely converted to CO, CO_2 and hydrogen (H_2) using steam, a catalyst and a temperature of 825 °C and a pressure of 35 bar. The H_2 formed is ultimately necessary to make ammonia. Air is added to the post reformer, supplying nitrogen (N_2) into the process, which is necessary to make ammonia in the synthesis part. The oxygen from the air reacts with an amount of H_2 which increases the temperature even more. Due to the elevated temperature of approximately 1000 °C, the methane still present in the gas is cracked. To remove the CO_2 generated in the cracking process, the process gas is passed through a (physical) CO_2 scrubber. The last residues of CO and CO_2 are converted into methane (CH_4) using a catalyst and H_2.

In the synthesis process, the process gas mainly consists of the H_2 and N_2, in the ratio of 3:1. The reaction to ammonia takes place in the presence of a catalyst at approx. 200 bar and 515 °C (Haber-Bosch process). In the last part of the process the ammonia formed is cooled, separated from the unreacted and inert gases and reduced in pressure, followed by refrigeration to liquify the ammonia.

5.3.2 Failure of the water jacket of the post reformer (R1)

Post reformer R1 is part of the cracking process and is located downstream the reformer where most of the natural gas is cracked. In the post reformer the uncracked natural gas from the reformer is cracked under very high temperatures, up to 1000 °C. This temperature is reached by supplying air, which burns some of the hydrogen from the process gas. The air is supplied by the process air compressor with a pressure of approx. 38 bar, slightly higher than the pressure in the post reformer.

The post reformer is equipped with a water jacket that protects the inner wall against too high temperature. The water jacket has some open connections on top, meaning that the water is at boiling temperature. As the water jacket is slowly losing its contents, water has to be supplied continuously. If there's not enough water in the jacket, the wall's temperature becomes too high, and the wall will weaken and collapse under the prevailing process pressure of approx. 37 bar. This will result in an escape of process gas, followed by a jet fire or explosion. The water in the water jacket comes from the feed water pumps P1A and P1B, one of which always runs, and one is on stand-by mode. As a pump failure is seen as the most likely cause for failure of the water supply, this case will focus on the pumps' failure only. If the running pump fails, the other pump will start automatically. If both pumps fail, a motor alarm (MA P1) is activated, after which the operator can try and start one of the feed water pumps, start one of the condensate pumps or draw in canal water to feed the water jacket.

A low water supply to the water jacket is also detected by a low flow alarm (FAL1) that gives the operator enough time to act and to ensure sufficient water supply to the water jacket. This action is identical to that of the alarm MA P1: manual start of the feed water or condensate pumps or the intake of canal water. If the level of the water jacket becomes too low, two (low-level) alarms (LAL) installed on the water jacket will be activated. Although these two identical alarms can be considered as a 1-out of-2 system, they count in the calculation as if they were two separate alarms. In case the low-level alarms have been activated, the operator has some but limited time to identify and recover from the cause. Ultimately it can be decided to shut down the plant. All the operator actions are relatively simple and can be conducted out without much time pressure.

All four alarms have an RRL of 0.5. According to specification, the scenario is protected by a barrier system with a total RRL of 2. Figure 5.5 shows the post reformer with its alarms. Figure 5.6 shows the barriers in a bowtie designed to prevent the post reformer from having a too high wall temperature.

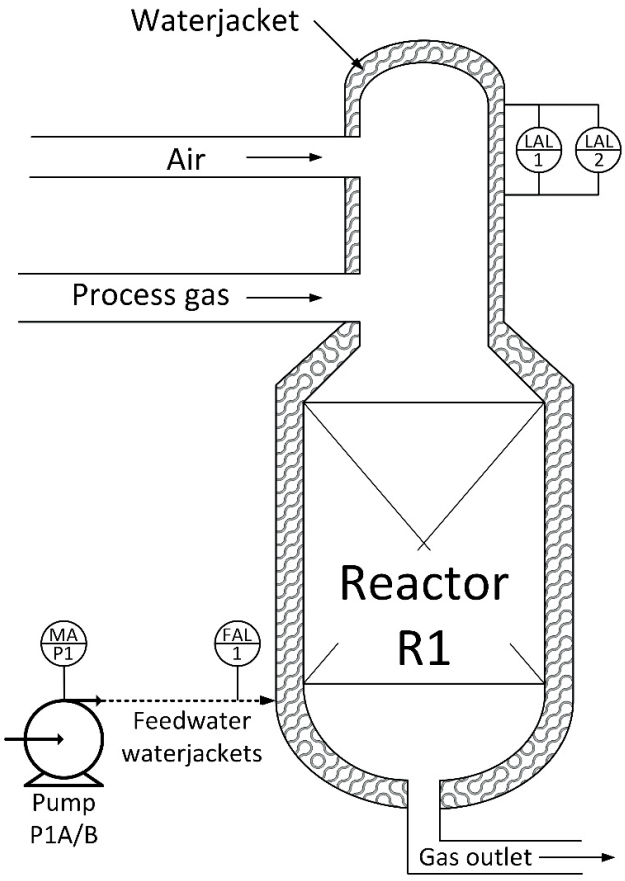

Fig. 5.5, post reformer R1 and its alarms

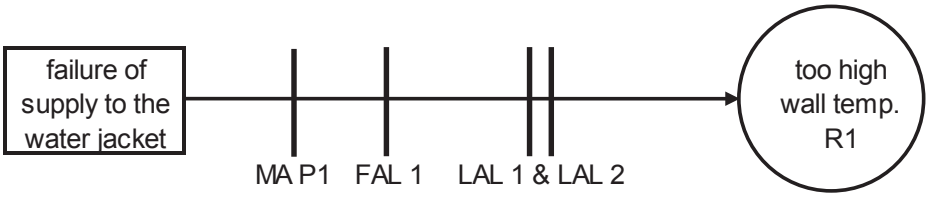

Fig. 5.6, scenario 'too high wall temperature R1' by failure of the water jacket cooling

Table 5.9 shows the preventive barrier indicator of the scenario "too high wall temperature R1" depending on the status of the (preventive) barrier system consisting of four alarms.

Table 5.9, preventive barrier indicator of the scenario 'too high wall temperature R1'

MA P1	FAL 1	LAL 1	LAL 2	RRL	RRRL	Prev. barrier indicator
V	V	V	V	2	100%	Green
V	V	V	?	1,7	85%	Green
V	V	V	Θ	1,5	75%	Yellow
V	V	?	V	1,7	85%	Green
V	V	?	?	1,4	70%	Yellow
V	V	?	Θ	1,2	60%	Yellow
V	V	Θ	V	1,5	75%	Yellow
V	V	Θ	?	1,2	60%	Yellow
V	V	Θ	Θ	1	50%	Orange
V	?	V	V	1,7	85%	Green
V	?	V	?	1,4	70%	Yellow
V	?	V	Θ	1,2	60%	Yellow
V	?	?	V	1,4	70%	Yellow
V	?	?	?	1,1	55%	Yellow
V	?	?	Θ	0,9	45%	Orange
V	?	Θ	V	1,2	60%	Yellow
V	?	Θ	?	0,9	45%	Orange
V	?	Θ	Θ	0,7	35%	Orange
V	Θ	V	V	1,5	75%	Yellow
V	Θ	V	?	1,2	60%	Yellow
V	Θ	V	Θ	1	50%	Orange
V	Θ	?	V	1,2	60%	Yellow
V	Θ	?	?	0,9	45%	Orange
V	Θ	?	Θ	0,7	35%	Orange
V	Θ	Θ	V	1	50%	Orange
V	Θ	Θ	?	0,7	35%	Orange
V	Θ	Θ	Θ	0,5	25%	Red
?	V	V	V	1,7	85%	Green
?	V	V	?	1,4	70%	Yellow
?	V	V	Θ	1,2	60%	Yellow
?	V	?	V	1,4	70%	Yellow
?	V	?	?	1,1	55%	Yellow
?	V	?	Θ	0,9	45%	Orange
?	V	Θ	V	1,2	60%	Yellow
?	V	Θ	?	0,9	45%	Orange
?	V	Θ	Θ	0,7	35%	Orange
?	?	V	V	1,4	70%	Yellow
?	?	V	?	1,1	55%	Yellow
?	?	V	Θ	0,9	45%	Orange
?	?	?	V	1,1	55%	Yellow
?	?	?	?	0,8	40%	Orange
?	?	?	Θ	0,6	30%	Orange
?	?	Θ	V	0,9	45%	Orange
?	?	Θ	?	0,6	30%	Orange
?	?	Θ	Θ	0,4	20%	Red
?	Θ	V	V	1,2	60%	Yellow
?	Θ	V	?	0,9	45%	Orange
?	Θ	V	Θ	0,7	35%	Orange
?	Θ	?	V	0,9	45%	Orange
?	Θ	?	?	0,6	30%	Orange
?	Θ	?	Θ	0,4	20%	Red
?	Θ	Θ	V	0,7	35%	Orange

Table 5.9, continued.

MA P1	FAL 1	LAL 1	LAL 2	RRL	RRRL	Prev. barrier indicator
?	Θ	Θ	?	0,4	20%	Red
?	Θ	Θ	Θ	0,2	10%	Red
Θ	V	V	V	1,5	75%	Yellow
Θ	V	V	?	1,2	60%	Yellow
Θ	V	V	Θ	1	50%	Orange
Θ	V	?	V	1,2	60%	Yellow
Θ	V	?	?	0,9	45%	Orange
Θ	V	?	Θ	0,7	35%	Orange
Θ	V	Θ	V	1	50%	Orange
Θ	V	Θ	?	0,7	35%	Orange
Θ	V	Θ	Θ	0,5	25%	Red
Θ	?	V	V	1,2	60%	Yellow
Θ	?	V	?	0,9	45%	Orange
Θ	?	V	Θ	0,7	35%	Orange
Θ	?	?	V	0,9	45%	Orange
Θ	?	?	?	0,6	30%	Orange
Θ	?	?	Θ	0,4	20%	Red
Θ	?	Θ	V	0,7	35%	Orange
Θ	?	Θ	?	0,4	20%	Red
Θ	?	Θ	Θ	0,2	10%	Red
Θ	Θ	V	V	1	50%	Orange
Θ	Θ	V	?	0,7	35%	Orange
Θ	Θ	V	Θ	0,5	25%	Red
Θ	Θ	?	V	0,7	35%	Orange
Θ	Θ	?	?	0,4	20%	Red
Θ	Θ	?	Θ	0,2	10%	Red
Θ	Θ	Θ	V	0,5	25%	Red
Θ	Θ	Θ	?	0,2	10%	Red
Θ	Θ	Θ	Θ	0	0%	Red
!	V	V	V	2	100%	!Green!
!	V	V	?	1,7	85%	!Green!
!	V	V	Θ	1,5	75%	!Yellow!
!	V	?	V	1,7	85%	!Green!
!	V	?	?	1,4	70%	!Yellow!
!	V	?	Θ	1,2	60%	!Yellow!
!	V	Θ	V	1,5	75%	!Yellow!
!	V	Θ	?	1,2	60%	!Yellow!
!	V	Θ	Θ	1	50%	!Orange!
!	?	V	V	1,7	85%	!Green!
!	?	V	?	1,4	70%	!Yellow!
!	?	V	Θ	1,2	60%	!Yellow!
!	?	?	V	1,4	70%	!Yellow!
!	?	?	?	1,1	55%	!Yellow!
!	?	?	Θ	0,9	45%	!Orange!
!	?	Θ	V	1,2	60%	!Yellow!
!	?	Θ	?	0,9	45%	!Orange!
!	?	Θ	Θ	0,7	35%	!Orange!
!	Θ	V	V	1,5	75%	!Yellow!
!	Θ	V	?	1,2	60%	!Yellow!
!	Θ	V	Θ	1	50%	!Orange!
!	Θ	?	V	1,2	60%	!Yellow!
!	Θ	?	?	0,9	45%	!Orange!
!	Θ	?	Θ	0,7	35%	!Orange!
!	Θ	Θ	V	1	50%	!Orange!
!	Θ	Θ	?	0,7	35%	!Orange!
!	Θ	Θ	Θ	0,5	25%	!Red!
Θ	!	V	V	1,5	75%	!Yellow!
Θ	!	V	?	1,2	60%	!Yellow!

Table 5.9, continued.

MA P1	FAL 1	LAL 1	LAL 2	RRL	RRRL	Prev. barrier indicator
Θ	!	V	Θ	1	50%	!Orange!
Θ	!	?	V	1,2	60%	!Yellow!
Θ	!	?	?	0,9	45%	!Orange!
Θ	!	?	Θ	0,7	35%	!Orange!
Θ	!	Θ	V	1	50%	!Orange!
Θ	!	Θ	?	0,7	35%	!Orange!
Θ	!	Θ	Θ	0,5	25%	!Red!
Θ	Θ	!	Θ	0,5	25%	!Red!
Θ	Θ	!	!	1	50%	!Orange!
Θ	Θ	Θ	!	0,5	25%	!Red!

The screenshots below show a detailed process safety dashboard. Figure 5.7 shows the ammonia production unit with the two ammonia production installations and their related units. In ammonia plant 3 one of the indicators is coloured yellow. This can be investigated by zooming in to the reformer and CO shift unit, see Figure 5.8. Figure 5.8 shows that the post reformer (R3102, called R1 in the example) is coloured yellow. For further analysis, Figure 5.9 shows that two of the post reformer scenarios are coloured yellow and that two barriers have an abnormal status: FIAL1110 (in the example FAL1) is possibly not trustworthy and LAL1107 (in the example LAL1) is not trustworthy. Apparently, the inactivation of one of the low level alarms (LAL1107) also influences another scenario indicator (erosion of refractory).

Installing such a process safety dashboard can provide the control room with real-time information about the status of the barrier system, but it also enables management to view the *status quo* of their production unit at a high level.

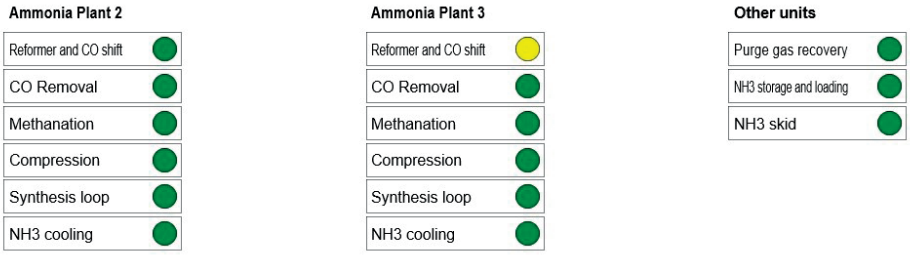

Fig. 5.7, screenshot of the process safety dashboard of the ammonia production unit

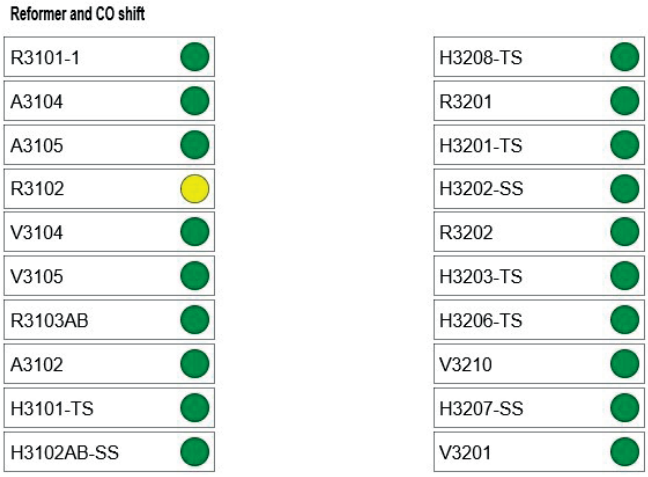

Fig. 5.8, screenshot of the process safety dashboard of the 'reformer and CO shift' section of ammonia plant #3

Fig. 5.9, screenshot of the process safety dashboard of the post reformer

5.4 DISCUSSION

This chapter shows that it is possible to give a qualitative estimate of the likelihood of the central event based on the preventive barrier status. However, the presented model has a few limitations:

- Barriers usually consist of 3 elements: a sensor, a decision maker, and a final element. All three must be monitored to determine the status of the (preventive) barrier. In particular, the final element does not always have self-diagnosis, so it

cannot be foreseen whether this barrier element is overridden or defective.

- If a barrier consists of an alarm, a (safety-critical) instruction and an operator intervention, a similar problem occurs. The trustworthiness of the operator is difficult to measure. Has the operator seen the alarm and understood the problem? Does he/she know how to act? Is he/she not too busy with other tasks?
- The failure rate regarding operator intervention is usually much higher than the failure rate of technical barrier elements. Hence, the reduction of equation $U(t) = 1 - e^{-\lambda t}$ to a widely used, simplified sawtooth of λt can not be applied as λt is not smaller than 0.01. In other words, care should be taken using Table 5.2 when applying it to human intervention.

Mechanical safeguards such as safety valves or check valves are rarely maintained, inspected and tested, for example once every 4, 6 or even 12 years. These barriers also do not provide feedback if they are defective. This means that the barrier status of mechanical safeguards will not change for a long time. Despite this limitation, it makes sense to include mechanical safeguards in the assessment of the preventive barrier indicator of the scenarios in which they apply. If there is a suspicion of malfunction during operation, which cannot be immediately verified or resolved, and for which corrective maintenance is planned, the barrier status could be set manually to possibly not trustworthy or not trustworthy.

Proper and timely maintenance, inspection and testing may not always guarantee the trustworthiness of barriers. Clearly, maintenance should be performed according to the manufacturer's guidelines and by competent personnel, but that does not mean a 100% safe barrier system. It is recommended to set up a registration system for safety critical equipment that records the findings of its maintenance, inspection and testing. The records should then be regularly checked so to establish whether the maintenance, inspection and testing regime should be adjusted. So will a higher frequency contribute to better trustworthiness. IEC 61511 (IEC, 2016) provides guidance on calculating the trustworthiness based on its frequency.

Another aspect is that an inspection and/or test must show whether the barrier is not only reliable/available but also effective, meaning capable of achieving the designed target within a specified time. After all, a barrier can be subject to wear or degradation and this should be reflected in the test procedure. Do valves close completely? Does the instrumental safeguard activate at the right process value? Is the fire-resistant coating not too much degraded? And is the anti-slip floor not worn too far? In other words, is the barrier still sound? When a barrier is returned to service after maintenance, inspection and testing it requires special attention. In case there are doubts about its trustworthiness, the barrier status should be classified as 'possibly not trustworthy'.

Four SIL levels are specified in IEC 61511, with SIL 4 being the highest and SIL 1 being the lowest. In addition, the standard specifies that the RR of a SIL 1 barrier is between 10 and 100, excluding 10 and including 100 (and for a SIL 2 barrier between 100 and 1000, excluding 100 and including 1000, etc.). In this chapter it is assumed that the RR of a SIL 1 barrier is also between 10 and 100 but including 10 and excluding 100. In the calculations an RR of 10 is applied for a SIL 1 barrier, an RR of 100 for SIL 2 and for SIL 3 an RR of 1000. This conservative approach is in line with CCPS (2015), which for a SIL 1, SIL 2 and SIL 3 barrier proposes an RR of respectively 10, 100 and 1000.

The calculation of the preventive barrier indicator does not consider simultaneous testing, the mean time to repair (MTTR) and the mean repair time (MRT), common cause errors and other factors that allow the different (serial) SIFs in a barrier system to interact. As a result, the final RR may be slightly lower than calculated. However, this chapter provides an indication of the likelihood of the scenario which should be seen as a relative change rather than an absolute value.

In m-out of-n systems, the numerical value of m and n is based on the number of sensors and not on the number of decision makers and final elements. The number of sensors may differ from the number of decision-makers and final elements. To determine the status of the barrier system, all barrier elements must be considered.

When applying the IEC 61511 risk graph or a risk matrix from LOPA (layer of protection analysis), the mitigation or risk reduction is given as a 10-, 100- or 1000-fold reduction. The development of a preventive barrier indicator based on the Briggs logarithm with base 10 is a logical consequence. In this way the RRLs of the various barriers can easily be summed. If Table 5.3 was not drawn up from the RRL but from the RR, not only would the distribution be disproportionately more spread, but the preventive barrier indicator could not become 0%. The RRR (Relative Risk Reduction) of an inactive barrier system will be a low number close to 0% but never 0% (RRR(t) = $[RR(t)/RR_{required}]$ x 100% = $[1/RR_{required}]$ x 100%). On the other hand, using the Briggs logarithm the RRRL will always be 0% when all barriers are inactive, no matter the size of the barrier system.
Several choices have been made in this chapter that influence the sensitivity of the preventive barrier indicator. First, a barrier is possibly not trustworthy at halving the RR. Table 5.2 shows, however, that another change in the RR can be opted to label a barrier as possibly not trustworthy. Second, the limits of the preventive barrier indicator in Table 5.3 are also freely selectable and offer the option of having the preventive barrier indicator coloured earlier or later. Both choices are up to each company to determine and are partly dictated by their policy. The choices made in this chapter are based on scenarios of the ammonia plants where the author works.

Finally, it should be emphasised that a scenario only develops when it has started. The chance of a central event does not only depend on the barrier status, but also on the chance that the 'initiating event' occurs. This chapter focusses on the barrier system but could be extended with indicators on the initiating events, such as (active) controls. This would provide a solution for barrier systems that consist of few barriers only.

5.5 CONCLUSIONS

The main question of this chapter is whether – based on the status of the barrier system – indicators can be derived that provide information about the development and likelihood of the major accident processes in the ammonia production process. To answer this question, various sub-questions have been investigated. A barrier system is defined as a set of existing barriers that must prevent causes from developing into consequences. The barrier system's status can be derived from the parameters reliability/availability and effectiveness. Both parameters are sensitive to change, which is considered an important indicator criterion. An indicator – called preventive barrier indicator – has been developed from these parameters. From the example the preventive barrier indicator has proven to monitor the level of safety, and enable the operators to decide where and which action is necessary. The preventive barrier indicator shows the development and likelihood of the scenario, which is not an absolute value, but rather an indication of the change in the *status quo* that should initiate further action.

Many incidents did not happen because a process value was extremely out of range, but rather because of a rare combination of deviating values (Ale, 2009). That is perhaps one of the reasons that the number of major process safety incidents in the process industry is low. It is better to look at the more frequent "precursor" incidents to measure safety (Hopkins, 2009). The concept elaborated in this chapter seems to comply with this: every technical change of the barrier system is used to determine the development and likelihood of the scenario. If the quality parameters of the barriers are incorporated in an automated system, the preventive barrier indicator can be calculated and displayed in real time. This is different for technical changes which are not automatically notified as they will have to be entered manually. A future validation, performed through retrospective research based on several (near) incidents, will have to show to what extent the preventive barrier indicator provides timely insight into the likelihood and development of the accident scenarios.

This sub-study focusses on the barrier system, but indicators can be developed at multiple levels. For example, Sonnemans et al. (2010) look at the smaller signals, meaning common precursors and latent conditions. The latent conditions allow

the presence of precursors to persist and undermine the effectiveness of the barrier system. Hassan and Khan (2012) provide different levels from which indicators can be derived, and Bellamy et al. (2007) distinguish between primary barriers and supporting barriers. At various levels, indicators can provide information about accident scenarios. Scenarios are influenced via barriers and management factors (the management delivery system) as the most important vectors. Further research is needed to design indicators at other levels that can provide information on major accident processes, starting with the management delivery system as the first higher aggregation level.

5.6 REFERENCES

Ale, B. (2009). More thinking about process safety indicators. *Safety Science, 47*, 470–471, http://dx.doi.10.1016/j.ssci.2008.07.012.

ANSI/API. (2010). *Process Safety Performance Indicators for the Refining and Petrochemical Industries*. ANSI/API RP 754, first edition. Retrieved from https://www.apiwebstore.org/publications/item.cgi?4d333980-c4b6-40ff-a33b-1e66389c2d02.

Badreddine, A., Romdhane, T.B., HajKacem, M.A.B., & Amor, N.B. (2014). A new multi-objectives approach to implement preventive and protective barriers in bow tie diagram. *Journal of Loss Prevention in the Process Industries, 32*, 238–253, http://dx.doi.org/10.1016/j.jlp.2014.09.012.

Bellamy, L.J., Ale, B.J.M., Geyer, T.A.W., Goossens, L.H.J., Hale, A.R., Oh, J., Mud, M., Bloemhof, A., Papazoglou, I.A., & Whiston, J.Y. (2007). Storybuilder – A tool for the analysis of accident reports. *Reliability Engineering and System Safety, 92*, 735–744, http://dx.doi.org/10.1016/j.ress.2006.02.010.

CCPS. (2011). *Process Safety Leading and Lagging Metrics*. Retrieved from https://www.aiche.org/sites/default/files/docs/pages/CCPS_ProcessSafety_Lagging_2011_2-24.pdf.

CCPS. (2015). *Guidelines for initiating events and independent protection layers in layer of protection analysis*. New York, U.S.: Wiley.

Crisislab. (2016). *Toeval of structureel incidentalisme? Negen incidenten uit 2015 bij Chemelot nader beschouwd*. Retrieved from http://crisislab.nl/wordpress/wp-content/uploads/2016-06-07-rapport-Chemelot-def.pdf.

Dokas, M., Feehan, J., & Syed, I. (2013). EWaSAP: An early warning sign identification approach based on a systemic hazard analysis. *Safety Science, 58*, 11–26, http://dx.doi.org/10.1016/j.ssci.2013.03.013.

European Chemical Industry Council (Cefic). (2011). *Guidance on Process Safety Performance Indicators*. Brussel, België: Cefic.

European Chemical Industry Council (Cefic). (2016). *Cefic guidance for reporting on the ICCA globally harmonised process safety metric*. Retrieved from https://cefic.org/app/uploads/2019/02/Cefic-ICCA-Guidance-on-Process-Safety-Performance-Indicators.pdf.

Guldenmund, F., Hale, A., Goossens, L., Betten, J., & Duijm, N.J. (2006). The development of an audit technique to assess the quality of safety barrier management. *Journal of Hazardous Materials, 130*, 234–241, http://dx.doi.org/10.1016/j.jhazmat.2005.07.011.

Hale, A. (2009). Why safety performance indicators?. *Safety Science, 47*, 479–480, http://dx.doi.org/10.1016/j.ssci.2008.07.018.

Hassan, J., & Khan, F. (2012). Risk-based asset integrity indicators. *Journal of Loss Prevention in the Process Industries, 25*, 544–554, http://dx.doi.org/10.1016/j.jlp.2011.12.011.

Hollnagel, E. (2008). Risk + barriers = safety?. *Safety Science, 46*, 221–229, http://dx.doi.org/10.1016/j.ssci.2007.06.028.

Hopkins, A. (2009). Thinking about process safety indicators. *Safety Science, 47*, 460–465, http://dx.doi.org/10.1016/j.ssci.2007.12.006.

Houtermans, M. (2014). *SIL and Functional Safety in a NUTSHELL* (First edition). Zug, Zwitserland: Risknowlogy.

HSE. (2006). *Process safety indicators, a step-by-step guide for the chemical and major hazards industries*, HSG 254. Richmond, Surrey, UK: The Office of Public Sector Information, Information Policy Team. Retrieved from http://www.hse.gov.uk/pUbns/priced/hsg254.pdf.

IEC. (2016). *Functional safety – Safety instrumented systems for the process industry sector*. Genève, Switzerland: IEC.

Knegtering, B., & Pasman, H. (2013). The safety barometer. How safe is my plant today? Is instantaneously measuring safety level utopia or realizable?. *Journal of Loss Prevention in the Process Industries, 26*, 821–829, http://dx.doi.org/10.1016/j.jlp.2013.02.012.

Landucci, G., Argenti, F., Allessandro, T. & Cozzani, V. (2015). Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. *Reliability Engineering and System Safety, 143*, 30–43, http://dx.doi.org/10.1016/j.ress.2015.03.023.

Mannan, S. (2005). *Lees' Loss Prevention in the Process Industries*. Oxford, U.K.: Elsevier Butterworth-Heinemann.

OGP. (2011). *Process safety, recommended practice on key performance indicators*. Report nr 456. Retrieved from http://www.learnfromaccidents.com.gridhosted.co.uk/images/uploads/OGP_456_KPIs_for_Pro-

cess_safety.pdf.
Øien, K., Utne, I., & Herrera, I. (2011a). Building Safety indicators: Part 1 – Theoretical foundation. *Safety Science, 49*, 148–161, http://dx.doi.org/10.1016/j.ssci.2010.05.012.
Øien, K., Utne, I., Tinmannsvik, R., & Massaiu, S. (2011b). Building Safety indicators: Part 2 – Application, practices and results. *Safety Science, 49*, 162–171, http://dx.doi.org/10.1016/j.ssci.2010.05.015.
OVV. (2018). *Chemie in samenwerking – Veiligheid op het industriecomplex Chemelot*. Retrieved from https://www.onderzoeksraad.nl/nl/page/4707/chemie-in-samenwerking---veiligheid-op-het-industriecomplex-chemelot.
Schmitz, P., Swuste, P., Theunissen, J., Reniers, G., Decramer, G., & Uijterlinde, P. (2018). Een aanpak voor het bepalen van een realistische ranking van de gevaarlijkste procesonderdelen van het ammoniakproductieproces. *Tijdschrift voor toegepaste Arbowetenschap, 2018*(2), 42–56.
Schmitz, P., Swuste, P., Reniers, G., & Nunen van, K. (2019a). Mechanical integrity of process installations: an assessment based on bow-ties. *Chemical Engineering transactions, 77*, 97–102, http://dx.doi.org/10.3303/CET1977017.
Schmitz, P., Swuste, P., Reniers, G., & Decramer, G. (2019b). Een aanpak voor het beoordelen van mechanische faalmechanismen van statische apparaten van het ammoniakproductieproces. *Tijdschrift voor toegepaste Arbowetenschap, 2019*(2), 34–54.
Schmitz, P., Swuste, P., Reniers, G., & Nunen van, K. (2020). Mechanical integrity of process installations: Barrier alarm management based on bowties. *Process Safety and Environmental Protection, 138*, 139–147, https://doi.org/10.1016/j.psep.2020.03.009.
Sinelnikov, S., Inouye, J., & Kerper, S. (2015). Using leading indicators to measure occupational health and safety performance. *Safety Science, 72*, 240–248, http://dx.doi.org/10.1016/j.ssci.2014.09.010.
Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries, 19*, 494–506, http://dx.doi.org/10.1016/j.jlp.2005.12.004.
Sonnemans, P.J.M., Körvers, P.M.W., & Pasman, H.J. (2010). Accidents in "normal" operation – Can you see them coming? *Journal of Loss Prevention in the Process Industries, 23*, 351–366, http://dx.doi.org/10.1016/j.jlp.2010.01.001.
Swuste, P., Theunissen, J., Schmitz, P., Reniers, G., & Blokland, P. (2016). Process safety indicators, a review of literature. *Journal of Loss Prevention in the Process Industries, 40*, 162–173, http://dx.doi.org/10.1016/j.jlp.2015.12.020.
Vinnem, J.E., Aven, T., Husebø, T., Seljelid, J., & Tveit, O.J. (2006). Major hazard risk indicators for monitoring of trends in the Norwegian offshore petroleum sector. *Reliability Engineering and System Safety, 91*, 778–791, http://dx.doi.org/10.1016/j.ress.2005.07.004.
Vinnem, J.E. (2010). Risk indicators for major hazards on offshore installations. *Safety Science, 48*, 770–787, http://dx.doi.org/10.1016/j.ssci.2010.02.015.

6

PREDICTING MAJOR HAZARD ACCIDENTS IN THE PROCESS INDUSTRY BASED ON ORGANISATIONAL FACTORS: A PRACTICAL, QUALITATIVE APPROACH[6]

6 The Chapter is based on the paper: Schmitz, P., Reniers, G., Swuste, P. & Nunen van, K. (2021b). Predicting major hazard accidents in the process industry based on organizational factors: a practical, qualitative approach. *Process Safety and Environmental Protection, 148*, 1268–1278. https://doi.org/10.1016/j.psep.2021.02.040, and was formatted and edited for this thesis.

ABSTRACT

This chapter answers the question to what extent major hazard accidents in the ammonia production process can be predicted from organisational factors, also called management delivery systems. Organisational factors are linked to accident processes and their barrier systems, using the bowtie metaphor. It is shown that organisational factors indirectly impact accident processes as they strongly influence the quality or trustworthiness of the barrier systems. By putting the right focus on organisational factors during audits or reviews, major accident processes get the attention they deserve, and the necessary actions are taken at the right management level. Qualitative and quantitative monitoring of organisational factors can provide a picture of their operation and efficiency. Using an example on retrospective data it is demonstrated that information from organisational factors could have stopped the development of the near-accident prematurely. However, organisational factors should first be qualitatively assessed before they are quantitatively monitored. A quantitative assessment has been worked out for one of the management delivery systems so to provide an example of management indicators. Determining these (management) indicators from threshold values is an intricate matter due to the complicated influence of organisational factors on accident processes, and requires more follow-up research.

6.1 INTRODUCTION

In the previous chapter the concept of the preventing barrier indicator has been discussed. This chapter considers the barrier's management and demonstrates that the barrier's quality is strongly determined by the (efficiency of the) organisational factors. Those organisational factors are selected and investigated which are closely related to the barrier systems and the major hazard accident processes. The following research question is answered:

> *Can major hazard accident processes related to the ammonia production process be predicted by monitoring organisational factors?*

The associated sub-questions to be investigated are:

1) What are organisational factors?
2) How are organisational factors linked to the accident processes?
3) What are the organisational factors in the ammonia production process of OCI Nitrogen?
4) What information can organisational factors provide about the accident processes?
5) How can the information from the organisational factors influence the accident processes of OCI Nitrogen?

Accident processes related to occupational safety that originate from working conditions are excluded in this sub-study. This chapter is exclusively concerned with potential accidents related to process safety and, in addition, only those that are major or catastrophic.

This chapter starts with definitions and examples of organisational factors from the literature, followed by their relationship with the safety management system and the process barrier systems to link them to accident processes. A list of organisational factors or management delivery systems applicable for OCI Nitrogen has been compiled which outlines their information about accident processes. An example shows how the information from some organisational factors could have influenced a near-accident. In a high pressure scenario example the management delivery systems are named which are relevant to maintain barrier system's quality.

6.1.1 Organisational factors

The term "organisational factors" has many synonyms. It has been argued since the late 1970s that major hazard accident processes often start less conspicuously (Turner, 1978; Perrow, 1984; Kletz, 1988). The attention to latent factors in an organisation led Turner to introduce his idea of incubation time. Incubation refers to mechanisms in

organisations that deny dangers and risks. In the Swiss cheese metaphor of Reason (1987, 1997), the latent factors ("pathogens") are visualised through the holes in barriers, later elaborated as basic risk factors of the Tripod model (Swuste et al., 2016b, 2020a, 2020b).

The Joint Research Centre of the European Commission started two projects at the beginning of this millennium to develop a structure of risk management for the process industry. ARAMIS (Accident Risk Assessment Methodology for Industries) and I-Risk (the development of an integrated technical and management risk methodology for chemical installations) both examined the position and influence of organisational factors. In the context of ARAMIS they are called delivery systems (Hale et al., 2007) and with reference to I-Risk they are named management delivery systems (Guldenmund et al., 2006). Kongsvik, Almklov and Fenstad (2010) refer to organisational factors as organisational safety conditions, Øien et al. (2011) as functional areas and Hassan and Khan (2012) as activity indicators. But organisational factors are also described as secondary management processes (Papazoglou et al., 2003) or support safety barriers (Bellamy et al., 2007; Ale et al., 2008), emphasizing the indirect impact on accident processes. Delivery systems are principal management systems that influence and ensure the continuous functioning of barriers (Duijm & Markert et al., in Li et al., 2020). In professional literature, organisational factors or delivery systems can often be elements of a (process) safety management system (CCPS 2016; OSHA, s.d.) or parts of a risk management system (HSE, 2006). Finally, organisational factors can be extracted from research methods, such as the basic risk factors of the Tripod model (Wagenaar et al., 1994).

In this chapter, in addition to organisational factors, the term "management delivery systems" is used in the same context. The term "management delivery systems" has been used more often in the context of this research, while "organisational factors" are easier to translate into practical reality.

Table 6.1 provides a (non-exhaustive) overview of various organisational factors or management delivery systems as found in the scientific and professional literature. There are some duplicated terms in the table where the organisational factors or management delivery systems are used in a different context.

Table 6.1, a (non-exhaustive) overview of organisational factors or management delivery systems, taken from referred literature

Organisational factors or management delivery systems	Reference
Competence, suitability	Hale (2005), HSE 254, Kongsvik et al. (2010), Øien (2001b), Hassan and Khan (2012), Bellamy (2015), Duijm (2009), Guldenmund et al. (2006)
Commitment, organisational management	Hale (2005), Duijm (2009), Guldenmund et al. (2006), Wagenaar et al. (1994)
Communication, coordination of teams	Hale (2005), HSE 254, Kongsvik et al. (2010), Hassan and Khan (2012), Bellamy (2015), Duijm (2009), Guldenmund et al. (2006), Wagenaar et al. (1994)
Procedures, rules and goals	Hale (2005), HSE 254, Bellamy (2015), Duijm (2009), Guldenmund et al. (2006)
Technical design and hardware	Hale (2005), HSE 254, Øien (2001b), Bellamy (2015), Wagenaar et al. (1994)
Interface, ergonomics	Hale (2005), Bellamy (2015)
Manpower planning and availability	Hale (2005), Bellamy (2015), Duijm (2009), Guldenmund et al. (2006)
Inspection and maintenance	HSE 254, Øien (2001b), Hassan and Khan (2012)
Instrumentation and alarms	HSE 254
Plant changes	HSE 254, Kongsvik et al. (2010)
Permit to work	HSE 254, Hassan and Khan (2012)
Emergency arrangements	HSE 254
Work practise	Kongsvik et al. (2010)
Instructions and documentation	Kongsvik et al. (2010), Wagenaar et al. (1994)
Workload and physical environment	Kongsvik et al. (2010)
Planning and coordination	Kongsvik et al. (2010)
Individual factors (slips, lapses)	Øien (2001b)
Procedures, job safety analysis, guidelines, instructions	Øien (2001b)
Planning, coordination, organisation, control	Øien (2001b)
Inspection and maintenance management	Hassan and Khan (2012), Wagenaar et al. (1994)
Engineering assessment	Hassan and Khan (2012)
Operating performance	Hassan and Khan (2012)
State of hardware	Hassan and Khan (2012), Wagenaar et al. (1994)
Plant configuration and modification	Hassan and Khan (2012)
Engineering safety system	Hassan and Khan (2012), Wagenaar et al. (1994)
Crisis management	Hassan and Khan (2012)
Safety culture	Hassan and Khan (2012), Duijm (2009)
Motivation	Bellamy (2015)
Conflict resolution	Bellamy (2015), Duijm (2009), Guldenmund et al. (2006)
Hard/software purchase, build, interface, install	Duijm (2009), Guldenmund et al. (2006)
Hard/software inspect, maintain, replace	Duijm (2009), Guldenmund et al. (2006)
Risk identification, barrier selection and specification	Guldenmund et al. (2006)
Monitoring, feedback, learning and change management	Guldenmund et al. (2006)
Error-enforcing conditions	Wagenaar et al. (1994)
Housekeeping	Wagenaar et al. (1994)
Incompatible goals	Wagenaar et al. (1994)
Training	Wagenaar et al. (1994)

6.1.2 Safety management system

The organisational factors or management delivery systems support the overall management of safety barriers (Li et al., 2020). They are an integral part of the safety management system (Hale, 2005). The integrity of the primary barriers (barriers with

a direct influence on the accident process, see Figure 6.2) is maintained by the safety management system (Bellamy et al., 2007). The management delivery systems that support the primary barriers are considered non-technical because their working method is based on work processes and procedures in which human actions and decision-making predominate.

In order to reduce the number of accidents it is, according to Hale's concept of a safety management system, necessary to identify the hazards, determine the risks and to lower them by means of barriers, manage the barriers using management delivery systems and to review and learn from this process (Li, 2019). This chapter provides a guide for the last two steps: which management delivery systems are necessary to manage the barrier systems and what do they provide to prevent future accidents?

Figure 6.1 shows the role of the management delivery systems in risk management (based on Figure 3.1 from Li, 2019). In Hale's concept (2005) the management delivery systems are incorporated in the safety management system (SMS), in this context also referred to as process safety management (PSM). The influence of the management delivery systems on the accidents and near-accidents is indirect, meaning via the barrier systems. In addition to the SMS element "review and audit", Figure 6.1 shows three feedback loops based on which the safety management system can be improved. The information from the three feedback loops can be used to develop indicators. They can provide information concerning the quality of the management delivery systems (loop 1) and of the barrier systems (loop 2). This chapter aims to develop the indicators of loop 1. The loop 2 indicators, which provide insight into the status and quality of the barrier systems, are described in the previous chapter (Schmitz et al., 2020b). The loop 3 indicators can be found in analysed (near) accident processes and are an informative feedback loop regarding learning from accidents and the functioning of the safety management system. The loop 3 indicators, also called lagging indicators, are no part of this study.

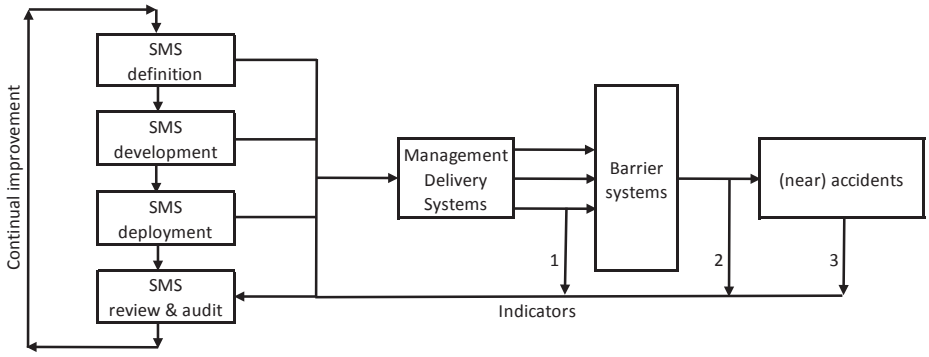

Fig. 6.1, the role of the management delivery systems in the management of risks (SMS = Safety Management System)

6.1.3 Barrier systems

Since the management delivery systems strongly influence the quality of the barrier systems, the question arises where the influence of the management delivery systems on the barrier systems takes place. And how barrier systems are constructed. A barrier system is a set of barriers that are present to prevent causes from developing into consequences (Schmitz et al., 2020b). A barrier consists of elements that detect, decide or act (Guldenmund et al., 2006). Barrier elements can be physical and non-physical or technical and non-technical but can also be subdivided as hardware (with or without software/logic) and humans (Duijm, 2009; Pitblado et al., 2016; Sobral and Guedes Soares, 2019; Li et al., 2020). The human acts as an individual based on his/her knowledge and experience or acts as part of an organisation with its agreements and procedures. In this chapter, the influence of the management delivery systems on the barrier elements (detection, decision, action) is investigated. It is assumed that barrier elements are technical or non-technical, whereby non-technical can be organisational or human in the form of an action or a behaviour.

Occasionally a distinction is made between life cycles for barrier systems. In this sub-study, however, a subdivision per life cycle is not meaningful, because this chapter concerns a characterisation of the various management delivery systems and an overview of the activities of each of them.

6.1.4 Management indicators

What information can organisational factors provide about the accident processes? From scientific and professional literature many indicators can be linked to management delivery systems or organisational factors (Swuste et al., 2016a). Indicators are measures used to describe the state of a broader phenomenon or aspect of reality (Øien, 2001a). According to this definition, management indicators should provide information concerning the operation and efficiency of the management delivery systems or organisational factors.

To assess the quality of the management delivery systems, both qualitative and quantitative measurements must be taken (Nunen van et al., 2018). For example, a management indicator, such as the number of employees who have received safety training, can give a false impression of the quality of the training programme, as it is measured quantitatively but does not consider the content (quality) of the training. Vinnem (2010) cites the preventive maintenance programme as an example: if inspection intervals are too long, there may be no inspection backlog, while the risk may be unacceptably high. On the other hand, if the inspection intervals are very short, the risk of a backlog may still be acceptable.

Audits are the principle tools to assess the quality of management delivery systems. Broadly speaking, there are two types of audits: one focussed on compliance and one on risks.

6.2 COMPLIANCE VERSUS RISK-BASED AUDITS

The 2005 explosion at the BP Texas City refinery is perhaps one of the best investigated incidents and provides a wealth of new insights. One of these insights is the Baker Panel's concern on BP's principal focus of the audits on compliance and verifying that required management systems were in place to satisfy legal requirements (Baker Report, 2007). This was also emphasised in BP's own investigation in which it was stated that audits must include physical verification of the work activity being undertaken to ensure that the practise matches the documented procedure (Mogford, 2005). Numerous audits had been conducted at the site in line with regulatory and corporate requirements, but they had generally failed to identify the systemic problems with work practises (CSB, 2007). However, requiring compliance rather than risk assessments prevents endless discussions about whether certain risk mitigation strategies are needed (Hopkins, 2008). There is clearly a difference in audits that take place on the basis of compliance with legislation, and regulations and audits where risk plays a prominent role.

At the beginning of the millennium, there was a growing interest in what is called "scenario based auditing" (Guldenmund et al., 2006; Zemering and Swuste, 2005). Where regulatory inspections tend to be focussed at the technical level, Hopkins (2008) suggests an additional focus on organisational issues. According to Hopkins, root causes of major accidents, like the BP Texas City refinery incident, are to be found at the organisational level in decisions made by senior managers who are remote from the accident. This chapter provides a way to conduct audits or reviews which are both compliance and risk-based, and which focus on organisational factors that influence the quality of barriers and thus influence the major accident processes. By doing so, major accident processes get the attention they deserve, and the necessary actions are taken at the right management level.

6.3 METHODOLOGY

Management must ensure that barriers work effectively via the management delivery systems (Guillaume, 2011). In Figure 6.2 the management delivery systems are indicated below the bowtie, which shows the integration with the organisation according to De Ruijter and Guldenmund (2016). The bottom-up arrows in Figure 6.2 indicate the

influence of the management delivery systems on the primary barriers. The primary barriers are drawn as thick, vertical lines in the scenario. They stop the development of an accident process and consist of both technical and non-technical barrier elements. Management delivery systems are non-technical in nature. They are work processes and procedures in which human action and decision-making predominate.

Figure 6.2 also shows arrows that do not point at barriers but at scenarios. There are management delivery systems that may promote errors and create latent, dangerous conditions if not properly managed. They are called "performance influencing factors" or "error producing conditions". They may have a general influence on scenarios and impair the effectiveness of the barrier systems (Sonnemans et al., 2010). An example of this is communication such as shift (transfer) reports and work agreements between the maintenance and production departments.

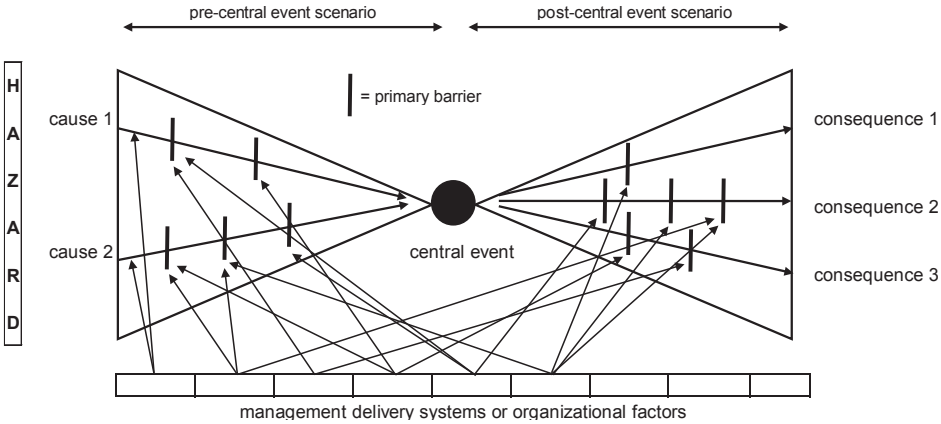

Fig. 6.2, the management delivery systems or organisational factors related to the bowtie

Management delivery systems provide support to the primary barriers. A plan must be drawn up to guarantee this support. The plan may include a course of action or strategy as well as the roles and responsibilities of staff and the deployment of resources. In addition, the plan may contain success factors and goals, and address items like backlog in planning, quality of the work delivered, follow-up of actions, reporting, qualifications of personnel and evaluation of the implementation. The plan must be checked and approved, known and accessible. The design and quality of the plan influence the results of the implementation, both quantitative and qualitative. The results determine the extent to which the primary barriers receive and benefit from the necessary support. The plan must therefore not only be well designed, but also be properly implemented.

When monitoring management delivery systems, it should be determined whether and to what extent they deliver such an output that 1. the barrier systems can be expected to be trustworthy, meaning reliable/available and effective (Schmitz et al., 2020b); 2. no latent, dangerous conditions are created. To assess the management delivery systems, both the plan and the implementation should be monitored qualitatively as well as quantitatively. Existing laws and regulations, the applicable internal requirements and guidelines, current 'good practises' and 'expert judgment' largely set the standard.

6.4 CASE STUDY

A safe installation requires a robust design based on "defence in depth". For any barrier installed to prevent a dangerous scenario from developing, the essential conditions must be identified by the organisation for it to work (Hale, 2005). Once this has been completed, it will then have to be monitored to determine whether the conditions are always being met. Monitoring can be done not only at the level of the (primary) barriers (loop 2 in Figure 6.1), but also at the level of the management delivery systems (loop 1, Figure 6.1). In any case there should be a focus on potential changes (Øien, 2001b). In this way, management delivery systems, as part of the safety management system, contribute to the safe management of organisational to operational level.

6.4.1 The management delivery systems of OCI Nitrogen

In Table 6.2, the organisational factors from Table 6.1 are combined into nine management delivery systems, which are able to support all primary barriers of the accident processes at OCI Nitrogen. They are each described regarding their function and purpose. A management delivery system does not necessarily have to be implemented by one department or team, but can be divided within an organisation, whereby the responsibility may lie with several departments, teams or roles. For example, inspections of pressure equipment are conducted by an independent or external notified body, whereas the testing of instrumental safeguards is done by a maintenance department. Training and education is provided by a number of instructors, who are part of the operational staff. Selection and competence management is done by the HR department in consultation with operational management.

Table 6.2 also provides an overview of the main activities of the nine management delivery systems. The activities are divided into actions related to the plan to achieve the goals and to the implementation of the plan. In the next sections, a number of management delivery systems is elaborated on the basis of two examples.

Table 6.2, description of the organisational factors or management delivery systems at OCI Nitrogen including the associated activities subdivided by plan and implementation

Organisational factors or management delivery systems	Description	Plan and implementation	Activities
Maintenance	The management of predictive, preventive and corrective maintenance programmes (execution, planning and registration) of all hardware and software structures, systems and components.	Plan	Preventive maintenance plan, corrective maintenance goals, quality goals, and strategy regarding outstanding activities
		Implementation	Preventive maintenance backlog, corrective maintenance completion, quality of work and reporting, availability of plant equipment and backup systems, and action tracking
Inspection and testing	The management of the inspection and testing programmes (execution, planning and registration) of all hardware and software structures, systems and components.	Plan	Inspection plan, quality goals, strategy regarding outstanding activities, and inspection and test procedures
		Implementation	Inspection & testing backlog, quality of work and reporting, and action follow-up
Training and competence	The management of selection and training of personnel that guarantees sufficient knowledge and skills for the safe execution of the critical business processes and activities.	Plan	Training programme, training goals, and competence matrix including tasks and responsibilities
		Implementation	Knowledge and skills, education and training, and qualifications and certifications
Management	The management of a company or organisation in which the following aspects play a role: policy, commitment and motivation, goals, planning and availability of personnel, workload, safety culture, conflict management, leadership, and communication with the workforce.	Plan	Planning of work, availability of resources, and production, quality and safety goals
		Implementation	Staffing of teams, workload, follow-up of HSE actions, order and tidiness, committed and informed staff, and safe and healthy working environment, and supervision
Procedures	The management of a system in which rules, working methods and agreements are described concerning, among other things, changes in the plant (MoC, Management of Change), work permits (Permit to Work), job safety analysis (JSA), last minute risk assessment (LMRA), overriding, pre-start-up safety review (PSSR), LoToTo (log-out, tag-out, try-out), and special repair and golden weld procedures.	Plan	Procedures and working methods that are practically feasible and that comply with legislation and regulations
		Implementation	Implementation in accordance with the procedure
Plant documentation	The management of plant related documentation including operating instructions.	Plan	Review plan, and archiving policy
		Implementation	Readability (clarity and completeness), resemblance to the current situation, availability, and accessibility

Table 6.2, continued.

Organisational factors or management delivery systems	Description	Plan and implementation	Activities
Communication and coordination	All oral and written communication and coordination between the different departments of the primary business process.	Plan	Agreements about co-operation, communication, and reporting
		Implementation	Work and shift transfer, co-operation between Operations and Maintenance department, shift reporting, project transfer to the Operations department, and (near) accident reporting
Plant design and operations	The technical design and operation of the plant including the man-machine interface, ergonomics and physical environment.	Plan	Plant spec book, operating instructions, environmental permits, and safety studies including action plans
		Implementation	Plant performance, plant failure, trustworthiness of safety systems (override), plant control system performance (manual mode), use of backup systems, design & safety operating windows, alarm overload, permit violations, and action follow-up from safety studies
Hardware integrity	The condition of the hardware, including the safety critical systems.	Plan	Policy regarding plant availability and spare parts, legislation and regulations, and hardware assessment studies (FMEA, corrosion and mechanical failure mechanisms) including action plans, maintenance programmes, and condition monitoring
		Implementation	Hardware condition incl. safety systems, availability of plant equipment, backup systems and safety critical equipment, integrity operating window, and action follow-up from hardware studies

6.4.2 A near-accident as a result of hydrogen embrittlement

Ammonia was smelled during an operator round in 2018. Further investigation by the plant operator revealed that the insulation shell of a pipe was partially coloured and that synthesis gas and ammonia were leaking out. The ammonia plant was immediately stopped and depressurised. After the insulation material was removed, a crack could be seen along a weld of the pipe. As local repairs were not possible, part of the pipework was removed and replaced. The pipe was cracked circumferentially and partly through the entire wall of 50 mm, indicating high stresses in the pipe system. This was confirmed by the fact that all spring hangers of the pipe system were out of reach. The piping system is provided with spring hangers to balance slight vertical displacements. If the spring hangers are not properly adjusted or do not function properly, large, local tensions can arise in the pipe system.

Metallurgical research has shown that there were no weld defects and the weld met the standards. The conclusion of the metallurgical investigation was that internal, high stresses caused the cracking due to incorrect mounting, too high hardness and a notching effect of the weld. The failure mechanism was classified as hydrogen embrittlement, also known as stable crack growth.

Further investigation revealed that this pipe section was replaced in 2012 when a new heat exchanger was installed. The spring hangers of the pipe system were not fixed when the old pipe was dismantled at the time, after which the new pipe was measured incorrectly. In addition, the bend and the pipe were forcibly aligned before the pipe joint was welded. This resulted in permanent, high tensions at the location of the weld.

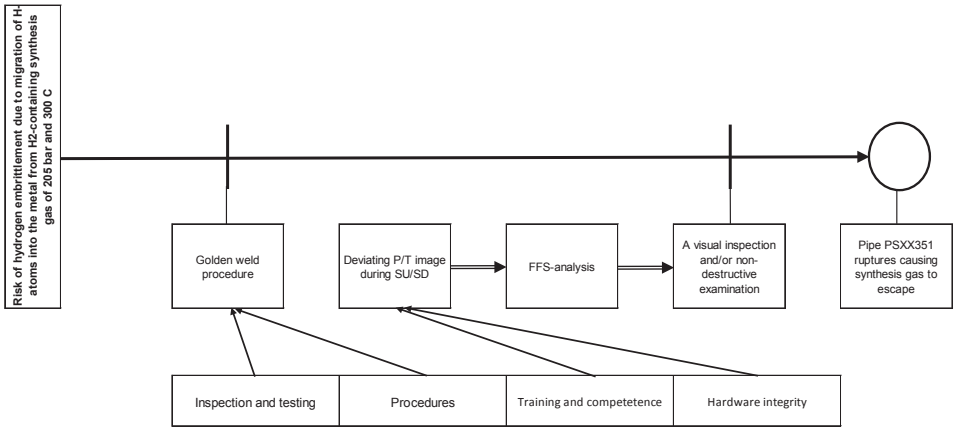

Fig. 6.3, left-hand side of the bowtie of a ruptured pipe due to hydrogen embrittlement (P/T: pressure/temperature; FFS: fitness for service; SU/SD: start-up/shutdown)

The left side of the bowtie of this accident process has been drawn up based on two internal, non-public investigation reports (Figure 6.3). This part of the bowtie shows two (primary) barriers, of which the first primary barrier has one barrier element and the second primary barrier has three elements. The first barrier concerns welding according to a procedure, the so-called golden weld procedure. The golden weld procedure is used in pipelines and piping networks where (hydrostatic) pressure tests can not be performed. The golden weld procedure ensures that safety-critical steps are taken. Failure to follow the procedure properly can lead to a latent, unsafe condition (Schmitz, 2012).

The second barrier comprises of three elements: a different pressure and temperature image during start-up or shutdown of the installation is an indication that hydrogen can become trapped in the metal grid. In combination with increased stresses (including stresses caused by a malfunctioning spring hanger), this may lead to hydrogen embrittlement and cracking. A fitness-for-service analysis and/or a stress calculation can show whether and where an inspection or non-destructive examination should take place. An inspection or non-destructive examination may reveal to what extent cracking has occurred and whether repair or replacement of the weld is necessary.

This accident process could develop because the two barriers did not function or were not present. The golden weld procedure has been in place for a long time and was a mandatory procedure at the time of the new heat exchanger. The investigation established that the procedure was not (fully) followed, meaning that the first barrier was not reliable/available and/or not effective. Knowledge regarding hydrogen embrittlement in this pipeline system was only acquired during the accident investigation. That means the second barrier was not present. A deviating pressure/temperature picture during the start-up and shutdown of the ammonia installation was not reported because it was not deemed necessary. The position of the spring hangers was not considered because their importance has been lost over time.

The four barrier elements of the two primary barriers can be linked to one or more of OCI Nitrogen's nine management delivery systems (Table 6.2) as is shown in Figure 6.3 for the first two barrier elements. The question here is to what extent the malfunctioning of the management delivery systems contributed to the failure of the barrier elements. In Table 6.3, the management delivery systems of the barrier elements "golden weld procedure" and "deviating P/T image" are elaborated.

For the golden weld procedure, the management delivery systems "inspection and testing" and "procedures" play a role and for deviating P/T image these are "training and competence" and "hardware integrity". Table 6.3 shows a non-exhaustive list of

in-depth questions regarding the plan and implementation of the four management delivery systems, which can be answered during an audit or peer review. In order to be able to assess the plan, questions must be asked that elaborate on the development of the plan (control, approval), the familiarity and accessibility, the content (scope, goals, planning, success factors, tasks and responsibilities) and the evaluation. In order to gain insight into the implementation, questions should be raised concerning the realisation of the activities, the backlog of the planning, the quality of the work, the follow-up of actions, the reporting, the qualifications of personnel, and the final evaluation.

Table 6.3, in-depth questions concerning management delivery systems

Management delivery system	Plan / implementation	In-depth questions
Inspection and testing	**Plan:** • Inspection plan • Quality goals • strategy regarding outstanding activities • Inspection and test procedures	• Who drew up the plan? • Who has checked and approved the plan? • What is in the plan (selection, planning)? • Are third parties, "certified bodies" involved? • What goals have been set? • Are the plan and goals known? • Is there a plan regarding outstanding activities? • Are the plan, goals and strategy periodically evaluated? • What is the quality of the inspection and test protocols? • Who has checked and approved these protocols? • Do the protocols meet standards and legislation?
	Implementation: • Inspection & testing backlog • Quality of work and reporting • Action follow-up	• Are the inspectors sufficiently qualified? • How and to whom is reported? • Who assesses and approves the reports? • What should be done in case of deviations? • Who assesses and approves repairs and corrective actions? • To what extent has the plan been implemented according to schedule? • How many inspections meet the set quality? • When is the inspection backlog too extensive? • How is the follow-up of actions arranged? • Is the implementation process periodically evaluated?
Procedures	**Plan:** • Procedures and working methods that are practically feasible and that comply with legislation and regulations	• Are the procedures known and understood? • Are the procedures accessible? • What is the quality of the procedures? • Are the procedures practically feasible? • Do the procedures comply with laws and regulations? • Are the procedures periodically evaluated?
	Implementation: • Implementation in accordance with the procedure	• How is the application of the procedures monitored? • Who assesses deviations in the implementation of the procedures? • What happens if the procedures are not applied or applied incorrectly? • What percentage of the procedures is applied as agreed? • Is the implementation process periodically evaluated?

Table 6.3, continued

Management delivery system	Plan / implementation	In-depth questions
Training and competence	**Plan:** • Training programme • Training goals • Competence matrix	• What is the quality of the training programme? • Are the goals realistic and achievable? • Are all roles addressed in the competence matrix? • Who has drawn up, checked and approved the training programme, goals and competence matrix? • Are the programme, goals and competence matrix periodically evaluated?
	Implementation: • Knowledge and skills • Education and training • Qualifications & certifications	• Is the training programme being carried out according to plan? • How are knowledge and skills tested? • Who assesses the substantive depth of the training courses? • Do the training courses correspond with practise? • Are non-standard situations also trained? • Is the practise supported by theory? • Are major hazard accident processes also discussed? • What happens if someone is insufficiently qualified? • What qualifications do the trainers have? • Is the implementation process periodically evaluated?
Hardware integrity	**Plan:** • Policy regarding plant availability and spare parts • Legislation and regulations • Hardware assessment studies (FMEA, corrosion and mechanical failure mechanisms), including action plans	• Who has drawn up the policy? • Who has checked and approved the policy? • Is the policy periodically evaluated? • Are the latest laws and regulations being acted upon? • Have the corrosion and mechanical failure mechanisms been identified? • Who did the hardware assessment? • How often does a hardware assessment take place? • What are the starting points? • Who checks and approves the assessment studies?
	Implementation: • Hardware condition incl. safety systems • Condition monitoring • Availability and performance of devices • Availability of backup systems • Integrity operating window • Action follow-up from hardware studies	• What is the general condition of the hardware? • How many safety systems are inoperative and why? • How often is the plant availability due to deteriorated hardware condition? • What is the availability of backup systems “on demand”? • Has an integrity operating window been defined? • How often has the integrity operating window been exceeded? • What is the procedure when the integrity operating window has been exceeded? • How is the follow-up of actions from hardware studies arranged? • What is the size of the backlog? • Is the implementation process periodically evaluated?

The golden weld procedure is a well-known procedure which importance and content should be understood by the users. The procedure has been adjusted at times but has never been thoroughly evaluated. Too often the use of the procedure has been supervised from the desk and too little in the field, whereas this is stated in

the procedure. It relied on verbal feedback rather than on field verification. This also applied to the welding in 2012: the bend and the pipe were forcibly aligned before the pipe joint was welded. Had the inspector been on site, the work would have been rejected before welding had even started. The question of how the application of the procedure was supervised, should have provided an indication that the method used in practise deviates from what is stated in the procedure and may have led to dangerous situations.

Knowledge regarding hydrogen embrittlement plays a major role in the second barrier. There was no knowledge concerning the failure mechanism and deviating pressure/ temperature images were not reported because their danger was unknown. Until recently, only the corrosion and mechanical failure mechanisms that could develop during normal operation of the ammonia plant had been assessed. It was only very recently that this was also done for the operational phases of start-up and shutdown, which resulted in knowledge regarding hydrogen embrittlement, and stable crack growth in particular. The studies conducted in the past had never been assessed by an (external) expert. Substantive questions about the results and starting points of the assessment studies could have discovered this gap.

6.4.3 An example of an overpressure scenario

Major hazard accidents are prevented by barriers, which are divided into eleven types by Guldenmund et al. (2006). Three of the most common barrier types are: "activated - manual, human action triggered by active hardware detection(s)", "activated - automated", and "activated - hardware on demand". As explained in section 6.1.3, barrier elements can be technical or non-technical, meaning that they are either hardware or software related, or human or organisation related. The following example examines the management delivery systems of a human barrier element (activated - manual, human action triggered by active hardware detection(s)) and a hardware barrier element (activated – hardware on demand).

Once ammonia is formed, it is cooled and collected in vessel V3304 at 200 bar. From this level controlled vessel, the liquid ammonia is depressurised through an orifice and collected in another vessel (V3305) at much lower pressure. The receiving vessel V3305 may be overpressurised when the orifice is not working properly. This is the case when vessel V3304 is empty and is releasing ammonia gas in stead of liquid. The overpressure scenario is safeguarded by two low level alarms (LAL3045 and LAL3046) installed at V3304 followed by an operator action to close both drain valves (LPV3045 and LPV3046), and a (mechanical) pressure relief valve (PSV3014) at the receiving vessel, as shown in Figure 6.4.

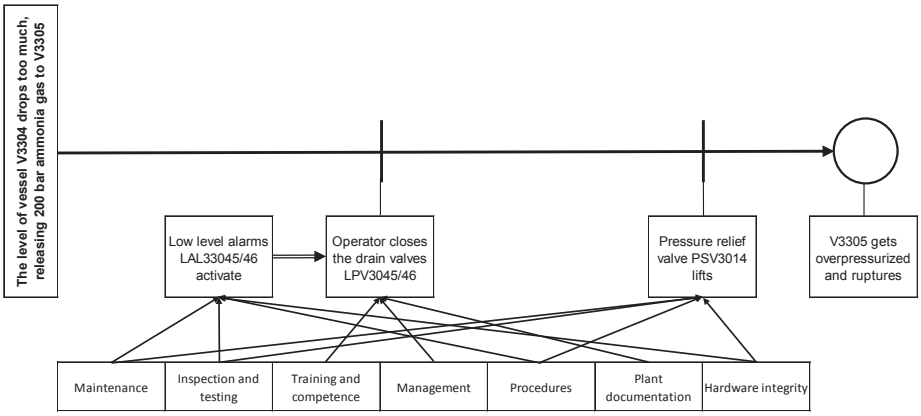

Fig. 6.4, left-hand side of the bowtie of an overpressure scenario of V3305

The barrier system basically consists of two different barrier elements: human and hardware. For the barrier element human (the operator action) the management delivery systems training & competence, plant documentation, and management come into consideration. For the hardware barrier elements, these are maintenance, inspection & testing, procedures, and hardware integrity.

The operator is, as it were, the acting barrier element of the alarm. He/she should know what to do according to the operating instructions. The operator should be trained, know his tasks and responsibilities, and have the most recent information. The organisation should maintain the level of knowledge and ensure that the operators are competent and focussed on their tasks. The "training & competence" plan outlined in Table 6.2 should ensure that there is a training programme that reflects reality, training goals are defined, and a competence matrix is in place including tasks and responsibilities. The department responsible for maintaining the plant documentation also plays an important role. For example, not only should operating instructions be regularly reviewed to ensure they are up to date, but they should also be readily accessible. An archiving policy must ensure that only the most recent version can be requested. Based on the planning and the availability of resources, management must ensure a proper workload, staffing of teams, and supervision on the shopfloor. Because even if the operator has received the right knowledge and operating instructions, unnecessary mistakes are made under work pressure and when supervision is lacking. Good maintenance, testing and inspections are necessary to guarantee the trustworthiness of the (hardware) barriers. The hardware should at least be maintained according to the manufacturer's manual so that the most common defects are avoided. And if a barrier fails, it must be determined in advance with what priority it

will be restored. The maintenance regime can be judged by its backlog of preventive maintenance and the completion of corrective maintenance, but also by the quality of the work and ultimately the availability of the hardware. In addition to proper maintenance, the trustworthiness of barriers must also be guaranteed through testing and inspection. A plan must be drawn up for this, whereby the implementation takes place according to established procedures under the supervision of qualified personnel. Its implementation can be checked based on the measured backlog, the quality of the work and its reporting, and the action follow-up. An override procedure should control the barriers' availability by an established working method and responsibilities. Finally, the assessment of the hardware condition provides a general picture. Use of hardware under extreme conditions make hardware failures more likely. Hardware studies such as a failure mode and effect analysis and condition monitoring can contribute to a better trustworthiness of safety critical equipment, including safety barriers.

6.5 RESULTS AND DISCUSSION

Figure 6.1 shows that there are several feedback loops from which information can be obtained to predict major hazard accidents or detect flaws in the process safety management. Qualitative information of management delivery systems can be generated from audits or peer reviews that are conducted once every three to four years by internal and/or external experts. Management delivery systems can also be partly monitored by self-assessments on a more frequent basis, say annually, by anyone not belonging to the management delivery system but to the organisation and therefore familiar with the organisational issues and work processes. Quantitative monitoring on a more frequent basis should only be conducted when audits or peer reviews do not reveal major shortcomings or findings.

In both the near-accident and the overpressure example, only a qualitative consideration of the management delivery systems has been made. The questions of Table 6.3 are closed questions, to be answered by a yes or no, or by a statement. It is up to the auditors to give their judgement on the plan and implementation. Only if they are confident that the management delivery system is able to guarantee the barrier system's quality, it is meaningful to monitor some critical elements in a quantitative way. An example of a quantitative assessment of the (activities of the) management delivery system "inspection and testing" is shown below. Note that the threshold values are indicative and can serve as management indicators once they are established.

- Periodic evaluation of the plan, goals and strategy: the evaluation is on time and the report is finished no later than two weeks after that;

- Approval of inspection and test protocols: at least 90% has been approved by a third party before execution;
- Protocols meeting standards and legislation: at least 75% has to be compliant;
- Inspectors qualifications: no underqualified inspectors;
- Reporting approval: at least 75% is checked by a peer inspector within the deadline;
- Reporting quality: at least 75% is right the first time;
- Inspection backlog: 90% inspections are done on time and right the first time;
- Action follow-up: no actions overdue longer than 1 month.

Organisational factors or management delivery systems are non-technical in nature and must be regarded as work processes and procedures in which human actions and decision-making predominate. Humans are partly influenced by the environment in which they work and by the systems with which they work, in the course of which they will always try and find the easiest way, even if it is more dangerous. It cannot be assumed that humans always act rationally. Only when an organisation has the right questioning attitude, it will be able to find the mechanisms obstructing their work processes and procedures. Conducting an audit or peer review requires more than just asking questions. According to Hale (2005), safety auditing is an art with very little scientific basis. Both an audit or review and a self-assessment of the plan and its implementation should in any case be substantiated with sufficient samples. It is hard to direct how many samples should be checked from which the auditor or assessor can give an opinion about the functioning and quality of a management delivery system. It mostly depends on the auditee's answers whether follow-up questions are being asked or not.

The questions in Table 6.3 are mainly procedural in nature and largely ignore interpersonal relationships. Communication and co-operation (not understanding, poor communication, not being informed) are vital and necessary for work processes and procedures to function properly. In addition, there may be contradictory goals or limitations in time and/or resources, as a result of which choices must be made, making it not always possible to follow the procedure in full. It is up to the auditor to discover these sensitivities and determine to what extent they hinder the functioning of the management delivery systems as a whole.

6.6 CONCLUSIONS

The main question of this sub-study is whether major hazard accidents related to the ammonia production process can be predicted by monitoring organisational factors. This question has been answered from five sub-questions. A (non-exhaustive) overview

has been provided of organisational factors or management delivery systems from the scientific and professional literature. The relation of the organisational factors with the accident processes runs through the barrier systems. Organisational factors indirectly impact accident processes as they strongly influence the quality or trustworthiness of the barrier systems. Qualitative and quantitative monitoring of organisational factors can provide a picture of their operation and efficiency. A list of nine organisational factors or management delivery systems has been compiled which are applicable for OCI Nitrogen. By putting the right focus on organisational factors during audits or reviews, major accident processes get the attention they deserve, and the necessary actions are taken at the right management level. From an example on retrospective data it has been demonstrated that targeted questions could have provided such an insight into several organisational factors or management delivery systems that it is conceivable that further in-depth investigation would have prevented the near-accident from happening.

Malfunctioning management delivery systems can promote a major hazard accident process. Management delivery systems like management, and communication and coordination could also be considered as “performance influencing factors” or “error producing conditions”. Their influence on scenarios is more general in nature and not through the barrier systems, but via promoting errors and creating latent, dangerous conditions if they are not properly managed.

A quantitative assessment has been worked out for one of the management delivery systems so to provide an example of management indicators. But as the examples shows, determining threshold values for which action is required is an intricate matter, because the influence on the accident processes is difficult to determine. More retrospective research into accidents is required to validate these threshold values. Once threshold values have been set, (management) indicators can be developed, which are measured at a frequency of, for example, once a month or once a quarter.

6.7 REFERENCES

Ale, B., Baksteen, H., Bellamy, L., Bloemhof, A., Goossens, L., Hale, A., Mud, M., Oh, J., Papazoglou, I., Post, J. & Whiston, J. (2008). Quantifying occupational risk: The development of an occupational risk model. *Safety Science, 46*, 176–185. http://dx.doi.org/10.1016/j.ssci.2007.02.001.

Baker report. (2007). *The report of the BP U.S. refineries independent safety review panel*. Retrieved from https://www.csb.gov/bp-america-refinery-explosion/.

Bellamy, L.J., Ale, B.J.M., Geyer, T.A.W., Goossens, L.H.J., Hale, A.R., Oh, J., Mud, M., Bloemhof, A., Papazoglou, I.A., & Whiston, J.Y. (2007). Storybuilder – A tool for the analysis of accident reports. *Reliability Engineering and System Safety, 92*, 735–744. http://dx.doi.org/10.1016/j.ress.2006.02.010.

Bellamy, L. (2015). Exploring the relationship between major hazard, fatal and non-fatal accidents through outcomes and causes. *Safety Science, 71*, 93–103. http://dx.doi.org/10.1016/j.ssci.2014.02.009.

CCPS. (2016). *Guidelines for implementing process safety management* (2nd ed.). Hoboken, US: John Wiley & Sons Inc.

Crisislab. (2016). *Toeval of structureel incidentalisme? Negen incidenten uit 2015 bij Chemelot nader beschouwd*. Retrieved from http://crisislab.nl/wordpress/wp-content/uploads/2016-06-07-rapport-Chemelot-def.pdf.

CSB. (2007). *Investigation report, Refinery Explosion and Fire BP Texas City*. Retrieved from https://www.csb.gov/bp-america-refinery-explosion/.

Duijm, N. (2009). Safety-barrier diagrams as a safety management tool. *Reliability Engineering and System Safety, 94*, 332–341. http://dx.doi.org/10.1016/j.ress.2008.03.031.

Guillaume, E. (2011). *Identifying and responding to weak signals to improve learning from experiences in high-risk industry* (Doctoral's thesis). Retrieved from https://repository.tudelft.nl/islandora/object/uuid:f455e8a0-cce5-4a36-8a98-f83371dc2a2a.

Guldenmund, F., Hale, A., Goossens, L., Betten, J., & Duijm, N.J. (2006). The development of an audit technique to assess the quality of safety barrier management. *Journal of Hazardous Materials, 130*, 234–241. http://dx.doi.org/10.1016/j.jhazmat.2005.07.011.

Hale, A. (2005). Safety Management, what do we know, what do we believe we know, and what do we overlook? *Tijdschrift voor toegepaste Arbowetenschap, 2005*(3), 58–66.

Hale, A., Ale, B., Goossens, L., Heijer, T., Bellamy, L., Mud, M., Roelen, A., Baksteen, H., Post, J., Papazoglou, I., Bloemhoff, A. & Oh, J. (2007). Modelling accidents for prioritizing prevention. *Reliability Engineering and System Safety, 92*, 1701–1715. http://dx.doi.org/10.1016/j.ress.2006.09.025.

Hassan, J., & Khan, F. (2012). Risk-based asset integrity indicators. *Journal of Loss Prevention in the Process Industries, 25*, 544–554. http://dx.doi.org/10.1016/j.jlp.2011.12.011.

Hopkins, A. (2008). *Failure to Learn*. Sydney, Australia: CCH Australia Ltd.

HSE. (2006). *Developing process safety indicators, a step-by-step guide for the chemical and major hazards industries*. Retrieved from http://www.hse.gov.uk/pUbns/priced/hsg254.pdf.

Kletz, T. (1988). *Learning from accidents in industry*. London, UK: Butterworths.

Kongsvik, T., Almklov, P. & Fenstad, J. (2010). Organisational safety indicators: Some conceptional considerations and a supplementary qualitative approach. *Safety Science, 48*, 1402–1411. http://dx.doi.org/10.1016/j.ssci.2010.05.016.

Li, Y. (2019). *A systematic and Quantitative Approach to Safety Management* (Doctoral's thesis). Retrieved from https://repository.tudelft.nl/islandora/object/uuid%3A458a384f-6f8a-4fc3-8bc4-c01397b54b59.

Li, Y., Guldenmund, F. & Aneziris, O. (2020). Delivery systems: A systematic approach for barrier management. *Safety Science, 121*, 679–694. http://dx.doi.org/10.1016/j.ssci.2017.02.007.

Mogford, J. (2005). *Fatal accident investigation report*. Retrieved from http://cip.management.dal.ca/publications/final_report.pdf.

Nunen van, K., Swuste, P., Reniers, G., Paltrinieri, N., Aneziris, O. & Ponnet, K. (2018). Improving Pallet Mover Safety in the Manufacturing Industry: A Bow-Tie Analysis of Accident Scenarios. *Materials, 11*, 1–19. http://dx.doi.org/10.3390/ma11101955.

Øien, K. (2001a). Risk indicators as a tool for risk control. *Reliability Engineering and System Safety, 74*, 129–145.

Øien, K. (2001b). A framework for the establishment of organizational risk indicators. *Reliability Engineering and System Safety, 74*, 147–167.

Øien, K., Utne, I. & Herrera, I. (2011). Building Safety indicators: Part 1 – Theoretical foundation. *Safety Science, 49*, 148–161. http://dx.doi.org/10.1016/j.ssci.2010.05.012.

OSHA. (s.d.). *Process Safety Management*. Retrieved from https://www.osha.gov/Publications/osha3132.html.

OVV. (2018). *Chemie in samenwerking – Veiligheid op het industriecomplex Chemelot*. Retrieved from https://www.onderzoeksraad.nl/nl/page/4707/chemie-in-samenwerking---veiligheid-op-het-industriecomplex-chemelot.

Papazoglou, I., Bellamy, L., Hale, A, Aneziris, O., Ale, B., Post, J. & Oh, J. (2003). I-Risk: development of an

integrated technical and management risk methodology for chemical installations. *Journal of Loss Prevention in the Process Industries, 16*, 575–591. http://dx.doi.org/10.1016/j.jlp.2003.08.008.

Perrow, C. (1984). *Normal accidents. Living with high-risk technologies*. New York, US: Basic Books.

Pitblado, R., Fisher, M., Nelson, B., Fløtaker, H., Molazemi, K. & Stokke, A. (2016). Concepts for dynamic barrier management. *Journal of Loss Prevention in the Process Industries, 43*, 741–746. http://dx.doi.org/10.1016/j.jlp.2016.07.005.

Reason, J. (1987). The Chernobyl errors. *Bulletin of the British Psychological Society, 40*, 201–206.

Reason, J. (1997). *Managing the risks of organizational accidents*. Abingdon, UK: Taylor & Francis.

Ruijter, A. de, & Guldenmund, F. (2016). The bowtie method: A review. *Safety Science, 88*, 211–218. http://dx.doi.org/10.1016/j.ssci.2016.03.001.

Schmitz, P. (2012). *Meer veiligheid met minder regels* (Master's thesis).

Schmitz, P., Swuste, P., Theunissen, J., Reniers, G., Decramer, G., & Uijterlinde, P. (2018). Een aanpak voor het bepalen van een realistische ranking van de gevaarlijkste procesonderdelen van het ammoniakproductieproces. *Tijdschrift voor toegepaste Arbowetenschap, 2018*(2), 42–56.

Schmitz, P., Swuste, P., Reniers, G., & Decramer, G. (2019). Een aanpak voor het beoordelen van mechanische faalmechanismen van statische apparaten van het ammoniakproductieproces. *Tijdschrift voor toegepaste Arbowetenschap, 2019*(2), 34–54.

Schmitz, P., Swuste, P., Reniers, G., & Nunen van, K. (2020a). Mechanical integrity of process installations: barrier alarm management based on bow-ties. *Process Safety and Environmental Protection, 138*, 139–147. https://doi.org/10.1016/j.psep.2020.03.009.

Schmitz, P., Swuste, P., Reniers, G., & Nunen van, K. (2020b). Een praktische aanpak voor het voorspellen van majeure ongevallen in de procesindustrie op basis van de barrière status op scenario niveau. *Tijdschrift voor toegepaste Arbowetenschap, 2020*(2), 47–66.

Sobral, J. & Guedes Soares, C. (2019). Assessment of the adequacy of safety barriers to hazards. *Safety Science, 114*, 40–48. https://doi.org/10.1016/j.ssci.2018.12.021.

Sonnemans, P.J.M., Körvers, P.M.W., & Pasman, H.J. (2010). Accidents in "normal" operation – Can you see them coming?. *Journal of Loss Prevention in the Process Industries, 23*, 351–366. http://dx.doi.org/10.1016/j.jlp.2010.01.001.

Swuste, P., Theunissen, J., Schmitz, P., Reniers, G., & Blokland, P. (2016a). Process safety indicators, a review of literature. *Journal of Loss Prevention in the Process Industries, 40*, 162–173. http://dx.doi.org/10.1016/j.jlp.2015.12.020.

Swuste, P., Gulijk van, C., Zwaard, W., Lemkowitz, S., Oostendorp, Y. & Groeneweg, J. (2016b). Developments in the safety science domain, in the fields of general and safety management between 1970 and 1979, the year of the near disaster on Three Mile Island, a literature review. *Safety Science, 86*, 10–26. http://dx.doi.org/10.1016/j.ssci.2016.01.022.

Swuste, P., Gulijk van, C., Groeneweg, J., Zwaard, W., Lemkowitz, S. & Guldenmund, F. (2020a). Occupational safety and safety management between 1988 and 2010: Review of safety literature in English and Dutch language scientific literature. *Safety Science, 121*, 303–318. http://dx.doi.org/10.1016/j.ssci.2019.08.032.

Swuste, P., Gulijk van, C., Groeneweg, J., Zwaard, W., Lemkowitz, S. & Guldenmund, F. (2020b). From clapham junction to macondo, deepwater horizon: Risk and safety management in high-tech-high-hazard sectors. A review of English and Dutch literature: 1988–2010. *Safety Science, 121*, 249–282. http://dx.doi.org/10.1016/j.ssci.2019.08.031.

Turner, B. (1978). *Man-made disasters*. Oxford, UK: Butterworth-Heinemann.

Vinnem, J.E. (2010). Risk indicators for major hazards on offshore installations. *Safety Science, 48*, 770–787. http://dx.doi.org/10.1016/j.ssci.2010.02.015.

Wagenaar, W., Groeneweg, J., Hudson, P. & Reason, J. (1994). Promoting safety in the oil industry. The Ergonomics Society Lecture Presented at the Ergonomics Society Annual Conference, Edinburgh, 13-16 April 1993. *Ergonomics, 37:12*, 1999–2013. http://dx.doi.org/10.1080/00140139408964963.

Zemering, C., & Swuste, P. (2005). Voorstel voor een methode ter preventie van incidenten en rampen in de procesindustrie. *Tijdschrift voor toegepaste Arbowetenschap, 2005*(4), 79–88.

7

PREDICTING MAJOR HAZARD ACCIDENTS BY MONITORING THEIR BARRIER SYSTEMS: A VALIDATION IN RETROSPECTIVE[7]

7 The Chapter is based on the paper: Schmitz, P., Reniers, G. & Swuste, P. (2021). Predicting major hazard accidents by monitoring their barrier systems: a validation in retrospective. *Process Safety and Environmental Protection, 153*, 19–28. https://doi.org/10.1016/j.psep.2021.07.006, and was formatted and edited for this thesis.

ABSTRACT

This chapter contains a validation of the model by looking at the BP Texas City incident in 2005. The bowtie metaphor is used to visually present the BP Texas City refinery incident, showing the barrier system from different perspectives. Not only is the barrier system looked at from its trustworthiness on the day of the incident but also from the perspective of the control room operator, and from a design to current standards of best practise. The risk reductions of these different views are calculated and compared to their original design. In addition, evidence and findings from the investigations have been categorised as flaws and allocated to nine organisational factors. These flaws may affect the barrier system's quality or trustworthiness, or may act as 'accident pathogens' (see also Reason, 1990) creating latent, dangerous conditions. This chapter sheds new light on the monitoring of accident processes and the barrier management to control them, and demonstrates that the BP Texas City refinery incident could have been foreseen using preventive barrier indicators and monitoring organisational factors.

7.1 INTRODUCTION

This chapter offers a validation of the model by looking in retrospect at a major hazard accident, the 2005 BP Texas city incident, using chapter 5 and 6 in particular. It answers the following research question:

> *To what extent could the BP Texas City refinery incident have been foreseen using preventive barrier indicators and monitoring organisational factors?*

BP's Texas City refinery incident in 2005 is probably one of the most extensively investigated incidents ever. It has been investigated by BP internally (BP, 2005) as well as externally by the U.S. Chemical Safety and Hazard Investigation Board (CSB, 2007). During the CSB investigation two major incidents occurred which were so shocking that the CSB urged BP to conduct a study into the effectiveness of BP North America's corporate oversight of safety management systems at its refineries and its corporate safety culture, known as the 'Baker report' (Baker, 2007). According to Baker's report, BP's most recent internal audits revealed deficiencies at their Texas City site, such as poor safety culture, poor condition of the assets, and inability to identify and assess process hazards and risks, to mention just a few. However, BP did not ensure timely compliance with its internal process safety standards and programs. Hopkins was asked by the CSB to join their inquiry and issued a book in 2008 on BP's failure to learn (Hopkins, 2008), in which he discloses various aspects of BP's malfunctioning management and inability to take process risks seriously (Swuste, 2010). All these reports have been used to find evidence of the declining barrier system and the loss of efficiency of the organisational factors or management delivery systems which played a role in this incident. This chapter investigates how and to what extent this evidence could have served as an early warning. As this investigation is focussed on prevention of the incident, it does not look into the accident process after the overfilling of the blowdown drum, like the trailer siting and the traffic policy.

This section will briefly explain the chemical process concerned in the BP Texas City disaster and how the accident unfolded. The raffinate splitter section is shown in Figure 7.1 (CSB, 2007). During start-up, heavy raffinate is pumped into the 170 ft tall raffinate splitter tower, also called splitter. The heavy raffinate output exits the splitter at the bottom and is routed through two heat exchangers, the first one to preheat the raffinate feed into the splitter, the second one to cool down before being sent to the storage tanks. The light raffinate leaves at the top of the splitter and is routed down a 45 m pipe along the side of the splitter after which it passes a condenser and is sent to the light raffinate storage tanks.

The splitter is provided with a level transmitter (LT) from which a high alarm is derived, and with an independent, hard-wired high and low level alarm (LAH resp. LAL). The overhead line is equipped with a pressure transmitter (PT) from which a high pressure alarm (by BP indicated as high high pressure alarm) is derived, and with three safety relief valves, which outputs are connected to the blowdown drum. The blowdown drum has a high level alarm (LAH).

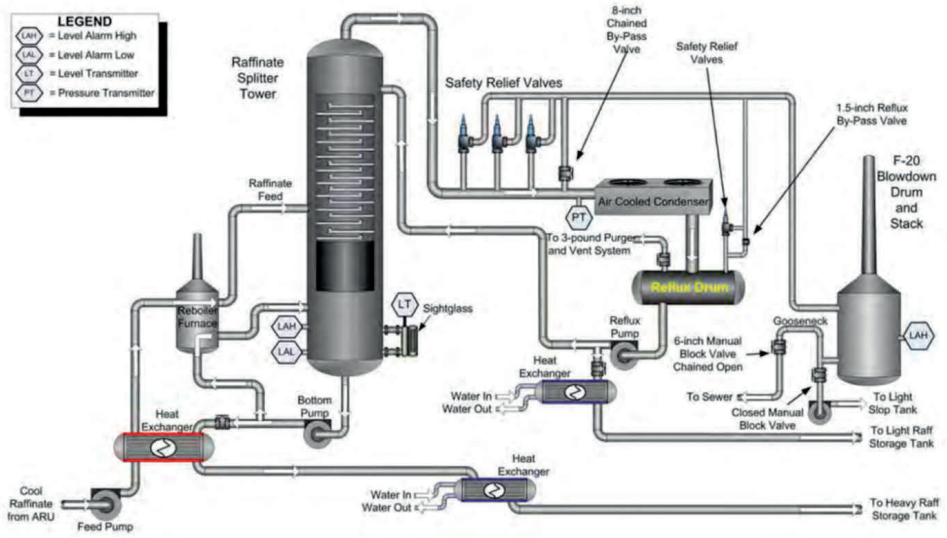

Fig. 7.1, raffinate section of the ISOM unit (CSB, 2007)

The CSB report (2007) described the incident as follows: On the morning of March 23, 2005, the raffinate splitter tower in the refinery's ISOM unit was restarted after a maintenance outage. During the start-up, operations personnel pumped flammable liquid hydrocarbons into the tower for over three hours without any liquid being removed, which was contrary to start-up instructions. Critical alarms and control instrumentation provided false indications that failed to alert the operators of the high level in the tower. Consequently, unknown to the operations crew, the 170-foot (52-m) tall tower was overfilled and liquid overflowed into the overhead pipe at the top of the tower.

The overhead pipe ran down the side of the tower to safety relief valves located 148 feet (45 m) below. As the pipe filled with liquid, the pressure at the bottom rose rapidly from about 21 pounds per square inch (psi) to about 64 psi. The three safety relief valves opened for six minutes, discharging a large quantity of flammable liquid to a blowdown drum with a vent stack to the atmosphere. The blowdown drum and stack overfilled with

flammable liquid, which led to a geyser-like release out of the 113-foot (34 m) tall stack. This blowdown drum was an antiquated and unsafe design; it was originally installed in the 1950s, and had never been connected to a flare system to safely contain liquids and combust flammable vapours released from the process.

The released volatile liquid evaporated as it fell to the ground and formed a flammable vapour cloud. The most likely source of ignition for the vapour cloud was backfire from an idling diesel pickup truck located about 25 feet (7.6 m) from the blowdown drum. The 15 employees killed in the explosion were contractors working in and around temporary trailers that had been previously sited by BP as close as 121 feet (37 m) from the blowdown drum.

7.2 REAL-TIME PERFORMANCE MONITORING AND DYNAMIC RISK ASSESSMENT

There is a lack of effective monitoring and modelling approaches that provide early warnings and help to prevent events (Kalantarnia et al., 2010). Major hazard accidents or low frequency, high consequence events are very rare events for which a classical statistical approach is ineffective (Meel et al., 2007). Static risk assessments conducted during an engineering phase or during a safety study do no longer satisfy today's needs. In recent years more and more research has been conducted into dynamic risk assessments in which methods have been developed to regularly update risk profiles. One option for real-time monitoring is based on physical parameters (operational deviations and mishaps) which can provide an actual picture of the risk performance of a (petro)chemical installation. This has been worked out for an ammonia plant in which mechanical integrity has a large share in its risk profile (Schmitz et al., 2020). Estimated risks can be readily revised when physical parameters are monitored and observed during process operation time (Khakzad et al., 2012). In recent studies (Aven et al., 2006; Meel and Seider, 2006; Meel et al., 2007; Vinnem et al., 2006, 2009; Kalantarnia et al., 2010; Rathnayaka et al., 2011; Skogdalen and Vinnem, 2012; Yang et al., 2013; Khakzad et al., 2011, 2013, 2014, 2015; Paltrinieri et al., 2015; Kang et al., 2016), the estimation of the rare event frequency is based on other precursor data, like the occurrence of (near) accidents over time, the human and equipment failure probabilities, and the performance of the safety barrier system.

The last one is central to this chapter's validation and is elaborated in the next section. It analyses not only the safety barrier system but also the management of it. The analysis can not only be used to update the risk profile in real-time, but can also be used to remove the vulnerabilities, optimise the (management of the) current safety

barrier system, and improve the design of new safety barrier systems.

7.3 METHODOLOGY

This validation is based on a method which is described in chapters 5 and 6, which relate to preventive barrier indicators, and organisational factors respectively. The model uses the bowtie metaphor to visually present the accident process of the BP Texas City refinery incident. It shows the initiating event (the restart of the ISOM unit), the installed barriers, and the central event which is split up into the splitter overfilling and the blowdown drum overfilling. This research focusses on the left-hand side of the bowtie with the preventive barriers, meaning all barriers which should have prevented the blowdown drum from overfilling. Firstly, we assess the quality or trustworthiness of the preventive barrier system. The quality or trustworthiness of barriers relates to their parameters reliability/availability and effectiveness and establishes the risk reduction. The risk reduction of the barrier system is determined by the risk reduction of the individual barriers. Decrease of quality or trustworthiness of one or more barriers means less risk reduction of the barrier system. A full risk reduction according to design is only guaranteed if all barriers are trustworthy.

When the risk reduction of the barrier system is expressed using the Briggs logarithm (logarithm with base 10), it can be readily compared with its designed risk reduction. This relative risk reduction in Briggs logarithm (RRRL) is expressed as a percentage and called preventive barrier indicator. Its value serves as an indicator for the likelihood of the central event, which is not an absolute value, but rather an indication of the change in the *status quo* that should initiate further action (for more information see also Schmitz et al., 2021a). For the calculation of the preventive barrier indicator, the scenario is looked at in three ways:

1) With the preventive barrier system as designed on the day of the incident, meaning a level control including a high level alarm derived from it, a start-up procedure, a hard-wired high level alarm, a high pressure alarm in the overhead line, and a high level alarm at the blowdown drum, most of which were only partly trustworthy;
2) With the preventive barrier system as perceived by the day shift control room operator on the day of the incident, meaning a level control including a high level alarm derived from it, a start-up procedure, a hard-wired high level alarm, a high pressure alarm in the overhead line, and a high level alarm at the blowdown drum, all of which were assumed to be fully trustworthy;
3) With the preventive barrier system according to current standards of best practise, meaning a level control including a high level alarm derived from it,

a start-up procedure, a mass imbalance alarm, a hard-wired high level alarm, a high pressure switch in the overhead line, and a high level switch at the blowdown drum, most of which are designed to be fully trustworthy.

Secondly, we study the organisational factors or management delivery systems which can also be linked to accident processes and their barrier system (Schmitz et al., 2021b). Flaws in organisational factors may indirectly impact accident processes as organisational factors are responsible for delivering the required quality or trustworthiness of the barrier system. For each barrier, the appropriate organisational factors are selected as well as the shortcomings identified from the investigation reports, which could have provided information about the deterioration of the barrier's quality. In addition, organisational factors may also influence accident processes in a more general way, not through the barrier system, but via promoting errors and creating latent, dangerous conditions if they are not properly managed. In short, both the organisational factors related to the barriers and to the accident process itself are looked at so to determine which information could have supported BP Texas City HSE management to discover the development of this major hazard accident prematurely.

7.4 RESULTS

The critical initiating event of the BP Texas City refinery incident was the restart of the ISOM unit with raffinate flowing into the splitter but none flowing out (Saleh et al., 2014). The hazard, the raffinate's flammability, becomes uncontrollable at the central event, meaning at the overfilling of the splitter, and even worse at the overfilling of the blowdown drum. What happened after the geyser-like release from the blowdown stack is less relevant to this validation. In the first section, the barriers are assessed for their quality or trustworthiness. The scenario's barrier system is looked at from three different perspectives:

1) as designed on the day of the incident;
2) as perceived by the day shift control room operator on the day of the incident;
3) as meeting current standards of best practise.

The second section discusses the organisational factors that influenced the trustworthiness of the barriers as well as the organisational factors that contributed more generally to the incident.

7.4.1 Preventive barrier indicators

Figure 7.2 shows the barriers that were present on the day of the incident to prevent the splitter and blow-off drum from overfilling. The barriers are:

- A float-type level transmitter (indicated as LT in the splitter's bottom part in Figure 7.1) which measures the level in the splitter's bottom and enables controlling the level by draining heavy raffinate from it. The splitter's level can be read from the panels in the control room.
- A start-up procedure including some of the main following steps (BP, 2005): establish feed to the tower; pack the reboiler recirculation pumps; establish 50% level in the tower; establish reboiler circulation to pack reboiler circuit; establish heavy raffinate rundown flow to tankage; set tower level control to Auto with 50% set point; light reboiler furnace pilots; light reboiler furnace main burners; set reboiler furnace temperature control to Auto; heat up to 275°F at 50°F per hour; establish level in reflux drum.
- A signal (not indicated in Figure 7.1) derived from the level transmitter indicating to the control room operator that he is about to exceed the safe operating window. This first high level alarm was set at 72% of the transmitter value. To get the level back to a normal value, the control room operator could check the balance between in and output and adjust either one of them.
- A redundant hard-wired high level alarm (indicated as LAH in the splitter's bottom part in Figure 7.1) at 78% of the transmitter value, indicating that the level in the stripper's bottom is too high. At this point the control room operator should stop the stripper, meaning stop the feed and close the gas supply to the furnace.
- A high pressure alarm derived from the pressure transmitter (indicated as PT next to the air cooled condenser in Figure 7.1), located in the overhead line close to the relief valves and the air cooled condenser. Depending on the setting (which is unknown to the authors) the best way forward is to go to a safe state by stopping the stripper's feed and closing the gas supply to the furnace.
- A high level alarm at the blowdown drum (indicated as LAH in Figure 7.1) which indicates that the blowdown drum is filled up to the goose neck's level. At this alarm every potential source needs to be stopped as quickly as possible, which would include stopping the stripper's feed followed by shutting down the stripper's furnace.

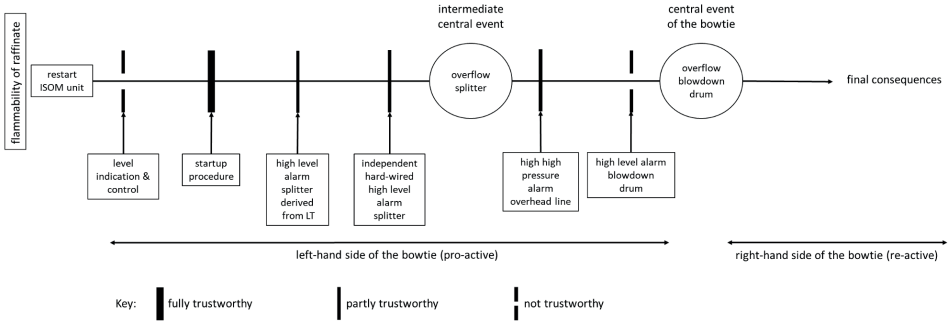

Fig. 7.2, the barrier system as designed on the day of the incident

Following the selection of the potential barriers, the next question is whether these barriers are trustworthy or sound in a way that they are able to timely stop the overfill scenario from developing. And in addition, to which extent will they reduce the risk?

From a LoPA or Layer of Protection Analysis (CCPS, 2015) view, a basic process control system is an independent layer of protection (IPL). A properly working level indication and control would have given the control room operator the opportunity to check the splitter's level over its entire length. This level transmitter however has a limited range and becomes unreliable when both impulse lines (connecting lines from the level transmitter to the splitter) are submerged. And even worse, the level indication was misleading when the splitter was heated up causing the operators to be unaware of the situation they were in (Hopkins, 2008). The operators were blind to the liquid level in the splitter which decreased their ability to 'see' and comprehend the developing hazardous situation (Saleh et al., 2014). Hence, the design of level indication and control in the control room is such that it can not be classified as an IPL or barrier on the day of the incident and as a result it provides no risk reduction.

Although the start-up procedure is not fully up to date, it is generally of high quality, with safety cautions and an appropriate level of detail addressing all the key process control steps (BP, 2005). If adhered to, the start-up procedure reduces the risk by 10, which is a generic reduction for a well designed operating procedure with simple steps that can be carried out without time pressure (CCPS, 2015; Kirwan, 1994).

The four (alarm) barriers are not fully independent as the control room operator is their common 'acting' barrier element. In general, human responses can reduce the risk by 10 (CCPS, 2015). This is only true if these human responses are trained, understood, easy to conduct, and can be taken in a reasonable time. The hardware side of the alarm should preferably be designed as a SIL1 classified instrument, or at least be

properly installed and well maintained. The risk reduction of the four alarms heavily depends on the control room operator's response and could look like this: for both the splitter's high-level alarms there is enough time to take action. However, since both alarms draw the control room operator's attention to a high level, and the second alarm activates if the response of the first has been unsuccessful, it is defensible that the joint risk reduction is close to 10. The action of the high pressure alarm is relatively simple, but should be carried out quickly in situations that are most likely to be stressful. As enhanced stress levels increase the human error probability (Kirwan, 1994), it is assumed to be between 1 (no risk reduction) and 10. In the event of a high level alarm of the blowdown drum, the control room operator must react quickly in a complex situation as it requires a highly coordinated action of operators to prevent a coming disaster. If the high level alarm would have functioned properly (which it did not at the time of the incident), it would have taken approximately two minutes before raffinate is released from the stack. The chance of a successful response appears to be so small that this barrier should be disregarded as such.

That brings the total reduction of the barrier system between 100 and 1000: a risk reduction of 10 for the start-up procedure, 10 for both level alarms of the splitter, and a risk reduction between 1 and 10 for the high pressure alarm. Expressed using the Briggs logarithm this would come down to a value between 2 and 3. Figure 7.2 shows the barriers which should be disregarded (with a hole), and which should be taken into account, meaning a thick solid line equals a risk reduction of 10, and a thin solid line equals a risk reduction between 1 and 10. The risk reduction expressed in Briggs logarithm (RRL) as designed is most likely 6 (a risk reduction of 10 for each barrier), which in reality turns out to be between 2 and 3 at most. The relative risk reduction expressed in Briggs logarithm (RRRL) is between 33% (2/6 x 100%) and 50% (3/6 x 100%) for the whole pre-central event scenario up to the blowdown drum overflow. If the pre-central event scenario would be considered up to the splitter's overflow, there are only four barriers and the RRRL equals 50% (2/4 x 100%).

From the day shift control room operator's perspective, using the accident investigation reports (BP, 2005; CSB, 2007; Hopkins, 2008), the barrier system looks slightly different as shown in Figure 7.3. He took over from the night shift control room operator and was probably under the impression that the preparatory activities were done. The preparatory activities include a pre start-up review which is merely a check that the procedure is still adequate for the task, and that the crew members understand the procedure. In addition, it includes a check of the instrumentation, alarms and trips, a commissioning of the utilities like steam, electric power, cooling water; ensure tightness, removal of air through vents, removal of water through low point drains, and removal of isolation blinds. In short, the preparatory activities should guarantee that

the installation is sound and fit for purpose, and that the crew is well informed, trained, and capable of starting up safely. The day shift control room operator had no reason to believe other than that he could proceed with the start-up, because he would have been told otherwise.

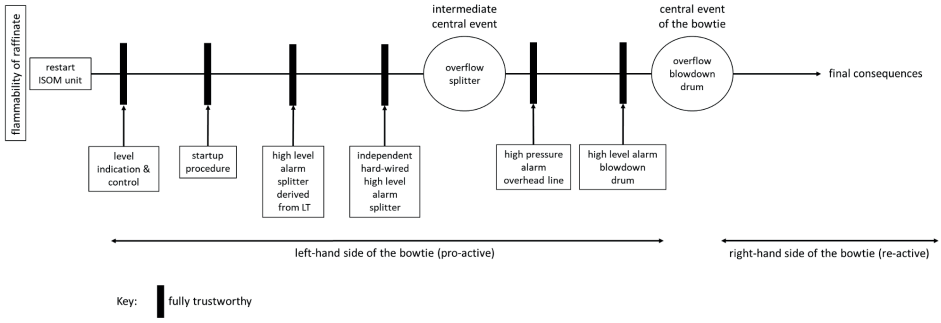

Fig. 7.3, the barrier system perceived by the day shift control room operator on the day of the incident

What did the barrier system look like on the day of the incident? From the investigations it appeared that the preparatory activities had not fully taken place and that the instrumentation, alarm and trip test had been aborted due to time pressure. The night shift control room operator loaded the stripper for 100% level where 50% is prescribed. The new shift did not realise the extent to which the column and pipework was packed. The heavy raffinate rundown was not established as the day shift control room operator believed that he had been instructed not to open the heavy liquid outflow valve (shown in Figure 7.1 between the splitter's bottom pump and the heat exchanger) because the storage tanks were full. This was true as during the management meeting the decision was made not to proceed because the heavy raffinate tanks were full. But the operators were not told of this decision and went ahead with the start-up (Hopkins, 2008). The day shift control room operator continued filling up the stripper and ignored setting the stripper's level control to auto with 50% set point, still with no outflow of heavy raffinate from the bottom. There is a good reason to slightly overfill the stripper's bottom as the pump and the furnace's pipework (when lit) could be damaged if the level would drop to zero while liquid is being pumped out of the bottom. As the equipment was safeguarded against damage by low level, which would terminate the start-up, operators had a good reason for this practise. In addition to the filling of the stripper, the stripper's liquid was heated up too much and too quickly which contributed to an unexpected level rise when the heavy raffinate was eventually drained. In short, important steps of the start-up procedure were not adhered to, causing the stripper to be overfilled.

The high level alarm derived from the splitter's level transmitter and set at 72%, had been ignored which makes sense when the intention was to fill the stripper to a higher level than prescribed. The setting of the independent, hard-wired high level alarm however was unknown to the day shift control room operator. Although Hopkins (2008) claims that this alarm is essentially irrelevant as the splitter was intended to be filled up to 9 feet or more, it could have been an early warning to investigate the 'real' level. Fact is that this level alarm was unavailable and was not activated. When the heavy raffinate was drained to the tankage, the stripper's level rose quickly and filled up the overhead line. The high pressure alarm alerted the control room operator when the relief valves lifted, which gave the operator hardly any chance to respond to this unknown, complex situation. Within minutes raffinate was released from the stack of the blowdown drum and formed a pool around its base, waiting to be ignited. The high level alarm of the blowdown drum sounded at the time of the explosion. It has clearly signaled too late. Although it was tested on February 28, a small hole was found in its float after the incident which may explain its late activation. If it would have signaled earlier, the incident would not have been prevented, but it could have prompted operators to sound the emergency alarm (BP, 2005).

From the day shift control room operator's view, all six barriers were trustworthy: the level indication and control, the start-up procedure, the splitter's derived high level alarm, the splitter's independent, hard-wired high level alarm, the high pressure alarm of the overhead line, and the blowdown drum's high level alarm. Although he did not adhere to the start-up procedure and ignored the high level alarm, he was fully confident of his violation and did probably not realise the extent of bypassing these two barriers. Classifying all six barriers equally with an RRL of 1, the RRRL from the operator's viewpoint was 100% (6/6 x 100%), which means a fully active barrier system with six barriers.

The investigation reports studied (BP, 2005; CSB, 2007; Hopkins, 2008) all indicated that the design of the splitter and blowdown drum did not meet current standards of best manufacturing practise. Figure 7.4 shows what a well designed (preventive) barrier system could look like to prevent the splitter's and blowdown drum's overfilling. The preventive barriers are described below:

- A level transmitter which indicates the splitter's level over its entire length, and which controls the drain of heavy raffinate from the splitter's bottom. The splitter's level should be indicated from the panels in the control room.
- A start-up procedure with clearly defined steps, among which the setting of 50% bottom level control on auto. The problem of the heater damage at low level should be solved to prevent the level control be put on manual.
- An alarm should be activated from the mass balance if there is a prolonged

imbalance between in and output which may lead to a significant level rise. The mass balance should be displayed on the panels in the control room so to support the operator to explain the level deviation from any imbalance of in and output.

- A signal derived from the level transmitter indicating to the control room operator that he is about to exceed the safe operating window.
- An independent, hardwired high level switch which will automatically shutdown the supply to the splitter.
- A hardwired high pressure switch which will automatically shutdown the splitter. The high pressure switch should be set at a pressure that it always acts prior to the safety relief valves.
- The blowdown drum should be equipped with a high level switch which automatically stops all its supplies.
- In addition, both the splitter and the blowdown drum should be provided with a level gauge which enables to check the level locally. As they may not be regarded as barriers, they are not drawn in Figure 7.4.

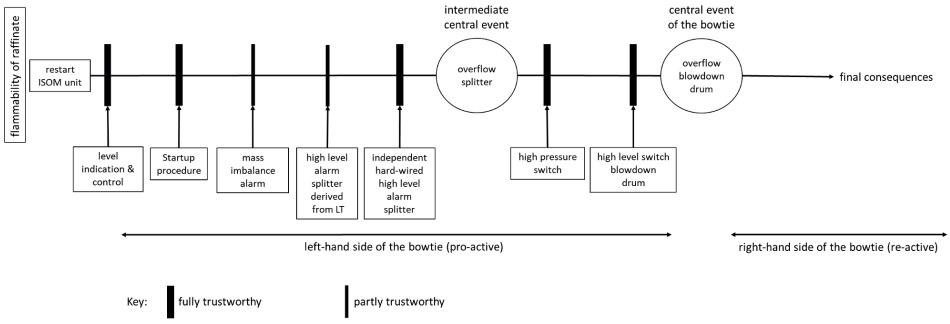

Fig. 7.4, a barrier system design of the splitter to protect against overfilling according to current standards

The barrier system design in Figure 7.4 is more operator independent than the design at the day of the incident. From a Layer of Protection Analysis (LOPA) view the level control is part of the basic process control system as an independent layer of protection (IPL). If designed properly it may account for a risk reduction of 10. The start-up procedure to be followed reduces the risk by 10 if it is a well written procedure describing all necessary steps, and provided its steps are simple and can be carried out without any time pressure. Both the alarm from mass balance calculation and the splitter's high level require a response from the control room operator. They would indicate to the operator that his start-up procedure is not successful at this point in time. It

is justifiable to give this joint barrier a risk reduction of 10. The high level switch may be designed as a SIL1 (RRL = 1) or SIL2 (RRL = 2) rated instrumental safeguard which comes down to a risk reduction of 10 or 100 respectively (CCPS, 2015). In short, the risk of overfilling of the splitter has reduced by 10,000 to 100,000 which comes down to an RRL of 4 to 5 respectively, from the uncontrolled process.

The high pressure switch and the high level switch in the blowdown drum can both reduce the risk by 10, which comes down to a further risk reduction of 100. With the suggested blowdown drum safety design, the total risk reduction of a liquid raffinate release from the stack would be reduced by 1 million to 10 million, meaning an RRL of 6 to 7 respectively. From this point, any failure, override or bypass of one of the barriers can be compared to its designed risk reduction and be calculated into an RRRL to verify if the risk is acceptable or not according to the company's own guidelines.

As concluded from Figure 7.2, the total risk reduction of the barrier system at the day of the incident was somewhere between 100 (RRL of 2) and 1000 (RRL of 3), whereas it should have been in the region of 1 (RRL of 6) to 10 million (RRL of 7), if properly designed according to current standards of best practise. The relative risk reduction expressed in Briggs logarithm (RRRL) on the day of the incident compared to a well safeguarded design according to current standards of best practise would have been somewhere between 29% (2/7 x 100%) at worst and 50% (3/6 x 100%) at best.

7.4.2 Organisational factors

Schmitz et al. (2021b) compiled nine organisational factors or management delivery systems (see legend of Figure 7.5). The relation of the organisational factors with the accident processes runs through the barrier systems. Figure 7.5 shows the organisational factors on the day of the incident, which relate to Figure 7.2. The organisational factors strongly influence the quality or trustworthiness of the barriers and are indicated in the box under each of the barriers. In addition, malfunctioning organisational factors can also promote accident processes in a more general way, not through the barrier systems. They can be considered as "performance influencing factors" or "error producing conditions", and may create latent, dangerous conditions if not properly managed. Reason (1990) referred to them as 'resident pathogens', whose effects are not immediately apparent, but can both promote unsafe acts and weaken defence mechanisms. This group of organisational factors is indicated in the box on the left-hand side in Figure 7.5 which directly points to the accident process or scenario.

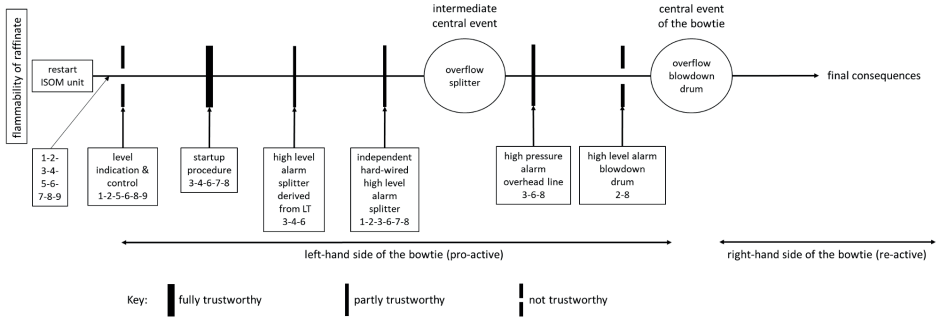

Fig. 7.5, the organisational factors on the day of the incident
(1. Maintenance; 2. Inspection and testing; 3. Training & competence; 4. Management; 5. Procedures; 6. Plant documentation; 7. Communication & coordination; 8. Plant design & operations; 9. Hardware integrity)

The investigation reports provide an overwhelming amount of evidence on what went wrong at BP's refinery site in Texas City. In Table 7.1 relevant evidence has been included as flaws for each of the nine organisational factors which had an influence on the accident process (as indicated in the box on the left-hand side of Figure 7.5). While some of the evidence could also be attributed to some barriers, they are more likely to be general findings which can be related to common flaws or shortcomings. It is obvious that these flaws have an influence on more accident processes than just the one of March 23, 2005.

Table 7.1, Organisational factors creating latent, dangerous conditions

Organisational factors	General flaws in the organisational factors
Maintenance	• Maintenance details were poorly documented (e.g. Instrumentation calibration).
Inspection & testing	• The start-up was to occur even though technicians had not had the time to carry out all instrumentation checks.
Training & competence	• Process trouble shooting was given in 2000 but no refresher training since. • Records showed incomplete training, little verification that all required training was occurring, operator's theoretical knowledge was not complete and rarely witnessed. • Training records for ISOM personnel regarding process safety training requirements reveals some gaps in training delivery and topics. • There was no training on how to handle abnormal situations. • The trailer siting and the traffic control policy are examples of a lack of risk awareness. • Safety measures were primarily focussed on lagging indicators for personal safety. • There was an inability to learn from previous start-up failures as they were not investigated.

Table 7.1, continued

Organisational factors	General flaws in the organisational factors
Management	• There was no fatigue prevention policy as operators worked long shifts for many days in a row. • Many steps of the start-up procedure were not conducted or signed off. • Supervisors and superintendents did not verify that the procedures were available and correct or being followed. • A high level of risk was routinely tolerated by both management and the work force. • The organisation was overly complex and changing. • Inadequate visible leadership. • Inadequate enforcement of policies, standards and procedures. • Unclear accountabilities. • The working relationships between leadership and workers, and employees and contractors were poor. • The control room operator was responsible for a total of three different process units which is more than a full load for one person.
Procedures	• Preparatory activities including a pre start-up review were not conducted. • Changes to the start-up procedures and training actions were not closed although indicated.
Plant documentation	• The start-up procedure was not fully updated. • There's no single database or register of safety critical equipment.
Communication & coordination	• Shift relief between the outgoing night shift and oncoming day shift outside operators did not occur on the ISOM unit and appears to be brief and inadequate. • The HSSE department was not notified 14 days prior to start-up. • Poor handover procedures. • Hundreds of contractors in the Ultracracker TA were unaware of the start-up. • The operator's logbook was brief and uninformative and there was no face to face contact between in and outgoing operators. • The incident reporting systems to highlight exceedances was not operational. • There is no reporting of process upsets from previous start-ups.
Plant design & operations	• The What-If analysis technique is not robust enough to consider all modes of operation or process upset scenarios. • Several aspects of the control room affect human factors: noisy, poor lighting. • Various authorities have recommended automatic shutdown devices to prevent overfilling. • The safeguarding system heavily relied on procedures initiated by alarms.
Hardware integrity	• Various pieces of equipment were malfunctioning, but not rectified before start-up.

Table 7.2 highlights the organisational factors which are of relevance to each of the preventive barriers. Evidence from the investigation reports has been collected and allocated to a barrier and its relevant organisational factor. The evidence demonstrates not only the flaws of the organisational factor but also shows the decline of the barrier's quality.

Table 7.2, Organisational factors for each preventive barrier, on the day of the incident

Organisational factors	Flaws in the organisational factors of each preventive barrier
	Level indication and control
Maintenance	• The splitter's level gauge had a build-up of residue and had been effectively useless for years.
Inspection & testing	• The level transmitter was not calibrated correctly. • The calibration records of the splitter displacer type level indicator were difficult to find.
Procedures	• The MoC once missed a change of the renewed specific gravity.
Plant documentation	• There was no updated datasheet to support the calibration.
Plant design & operations	• The level transmitter was not designed to show levels greater than 100% and was not reliable if both impulse lines are submerged. • Safe operating limits had not been defined for the liquid level of the splitter.
Hardware integrity	• The splitter's level gauge had a build-up of residue and had been effectively useless for years.
	Start-up procedure
Training & competence	• The risk of overfilling was unknown. • The training did not specifically address the risk of overfilling a tower to the point of liquid overflow, and the appropriate mitigation actions required. • It is unknown but likely that calculating a mass balance was not trained.
Management	• Checks prior to start-up were signed off as completed even though they were not. • The shift supervisor did not enforce, and the operators did not follow the start-up procedure. • The start-up was conducted across two shifts which is not well planned. • When the day shift supervisor left the site, it was not clear who should then take command. • Both the superintendent and day shift supervisor were absent during the start-up. The acting superintendent did not visit the ISOM to review progress with the operators. • The splitter start-up procedure was not reviewed with the crew. • The control room operator was responsible for three different process units.
Plant documentation	• The hazards related to overfilling were not mentioned in the start-up procedure and PHA's. • The start-up procedure was not fully up to date. • Making a mass balance was not prescribed and described in the start-up procedure.
Communication & coordination	• The night shift control room operator in the main control room was not involved in establishing levels in splitter and packing the reboiler circulation from the satellite control board. • The night shift operator left before the end of his shift and did not leave detailed information. • The start-up was not mentioned at the shift director's morning meeting. • The day shift supervisor did not inform adjacent process units or others in the immediate vicinity of the ISOM unit of the splitters start-up. • During the management meeting it was decided not to proceed because the heavy raffinate tanks were full. The operators were not told of this decision and went ahead with the start-up. • The control room operator believed that he had been instructed not to open the heavy liquid outflow valve because the storage tanks were full. The outside operators believed the light raffinate storage was full and closed its corresponding output valve. • Communication between the outside operators with the day shift control room operator was not complete or effective.
Plant design & operations	• The control room displays did not highlight the imbalance of in and output. • It was not easy for the control room operator to conduct a mass balance as the in- and output data were displayed on different screens.
	High level alarm splitter
Training & competence	• The alarm remained in alarm mode throughout but was ignored, which proves that the risk of overfilling was unknown.

Table 7.2, continued

Organisational factors	Flaws in the organisational factors of each preventive barrier
Management	• A lack of supervision allowed the alarm to be ignored.
Plant documentation	• The relevance of the alarm was not documented in the start-up procedure.
	Hard-wired high level alarm splitter
Maintenance	• The alarm required preventive maintenance as it did not work in 2003 for unknown reason.
Inspection & testing	• As it was not inspected prior to the start-up, its inspection regime may be questioned.
Training & competence	• The relevance of the alarm and its setpoint was unknown, which proves that the risk of overfilling was unknown.
Plant documentation	• The relevance of the alarm was not documented in the start-up procedure.
Communication & coordination	• The night shift did not report the faulty alarm to the day shift, verbally or in the shift log.
Plant design & operations	• This hardwired alarm was not classified as safety critical and should have automatically shutdown the splitter.
	High pressure alarm of the overhead line
Training & competence	• The cause of activation of the high pressure alarm due to overfilling the tower was unknown. • The change of the derated safety relief valves was not trained.
Plant documentation	• There was no reference of the cause of overpressurisation due to overfilling of the splitter in the start-up procedure and PHA's.
Plant design & operations	• This alarm was not classified as safety critical and should have automatically shutdown the splitter. • Locating the safety relief valves at the top of the splitter is inherently safer than near the condensing inlet.
	High level alarm of the blowdown drum
Inspection & testing	• Although a test was done on March 20, 2005, it did not sound in time.
Plant design & operations	• This hardwired alarm was not classified as safety critical and should have automatically shutdown the ISOM unit as there was not enough time to respond adequately. • The blowdown drum was not converted to an inherently safe relief system (a flare).

7

7.5 DISCUSSION

The information in this chapter came from the three investigation reports as well as from Hopkins' book "Failure to learn". BP's refinery site at Texas City has never been visited nor has anyone involved in the incident or their investigators been interviewed. As a result, this chapter may not contain all the facts that came to light, and in addition, the facts may not have been reported in the detail in which they were investigated. However, this does not detract from the final conclusions.

Some matters contributed to the accident in such a way that if the matter had been otherwise, the accident would not have happened. Clearly, an inherently safer design using a flare would have eliminated this accident scenario in the first place. However, it should be noted that the overflow of the blowdown drum leading to a raffinate

release from its stack is regarded as the central event. This validation only considers the accident process prior to the blowdown drum's overflow. The decision not to install an inherently safer design using a flare is not in the scope of this validation. Other matters do fall within the scope of this validation, such as a high level switch or cut-out device that could have stopped operators from overfilling the column, as it would certainly have prevented the accident. In other cases, such as fatigue, the same level of certainty does not apply because when the operators would have been less fatigued, the accident would most likely still have happened (Hopkins, 2008). Preparatory activities should guarantee that the installation is sound and fit for purpose. In addition, the crew needs to be well informed, trained, and capable of starting up safely. Regarding the preparatory activities it is questionable if this procedure would have stopped the scenario from overfilling. Not conducting the preparatory activities contributed to the incident, but that does not necessarily mean that conducting them would have stopped the development of the scenario. In this respect, preparatory activities should be disregarded as a barrier or independent protection layer.

One could argue about the categorisation of some of the evidence. Not identifying the cause of activation of the high pressure alarm due to overfilling the tower in the PHA's, is most likely due to a lack of knowledge whereas there is also a gap in the plant documentation. Either way, flaws like this should have been discovered during an audit or peer review.

Many of the deficiencies were common occurrences rather than isolated events (Saleh et al., 2014). Shortcomings that appeared to be structural and of influence on the accident process in a more general way by promoting errors and creating latent, dangerous conditions, have not been assigned to an organisational factor of a barrier but to an organisational factor of the accident process itself.

Both Baker (2007) and Hopkins (2008) investigated BP's safety culture. Clearly, a defective process safety culture impacts the process safety performance. Some management decisions taken at a higher level, such as decentralizing the organisational structure, cost cutting, a wrong focus in renumeration systems and a lack of attention from top leaders to safety may harm process safety on the long term. This chapter has not included indicators at this level.

The risk reduction of the individual preventive barriers at scenario level has been assessed using standardized values given by CCPS (2015). Their risk reduction values may be questioned, but more important is the concept of the loss of risk reduction caused by the degraded quality of the barrier system. In other words, the concept of the risk reduction should not be seen as an absolute decline but as a relative difference

from how it should be according the initial design. The relative risk reduction should initiate further action if below the company's threshold value.

The authors are unfamiliar with BP's risk assessments and auditing system and therefore unable to make a comparison with the model presented in this chapter. Clearly, the lack of BP's follow-up is a cultural aspect, which could have been discovered looking at both the barrier system and organisational factors as demonstrated in this chapter. The presented model is considered comprehensive, and able to define targeted action. The use of indicators should ensure timely action if addressed to the right organisational levels.

Although this validation is based on an incident from the petrochemical industry, and not from an ammonia plant or any other plant in the Fertilizer's industry, organisational factors are *a priori* not sector specific. This is confirmed by the investigation by the Dutch Safety Board (OVV) into a number of process safety related incidents at various site users of the Chemelot site in Geleen, The Netherlands (OVV, 2018). In addition, this validation considers an incident in retrospective, whereas OCI Nitrogen's aim is to view incidents prospectively and to stop major accident processes prematurely. However, this chapter shows that the barrier management approach can be used in a proactive way, regardless of the type of company within the (petro)chemical industry.

7.6 CONCLUSIONS

This chapter sheds new light on the monitoring of accident processes and their investigations. The BP Texas City refinery incident has been looked at from two different time perspectives. Firstly, the concept of the relative risk reduction looks at the barrier status on the day of the incident, and secondly, the organisational factors look at (latent) system failures as part of the on-site culture which may have been present for many years. Both the bowties including the preventive barrier indicators and the allocation of the investigation findings to the nine organisational factors show that the Texas City refinery incident could undoubtedly have been avoided if adequate barrier management would have been used, based on solid bowtie thinking linked to preventive barrier indicators and organisational factors. Even during the accident process supervisors and colleagues could have intervened as the overflow of the tower required a mass imbalance, high temperatures, and several hours of operator inattention. This accident would have happened sooner or later as the operators were blind to what happened in the splitter as two critical parameters were not measured: the liquid level and the net raffinate flow. Over the years, the BP Texas City refinery crew lost its sensitivity to danger, not only by the obsolete design, through which a certain

level of equipment malfunction came to be accepted as normal. But also because of BP's weak safety culture, from poor safety practises to inadequate procedures, and a repeated pattern of safety violation, which played a lurking role as accident pathogens. Accident scenario analysis with probability updating is the key to dynamic risk assessments. Bayesian Network (BN) is an alternative technique with ample potential for application in risk assessments (Khakzad et al., 2011, 2013). The use of BN will continuously reduce data uncertainty of the bowtie when a new set of accident related information becomes available. It provides the accident scenarios with real time analysis, which leads to an up-to-date picture of the process safety performance, and a better understanding of the current and future accident processes. Further research is needed to see whether this approach can improve the prediction of major hazard accidents.

7.7 REFERENCES

Aven, T., Sklet, S. & Vinnem, J.E. (2006). Barrier and operational risk analysis of hydrocarbon releases (BORA-Release), Part I. Method description. *Journal of Hazardous Materials, A137*, 681-691. http://dx.doi.org/10.1016/j.jhazmat.2006.03.027.

Baker, J. (2007). *The report of the BP U.S. refineries independent safety review panel*. Retrieved from https://www.csb.gov/assets/1/20/baker_panel_report1.pdf?13842.

Britisch Petrol (BP). (2005). *Fatal accident investigation report. Isomerization Unit Explosion* (Final Report). Retrieved from http://cip.management.dal.ca/publications/final_report.pdf.

Centre for Chemical Process Safety (CCPS). (2015). *Guidelines for initiating events and independent protection layers in layer of protection analysis*. New York, U.S.: Wiley.

Hopkins, A. (2008). *Failure to Learn*. Sydney, Australia: CCH Australia Ltd.

Kalantarnia, M., Khan, F. & Hawboldt, K. (2010). Modelling of BP Texas City refinery accident using dynamic risk assessment approach. *Process Safety and Environmental Protection, 88*, 191-199. http://dx.doi.org/10.1016/j.psep.2010.01.004.

Kang, J. Zhang, J. & Gao, J. (2016). Analysis of the safety barrier function: Accidents caused by the failure of safety barriers and quantitative evaluation of their performance. *Journal of Loss Prevention in the Process Industries, 43*, 361-371. http://dx.doi.org/10.1016/j.jlp.2016.06.010.

Khakzad, N., Khan, F., & Amyotte, P. (2011). Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. *Reliability Engineering and System Safety, 96*, 925-932. https://doi.org/10.1016/j.ress.2011.03.012.

Khakzad, N., Khan, F. & Amyotte, P. (2012). Dynamic risk analysis using bow-tie approach. *Reliability Engineering and System Safety, 104*, 36-44. http://dx.doi.org/10.1016/j.ress.2012.04.003.

Khakzad, N., Khan, F., & Amyotte, P. (2013). Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. *Process Safety and Environmental Protection, 91*, 46-53. http://dx.doi.org/10.1016/j.psep.2012.01.005.

Khakzad, N., Khakzad, S. & Khan, F. (2014). Probabilistic risk assessment of major accidents: application to offshore blowouts in the Gulf of Mexico. *Natural Hazards, 74*, 1759-1771. http://dx.doi.org/10.1007/s11069-014-1271-8.

Khakzad, N., Khan, F. & Amyotte, P. (2015). Major Accidents (Gray Swans) Likelihood Modeling Using Accident Precursors and Approximate Reasoning. *Risk Analysis, Vol. 35*, No. 7, 1336-1347. http://dx.doi.org/10.1111/risa.12337.

Kirwan, B. (1994). *A Guide to Practical Human Reliability Assessment*. Boca Raton, U.S.: CRC Press.

Meel, A. & Seider, W.D. (2006). Plant-specific dynamic failure assessment using Bayesian theory. *Chemical Engineering Science, 61*, 7036-7056. http://dx.doi.org/10.1016/j.ces.2006.07.007.

Meel, A., O'Neill, L.M., Levin, J.H., Seider, W.D., Oktem, U. & Keren, N. (2007). Operational risk assessment of chemical industries by exploiting accident databases. *Journal of Loss Prevention in the Process Industries, 20*, 113-127. http://dx.doi.org/10.1016/j.jlp.2006.10.003.

Onderzoeksraad voor de Veiligheid (OVV). (2018). *Chemie in samenwerking*. Retrieved from https://www.onderzoeksraad.nl/nl/page/4707/chemie-in-samenwerking---veiligheid-op-het-industriecomplex-chemelot.

Paltrinieri, N., Khan, F. & Cozzani, V. (2015). Coupling of advanced techniques for dynamic risk management. *Journal of Risk Research, Vol. 18*, No. 7, 910-930. http://dx.doi.org/10.1080/13669877.2014.919515.

Rathnayaka, S., Khan, F. & Amyotte, P. (2011). SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description. *Process Safety and Environmental Protection, 89*, 151-164. http://dx.doi.org/10.1016/j.psep.2011.01.002.

Reason, J. (1990). *Human error*. Cambridge, UK: University Press.

Saleh, J., Haga, R., Favarò, F. & Bakolas, E. (2014). Texas City refinery accident: Case study in breakdown of defense-in-depth and violation of the safety-diagnosability principle in design. *Engineering Failure Analysis, 36*, 121-133. http://dx.doi.org/10.1016/j.engfailanal.2013.09.014.

Schmitz, P., Swuste, P., Reniers, G. & Nunen van, K. (2020). Mechanical integrity of process installations: Barrier alarm management based on bowties. *Process Safety and Environmental Protection, 138*, 139-147. https://doi.org/10.1016/j.psep.2020.03.009.

Schmitz, P., Swuste, P., Reniers, G. & Nunen van, K. (2021a). Predicting major accidents in the process industry

based on the barrier status at scenario level: a practical approach. *Journal of Loss Prevention in the Process Industries, 71*, 104519. https://doi.org/10.1016/j.jlp.2021.104519.

Schmitz, P., Reniers, G., Swuste, P. & Nunen van, K. (2021b). Predicting major hazard accidents in the process industry based on organizational factors: a practical, qualitative approach. *Process Safety and Environmental Protection, 148*, 1268-1278. https://doi.org/10.1016/j.psep.2021.02.040.

Skogdalen, J.E. & Vinnem, J.E. (2012). Combining precursor incidents investigations and QRA in oil and gas industry. *Reliability Engineering and System Safety, 101*, 48-58. http://dx.doi.org/10.1016/j.ress.2011.12.009.

Swuste, P. (2010). Book review, Failure to Learn, the BP Texas City Refinery disaster, Andrew Hopkins. *Safety Science, 48*, 279-280. http://dx.doi.org/10.1016/j.ssci.2009.09.001.

U.S. Chemical Safety and Hazard Investigation Board (CSB). (2007). *Investigation report, Refinery Explosion and Fire BP Texas City*. Retrieved from https://www.csb.gov/bp-america-refinery-explosion/.

Vinnem, J.E., Aven, T., Husebø, T., Seljelid, J. & Tveit, O.J. (2005). Major hazard risk indicators for monitoring of trends in the Norwegian offshore petroleum sector. *Reliability Engineering and System Safety, 91*, 778-791. http://dx.doi.org/10.1016/j.ress.2005.07.004.

Vinnem, J.E., Seljelid, J., Haugen, S., Sklet, S. & Aven, T. (2009). Generalized methodology for operational risk analysis of offshore installations. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, Vol. 223*, Issue 1, 87-97. http://dx.doi.org/10.1243/1748006XJRR109.

Yang, M. Khan, F. & Ley, L. (2013). Precursor-based hierarchical Bayesian approach for rare event frequency estimation: A case of oil spill accidents. *Process Safety and Environment Protection, 91*, 333-342. http://dx.doi.org/10.1016/j.psep.2012.07.006.

8

CONCLUSIONS

8.1 CONCLUSIONS AND DISCUSSION

The main research question "To what extent can major hazard accidents in the process industry be prevented?" has been answered in a few steps, following the sub-questions. By assessing the quality of the barrier systems and considering the organisational factors or management delivery systems, a solid basis has been laid for an approach that can increase the likelihood of preventing major hazard accidents in the process industry.

In one of the first steps of this research, it was investigated what major process safety incidents are. In other words: which equipment can give rise to the most severe consequences in case of failure. The calculations show that the ammonia production process comprises several intrinsic hazards related to the process parameters such as pressure and temperature, and to the presence of steam, flammable gas, and ammonia. A release of a hazardous substance can lead to burns, internal injury or poisoning from exposure to heat radiation, flames, overpressure or toxic concentration respectively. In the front end of the ammonia production process, loss of containment scenarios may lead to heat radiation from jet fires, flame contact from flash fires or to overpressure from explosions due to the presence of flammable components. In the back end of this process, ammonia is also present, which when released may lead to high toxic concentration levels resulting in poisoning. It was concluded that the equipment in the highest pressure part of the ammonia process and the equipment with liquid ammonia, meaning from the syngas compressor to the ammonia separation vessel, the ammonia product pumps and the buffer tanks, are the most dangerous ones. This equipment has the potential to cause the largest adverse health impact on humans in the event of failure. In general, it can be concluded that when pressure, temperature, and mass will increase, the effects (and hence the adverse health impact on humans) become larger. In addition, liquid, 'hot' ammonia is a severe threat as it evaporates quickly at release and forms a large toxic cloud.

The subsequent study investigated how the likelihood of major process safety incidents can be monitored over time. The answer to this question was given using scenarios caused by mechanical failure of static process equipment. In response, the primary focus was on (very) probable scenarios, which either have already occurred at OCI, or are known from the international literature on accidents at ammonia plants. These scenarios have been visualised using bowties after which a risk-based approach has been developed providing information on the number, and quality of necessary barriers to reduce the risk to an acceptable level. Based on operating parameters like pressure, temperature, and flow, it is deemed possible to monitor the development of these scenarios. Early warnings derived from operating parameters can serve as an

indicator to show the development of the scenarios.

In the following two studies the extent has been investigated to which indicators provide information on the likelihood of the central event. In the first sub-study, indicators have been derived from the status of the barrier system. An indicator, referred to as 'preventive barrier indicator', has been developed which has proven to monitor the level of safety, and enable the operators to decide when, where, and which action is necessary. The preventive barrier indicator shows the development and possibility/ likelihood of a certain scenario, which is not an absolute value, but rather an indication of the change in the *status quo* that should initiate further action (or not).

In the second sub-study the aim was to investigate organisational factors or management delivery systems as they indirectly impact accident processes through their strong influence on the barrier systems' quality or trustworthiness. Qualitative and quantitative monitoring of organisational factors can display their operation and efficiency. A list of nine organisational factors or management delivery systems has been compiled which are applicable for OCI Nitrogen, but also for the process industry as a whole. Audits and peer reviews are the right tools to assess the efficiency of organisational factors. These tools ensure that major accident processes obtain the attention they deserve, and that the necessary actions are taken at the right management level. A quantitative assessment has been conducted for one of the management delivery systems as an example of management indicators. But as the example shows, determining threshold values for which action is required, is an intricate matter because the influence on the accident processes is difficult to determine. Once threshold values have been set, (management) indicators can be developed, which are measured at a certain frequency of, for example, once a month or once a quarter. The BP Texas City refinery accident of 2005 has been taken as an example to validate the model. The bowtie metaphor is used to visually present the BP Texas City refinery accident, showing the barrier system from three different perspectives. The risk reductions of these different views have been calculated and compared to their original design. In addition, evidence and findings from the BP and US Chemical Safety Board investigations have been categorised as flaws and allocated to the (nine) organisational factors. The validation sheds new light on the monitoring of accident processes and the barrier management to control them, and demonstrates that the BP Texas City refinery accident could have been foreseen using preventive barrier indicators and monitoring organisational factors.

The literature review at the start of this doctoral research (Swuste et al., 2016) shows the latest developments and uses regarding process safety performance indicators and comprises an inventory of their definitions in both scientific and professional

literature. In conjunction with the validation, it has been demonstrated that the design of process safety indicators from this model is practically feasible and sound, which refers to the first sub-question.

This research is innovative in the sense that the likelihood and development of major process-related accidents are monitored before the consequences become apparent. This is done on the basis of a combination of three indicators: 1. Early warnings based on process parameters such as pressure and temperature that show the initiation of an accident process, 2. Preventive barrier indicators that indicate the quality of the barrier system, but also the development of the scenario once the scenario has been initiated, and 3. Management indicators that provide information about the effectiveness of the organisational factors. In conclusion, with this research, process safety is one step closer to a much-needed theory.

8.2 RECOMMENDATIONS

This doctoral research concludes that barrier performance monitoring, using preventive barrier indicators and an audit technique focussed on organisational factors, is a very promising possible way forward to prevent major hazard accidents in the process industry. When a company aims to set up an operational barrier management to measure their process safety performance, it requires a step by step approach. These steps are outlined below in which the experiences from the investigation of the ammonia plants of OCI Nitrogen have been included.

The question of what major process safety incidents are, is strongly linked to the most dangerous process equipment. The consequences from a loss of containment should be calculated with a well-defined set of starting points. One of these starting points is the response time of five minutes of the control room operator, as stated in section 3.4. Although a doubling of the response time would not significantly change the final results of an ammonia plant, a much longer response time will. In emerging accidents (control room) operators may not always act rationally. They may be keeping the production process running since stopping it may lead to adverse operational issues. They may not (timely) detect or recognise the emerging risk, or have insufficient information, training, unclear procedures, or other urgent matters from an alarm overload. When a swift intervention is delayed, the seriousness of the accident could be significantly increased.

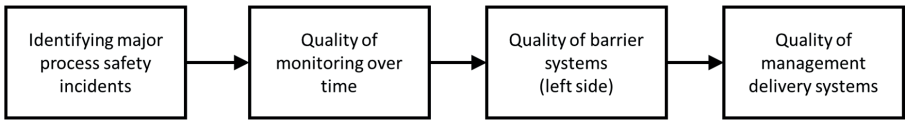

Figure 8.1, present model for prediction of incidents

Figure 8.1 shows the steps of the present model of this thesis. For toxic scenarios it should be considered to extend the model as indicated in Figure 8.2. The extended model has two feedback loops from which the response time can be determined more accurately, which may affect the relative ranking of the process equipment. In addition to the barriers on the left-hand side, also some of the right-hand side barriers following the central event, like gas detection monitoring, should be looked at for their quality or trustworthiness. And with that, its maintenance, inspection, testing, training, and procedures as supporting organisational factors should be assessed. This iteration will not only make the ranking of toxic scenarios more accurate, but will also lead to more severe consequences and a higher ranking of process equipment containing (acute) toxic substances.

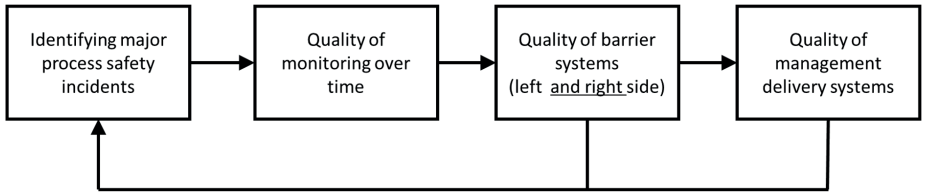

Figure 8.2, extended model for prediction of incidents

The method described in chapter 3 provides a relative ranking of process equipment which leads to an understanding of the relative position of the equipment with respect to their dangerousness. The effect calculation results can not only be used for risk mapping of an entire chemical plant, but also enables the plant to focus on the most dangerous process equipment only.

When the most dangerous process equipment have been selected, the next step is to identify the scenarios leading to their failure. Clearly, the focus for barrier management should be on the most credible scenarios. The combination of the most dangerous process equipment and the most credible scenarios results in a set of major process safety scenarios, meaning scenarios which are most likely to occur and have the largest

adverse health effects at equipment failure. Deviating process conditions during start-up and shutdown should also be carefully assessed as they may be very likely to occur. Once the most credible scenarios have been identified, they should be visualised in bowties including their preventive barriers.

Process hazards assessments (PHAs) are quite common in the process industry, if not already required by the regulator. They form the basis of what can go wrong as a result of process upsets, misoperation, a loss of mechanical integrity, or inadequate maintenance, to name just a few. PHAs are mostly performed by plant own personnel, sometimes chaired by an independent external consultant. Failure scenarios are generated from validated methods, and complemented with near incidents and accidents from the plant's history. To get the full picture of what can go wrong, it is recommended to conduct a thorough literature research to obtain an overview of all potential major hazard accidents from the chemical process concerned.

Loss of mechanical integrity and mechanical failure mechanisms are often not considered in PHAs. Material degradation and corrosion mechanisms are a concern in high pressure – high temperature equipment and pipework, which becomes even worse when hydrogen is involved. Mechanical failure mechanisms related to static equipment can occur at detail level such as in a dissimilar weld or a small part made from a deviating material. It is therefore important to know how an equipment is constructed, what materials it consists of and how it is made (e.g. post weld heat treatment). In the end, the devil is in the detail.

In some static equipment, barriers are installed or constructed which are not always readily recognised as such. Examples include refractory (brickwork), metal sleeves with insulation, and internal lining which are installed to protect the wall from a high temperature or corrosive chemicals. These provisions can be seen as inseparable parts and may therefore not be recognized as barriers, while they can fail. It is recommended to assign a trustworthiness to these barriers when the risk has been established, which will result in a regular inspection to check their quality.

Early warnings provide information on the current development and therefore on the likelihood of major process safety incidents over time. They are based on process parameters like pressure and temperature, and should be installed to warn against the above latent material degradation and corrosion mechanisms. In addition, early warnings can be used to do an inspection to monitor the mechanical failure scenario. Considering the shift from breakdown maintenance to preventive and predictive maintenance and risk-based inspection (RBI), inspections based on early warnings could also be a new step in the field of maintenance efficiency.

When deriving indicators from preventive barriers, several points must be taken into account. Once the preventive barriers have been identified, their quality and activation should be monitored. The aspect of quality comprises both reliability/availability and effectivity. An inspection and/or test must show whether a barrier is capable of achieving the designed target within a specified time. After all, a barrier can be subject to wear or degradation and this should be reflected in the test procedure. In other words, is the barrier still sound? When a barrier has returned to service after maintenance, inspection and testing, and some doubts about its trustworthiness still exist, the barrier status should be classified as 'possibly not trustworthy', and vigilance is required.

Mechanical safeguards such as safety valves or check valves are rarely maintained, inspected and tested, for example once every 4, 6 or even 12 years. These barriers also do not provide feedback if they are defective. This means that the barrier status of mechanical safeguards will not change for a long time. If there is a suspicion of malfunction during operation, which cannot be immediately verified or resolved, and for which corrective maintenance is planned, the barrier status could be set manually to 'possibly not trustworthy' or 'not trustworthy'.

A scenario only develops when it has started. The chance of a central event does not only depend on the barrier status, but also on the chance that the 'initiating event' occurs. Although this research focusses on the barrier system, it could be extended with indicators on the initiating events, such as failure of (active) controls. This would provide a solution for barrier systems that consist of few barriers only.

If a barrier consists of an alarm, an operating procedure, and an operator intervention, the trustworthiness is hard to establish. Has the operator seen the alarm and understood the problem? Does he/she know how to act? Is he/she not too busy with other tasks? It is recommended to test the knowledge and skills of operators in practice, and not through computer-based training. This counts particularly for operating procedures which are safety critical.

Proper and timely maintenance, inspection and testing may not always guarantee the trustworthiness of barriers. Clearly, maintenance should be performed according to the manufacturer's guidelines and by competent personnel, but that does not mean a 100% safe barrier system. It is recommended to set up a registration system for safety critical equipment that records the findings of its maintenance, inspection and testing. The records should then be regularly checked so to establish whether the maintenance, inspection and testing regime should be adjusted.

Qualitative information of organisational factors or management delivery systems can be obtained from audits or peer reviews that are conducted once every three to four years. They can also be partly monitored by self-assessments on a more frequent basis, say annually. Quantitative monitoring on a more frequent basis should only be started when audits or peer reviews do not reveal major shortcomings or findings.

Organisational factors or management delivery systems are non-technical in nature and must be regarded as work processes and procedures in which human actions and decision-making predominate. Only when an organisation has the right questioning attitude, it will be able to find the mechanisms obstructing their work processes and procedures. Conducting an audit or peer review requires more than just asking questions. Selecting the right auditors will substantially improve the audit's outcome.

8.3 DIFFICULTIES, SOLUTIONS AND LIMITATIONS OF THE PHD-RESEARCH

The calculation of adverse health effects on humans is based on many assumptions. The starting points were chosen by the authors based on scientific literature and their practical experience with the calculation model. It should be noted that the outcome is a relative ranking of equipment, which means that it does not claim to submit absolute results, but it leads to an understanding of the relative position of equipment with respect to their dangerousness. In this way, the ranking helps to set priorities in appointing the major hazard scenarios.

Hazard identification takes place during several safety studies but is strongly dependent on knowledge and experience of the participants. Often only hazards are considered that a company has been confronted with in the past, or that follow from legal obligations, such as a Seveso audit or an environmental permit. Hazards and scenarios that have occurred within the international sector are rarely considered. In ammonia plants, many (mechanical) failure scenarios are susceptible to start-up and shut-down situations, which are often not considered in the design. Additionally, ageing of equipment has revealed some completely unknown failure mechanisms in the ammonia plants, also called 'black swans'. And finally, human mistakes causing poor design, incorrect assembly or repair, and incomplete or inadequate inspections may (unexpectedly) initiate or contribute to a major hazard accident. It is therefore important to regularly update process safety related scenarios using the latest knowledge and experience within the ammonia industry.

Some types of barriers consist of barrier elements in which humans detect, diagnose

and/or act. These barrier types require enhanced attention and a different assessment as their trustworthiness is more difficult to estimate than when they are only technical. In addition, organisational factors or management delivery systems are non-technical in nature and must be regarded as work processes and procedures in which human actions and decision-making predominate. Humans are partly influenced by the environment in which they work and by the systems with which they work, in the course of which they will always try and find the easiest way, even if it is more dangerous. It cannot be assumed that humans always act rationally (Rasmussen, 1990; Le Coze, 2015). Only when an organisation has the right questioning attitude it will be able to find the mechanisms obstructing their work processes and procedures, and to assess the human barrier's trustworthiness.

Haddon was, in 1963, among the first to think about barriers in a systematic way using the Hazard-Barrier-Target model (Haddon, 1963). Multiple barriers are put in place to keep hazards (energy sources) from impacting a target, e.g. a person or asset. This concept has formed the basis for the Swiss Cheese model, Tripod, and for the bowtie metaphor. Although bowties are used to visualise the scenarios in this thesis, they provide a multiple linear presentation of an accident process in which the barrier system is shown sequentially, and extra-organisational factors are left out. Investigations of major hazard accidents in the process industry, as part of the high-tech – high-hazard sector, demonstrate that those accidents are often much too complex to be illustrated in a bowtie, Tripod, or Swiss cheese. Bowties are like other epidemiological accident models inadequate to capture the dynamics and nonlinear interactions between system components in complex socio-technical systems, and the influence of outside-company factors on accident processes. These interactions and events are hard to understand, and it is not sufficient to comprehend accident causation by employing the standard techniques in safety engineering alone (Qureshi, 2007). However, bowties, as a visualisation of these accident processes, can be readily understood as they show the barrier system which should be treated as the basis of safety, meaning the measures to prevent the accident from occurring.

The investigation reports of the BP Texas City refinery accident are readily available and provide an overwhelming amount of evidence on what went wrong at BP's refinery site in Texas City on March 23, 2005. However, there are two comments that can be made against this choice: 1. The validation of the model is based on an accident from the petrochemical industry and not from an ammonia plant, and 2. The validation considers an accident in retrospective. Nonetheless, firstly, organisational factors are *a priori* not sector specific, which is confirmed by the investigation by the Dutch Safety Board (OVV) into several process safety related incidents at the Chemelot site (OVV, 2018). Secondly, it is demonstrated that the barrier management approach can be

used in a proactive way, regardless of the type of company within the process industry. Two examples have been described in chapter 4 in which early warnings indicate that the integrity operating window is being exceeded. From chapter 5 it becomes clear that delayed maintenance or (partly) overriding of the barrier system increases the chance of a failure scenario. And lastly as described in chapter 6, monitoring the organisational factors could indicate flaws in the work processes eventually leading to decreased barrier quality. This approach of monitoring the early warnings, the barriers' quality and activation, and organisational factors provides relevant information for the plant management team, the plant staff and engineers (like the process control and asset engineers) as well as for the control room operators. All those informed will be able to conduct targeted actions at various levels of the operational organisation based on the increased risk. Procedures should ensure the right action, at the right moment and with the right urgency. However, decision making is difficult to predict as other issues or information may have to be considered which could be of influence on the final decision.

8.4 FUTURE WORK

The complexity of systems and the environments in which they operate, means process safety is not straightforward or linear, but a complex web of relationships and behaviours between humans, technology, and their environment (Underwood and Waterson, in Grant et al., 2018). Traditional accident modelling approaches, like Hazop, the Swiss Cheese Model, Tripod, and the bowtie metaphor (fault and event tree analysis), are not adequate to analyse accidents that occur in modern socio-technical systems, where accident causation is not the result of an individual component failure or human error (Qureshi, 2007). Traditional accident models are linear, or epidemiological and focus on intra-organisational factors (Van Schaardenburgh-Verhoeve, 2008). Instead, the prediction of accidents, or systems failures, should be driven by an appropriate accident causation model. While many accident causation models exist, with useful elements relating to understanding accident causation, there is no universally accepted model. In addition, little literature was found where dominant models were tested in a predictive context (Grant et al., 2018), although some contemporary accident causation models are tested, such as Rasmussen's framework and Leveson's STAMP model (Qureshi, 2007; Filho et al., 2019). Such systemic accident models describe an accident process as a complex and interconnected network of events (Qureshi, 2007). AcciMap, STAMP, FRAM and IPIC RAM identify extra-organisational factors (Van Schaardenburgh-Verhoeve, 2008). The use of systemic accident models for accident prediction (in conjunction with the model of this thesis) should be explored to discover the influence of extra-organisational factors from which additional indicators may be derived.

Many barrier elements are electronical devices or devices containing electronical components. These electronical equipment and inline instruments are increasingly designed with sensors that continuously indicate their status or functioning. They show immediately when they deviate from their normal operating window, when maintenance is required, or even when they should be replaced. This kind of data can be used in the future to determine the quality or trustworthiness of the barriers of the barrier system, and hence to calculate the real time likelihood of the major hazard accident process what they protect against.

In recent years, more and more research has been conducted into dynamic risk assessments, in which methods have been developed to regularly update risk profiles. In the most recent studies, this is done based on accidents and near misses, the likelihood of human and equipment failure in the production process, and the performance of the barrier systems. Accident scenario analysis with probability updating is the key to dynamic risk assessments. Bayesian Network (BN) is an alternative technique with ample potential for application in risk assessments (Khakzad et al., 2011, 2013). The use of BN will continuously reduce data uncertainty of the bowtie when a new set of accident related information becomes available. It provides the accident scenarios with real time analysis, which leads to an up-to-date picture of the process safety performance, and a better understanding of the current and future accident processes. Further research is needed to see whether this approach can improve the prediction of major hazard accidents.

Accident processes only develop when they are initiated. The start of an accident process is called an 'initiating event'. Initiating events are generally categorised in three groups, meaning a loss of personal, operational or mechanical integrity. In this study, the development and likelihood of an accident process is only based on the barrier system, while it can also be determined from the initiating event. Especially when barrier systems consist of few barriers, it may be considered to monitor the initiating events too.

A validation of potential major hazard accident processes from a prospective view may take several years and is difficult to perform in the time frame of a doctoral study. An investigation is currently underway at OCI to build a process safety performance dashboard that, based on the preventive barrier indicators, provides insight into the (process) safety performance of ammonia plant # 3. Such a dashboard should provide information at multiple operational levels in the organisation in such a way, that the right information is sent to the right people at the right moment. The extent to which major hazard accidents are prevented, will become clear in the coming years.

8.5 REFERENCES

Filho, A., Jun, G. & Waterson, P. (2019). Four studies, two methods, one accident – An examination of the reliability and validity of Accimap and STAMP for accident analysis. *Safety Science, 113*, 310–317. https://doi.org/10.1016/j.ssci.2018.12.002.

Grant, E., Salmon, P., Stevens, N., Goode, N. & Read, G. (2018). Back to the future: What do accident causation models tell us about accident prediction? *Safety Science, 104*, 99–109. https://doi.org/10.1016/j.ssci.2017.12.018.

Haddon, W. (1963). A note concerning accident theory and research with special reference to motor vehicle accidents. *Annals of the New York Academy of Science, 107*, 635–645.

Khakzad, N., Khan, F., & Amyotte, P. (2011). Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. *Reliability Engineering and System Safety, 96*, 925-932. http://dx.doi.org/10.1016/j.ress.2011.03.012.

Khakzad, N., Khan, F., & Amyotte, P. (2013). Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. *Process Safety and Environmental Protection, 91*, 46-53. http://dx.doi.org/10.1016/j.psep.2012.01.005.

Le Coze, J. (2015). Reflecting on Jens Rasmussen's legacy. A strong program for a hard problem. *Safety Science, 71*, 123–141. http://dx.doi.org/10.1016/j.ssci.2014.03.015.

Onderzoeksraad Voor Veiligheid (OVV). (2018). *Chemie in samenwerking – Veiligheid op het industriecomplex Chemelot*. Retrieved from https://www.onderzoeksraad.nl/nl/page/4707/chemie-in-samenwerking---veiligheid-op-het-industriecomplex-chemelot.

Qureshi, Z. (2007). *A Review of Accident Modelling Approaches for Complex Socio-Technical Systems*. Retrieved from https://www.researchgate.net/publication/228683461_A_review_of_accident_modelling_approaches_for_complex_socio-technical_systems.

Rasmussen, J. (1990). The role of error in organising behaviour. *Ergonomics, vol. 33*, 1185–1199. http://dx.doi.org/10.1080/00140139008925325.

Schaardenburgh van-Verhoeve, K. (2008). *Beyond Traditional Accident Investigation* (Master's thesis). Retrieved from https://www.incidenteel.com/wp-content/uploads/2014/02/2008-Searching-for-extra-organisational-factors_Van-Schaardenburgh-Verhoeve.pdf.

Swuste, P., Theunissen, J., Schmitz, P., Reniers, G., Blokland, P. (2016). Process safety indicators, a review of literature. *Journal of Loss Prevention in the Process Industries, 40*, 162–173. http://dx.doi.org/10.1016/j.jlp.2015.12.020.

A

LIST OF ABBREVIATIONS
ABOUT THE AUTHOR
PUBLICATIONS
ACKNOWLEDGEMENTS

LIST OF ABBREVIATIONS

Abbreviation	Meaning
AIChE	American Institute of Chemical Engineers
ANSI	American National Standards Institute
API	American Petroleum Institute
APPEA	Australian Petroleum Production & Exploration Association
BN	Bayesian Network
BP	British Petrol
BRZO	Besluit Risico Zware Ongevallen
B/W	Black & White
CCPS	Centre for Chemical Process Safety
Cefic	Conseil Européen des Federations de l'Industrie Chimique
COMAH	Control of Major Accident Hazards
CSB	U.S. Chemical Safety Board
DNV GL	Det Norske Veritas & Germanischer Lloyd
EPSC	European Process Safety Centre
ESD	Emergency shutdown
FAL	Flow alarm low
FIAL	Flow indicating alarm low
FMEA	Failure Mode and Effect Analysis
HRO	High Reliability Organisation
HSE	Health and Safety Executive
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IPL	Independent Protection Layer
IR	Infrared
JSA	Job Safety Analysis
KPI	Key Performance Indicator
LAL	Level alarm low
LMRA	Last Minute Risk Assessment
LOC	Loss of Containment
LOPA	Layer of protection analysis
LOPC	Loss of Primary Containment
LoToTo	Lock-out, Tag-out, Try-out
LT	Level Transmitter
LTIF	Lost Time Injury Frequency
MA	Motor alarm
MoC	Management of Change
MRT	Mean repair time
MTTR	Mean time to repair
NVVK	Nederlandse Vereniging van Veiligheidskundigen
OCI	Orascom Construction Industries
OECD	Organisation for Economic Co-operation and Development
OGP	International Association of Oil and Gas Producers
OSHA	Occupational Safety and Health Administration
OVV	Onderzoeksraad voor Veiligheid (Dutch Safety Board)
PHA	Process Hazard Assessment
PSE	Process Safety Event
PSM	Process Safety Management
PSSR	Process Safety Start-up Review
PT	Pressure Transmitter
P/T	Pressure/Temperature
RBI	Risk-Based Inspection
RCS	Risk Control System
RIVM	Rijksinstituut voor Volksgezondheid en Milieu
RR	Risk reduction
RRL	Risk reduction expressed in logarithm

Abbreviation	Meaning
RRRL	Relative risk reduction expressed in a logarithm
SCE	Safety Critical Equipment
SIF	Safety instrumented function
SIL	Safety integrity level
SMS	Safety Management System
SOP	Standard Operating Procedure
SU/SD	Start-up/Shutdown
SZW	Sociale Zaken en Werkgelegenheid
TI	Temperature Indicator
VROM	Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer

ABOUT THE AUTHOR

Peter Schmitz was born on March 19, 1964 in Hoensbroek, in the Netherlands. He graduated as a bachelor in process control from the HTS in Heerlen in 1987, and graduated again as a bachelor in chemical engineering some years later. Since 1987 he has worked in the process industry in several areas of interest, from process control and process safety engineering to daily operations. From 2005 to 2009, he worked as a global process safety competence manager. During this period, he became interested in measuring process safety which was initiated by the Baker report after the BP Texas City refinery incident in 2005. Various (petro)chemical companies were looking to measure their process safety performance using different indicators. When he graduated from the MoSHE course at the Technical University in Delft in 2012, a seed was planted to do further research in this field. In 2015, Peter met Paul Swuste, an associate professor working within the Safety and Security Science group of the Technical University of Delft, who was investigating the use and current practices in the process industry regarding process safety indicators. One year later, it was agreed to continue Paul's investigation, which resulted in this doctoral research. During his research, Peter gave several presentations at national and international safety conferences and symposia regarding the process safety topics in this dissertation.

PUBLICATIONS

Swuste, P., Theunissen, J., Schmitz, P., Reniers, G., Blokland, P. (2016). Process safety indicators, a review of literature. *Journal of Loss Prevention in the Process Industries, 40*, 162–173. http://dx.doi.org/10.1016/j.jlp.2015.12.020.

Schmitz, P., Swuste, P., Theunissen, J., Reniers, G., Decramer, G., & Uijterlinde, P. (2018a). Een aanpak voor het bepalen van een realistische ranking van de gevaarlijkste procesonderdelen van het ammoniakproductieproces. *Tijdschrift voor toegepaste Arbowetenschap, 2018(2)*, 42–56.

Schmitz, P. (2018b). Sustainable asset integrity, bijdrage CGC-NVVK bijeenkomst Brzo+ bedrijven, 'ageing' en inspectie. In Swuste, P. & Jongen, M. Verslag van de bijeenkomst van de Contactgroep gezondheid en Chemie en de Nederlandse Vereniging voor Veiligheidskunde op 18 januari 2018. *Tijdschrift voor toegepaste Arbowetenschap, 2018*(1), 24–27. https://www.arbeidshygiene.nl/-uploads/files/insite/tta-2018-01-verslag-cgc-nvvk-swuste-en-jongen.pdf.

Schmitz, P., Swuste, P., Reniers, G., & Nunen van, K. (2019a). Mechanical integrity of process installations: an assessment based on bow-ties. *Chemical Engineering transactions, 77*, 97–102. https://doi.org/10.3303/CET1977017.

Schmitz, P., Swuste, P., Reniers, G., & Decramer, G. (2019b). Een aanpak voor het beoordelen van mechanische faalmechanismen van statische apparaten van het ammoniakproductieproces. *Tijdschrift voor toegepaste Arbowetenschap, 2019*(2), 34–54.

Schmitz, P. (2019c). Mechanical Integrity of Process Installations: An Assessment Based on Bow-Ties. *Ammonia Technical Manual, 2019*, 17–28.

Schmitz, P., Swuste, P. & Reniers, G. (2019d). Een vlinderdas-analyse van statische apparatuur in een ammoniakfabriek. In Frijters, A., Groeneweg, J., Guldener van, V., Guldenmund, F., Jeen, T., Mud, M. & Mutu, A. (Eds.), *2025 Wat ga ik anders doen? Congresbundel 2019* (pp. 76-79). Alphen aan den Rijn, The Netherlands: Vakmedianet. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj_oY73k-zwAhXdA2MBHXIODZEQFjABegQIBBAF&url=https%3A%2F%2Fwww.nvvkveiligheidscongres.nl%2Fstream%2Flrnvvkcongres2019.pdf&usg=AOvVaw0gnkTqi1kcjM8BjeJUXsI5.

Swuste, P., Nunen van, K., Schmitz, P. & Reniers, G. (2019e). Hoe effectief zijn procesveiligheidsindicatoren? In Frijters, A., Groeneweg, J., Guldener van, V., Guldenmund, F., Jeen, T., Mud, M. & Mutu, A. (Eds.), *2025 Wat ga ik anders doen? Congresbundel 2019* (pp. 76-79). Alphen aan den Rijn, The Netherlands: Vakmedianet. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj_oY73k-zwAhXdA2MBHXIODZEQFjABegQIBBAF&url=https%3A%2F%2Fwww.nvvk-veiligheidscongres.nl%2Fstream%2Flrnvvkcongres2019.pdf&usg=AOvVaw0gnkTqi1kcjM8BjeJUXsI5.

Schmitz, P., Swuste, P., Reniers, G. & Nunen van, K. (2020a). Mechanical integrity of process installations: Barrier alarm management based on bowties. *Process Safety and Environmental Protection, 138*, 139–147. https://doi.org/10.1016/j.psep.2020.03.009.

Schmitz, P., Swuste, P., Reniers, G., & Nunen van, K. (2020b). Een praktische aanpak voor het voorspellen van majeure ongevallen in de procesindustrie op basis van de barrière status op scenario niveau. *Tijdschrift voor toegepaste Arbowetenschap, 2020*(2), 47–66.

Schmitz, P., Swuste, P., Reniers, G., & Nunen van, K. (2020c). Een praktische, kwalitatieve aanpak voor het voorspellen van majeure ongevallen in de procesindustrie op basis van organisatorische factoren. *Tijdschrift voor toegepaste Arbowetenschap, 2020*(4), 124–134.

Schmitz, P., Reniers, G. & Swuste, P. (2021a). Determining a realistic ranking of the most dangerous process equipment of the ammonia production process: A practical approach. *Journal of Loss Prevention in the Process Industries, 70*, 104395. https://doi.org/10.1016/j.jlp.2021.104395.

Schmitz, P., Reniers, G., Swuste, P. & Nunen van, K. (2021b). Predicting major hazard accidents in the process industry based on organizational factors: a practical, qualitative approach. *Process Safety and Environmental Protection, 148*, 1268–1278. https://doi.org/10.1016/j.psep.2021.02.040.

Schmitz, P., Swuste, P., Reniers, G. & Nunen van, K. (2021c). Predicting major accidents in the process industry based on the barrier status at scenario level: a practical approach. *Journal of Loss Prevention in the Process Industries, 71*, 104519. https://doi.org/10.1016/j.jlp.2021.104519.

Schmitz, P., Reniers, G. & Swuste, P. (2021d). Predicting major hazard accidents by monitoring their barrier systems: a validation in retrospective. *Process Safety and Environmental Protection, 153*, 19–28. https://doi.org/10.1016/j.psep.2021.07.006.

ACKNOWLEDGEMENTS

After several process safety incidents at OCI Nitrogen in 2015 and 2016, we asked ourselves whether these incidents could have been prevented. Even though, thankfully, there were no personal injuries, and consequences were limited to material damage and loss of production, we were alarmed. The request from the management of OCI Nitrogen to find a sustainable solution did not come as a surprise and marked the start of this doctoral research.

Over the past five years, many of my OCI and Sitech colleagues contributed to all kinds of sub-questions that I encountered along the way. Without their constructive commitment and critical attitude, this doctoral research would never have led to the current result, for which I am very grateful. If we succeed in implementing the model in the next phase, our installations will become even safer.

Writing is explaining something to yourself. It turned out to be a skill that I gradually mastered. My thanks go to the co-authors, the reviewers, the members of the doctoral committee, and those who contributed in other ways to the writing of the manuscripts and this thesis.

Finally, I would like to thank the Graduate school and the Safety and Security Science group of the Delft University of Technology for their great contribution to this research. The discussions we had were always inspiring as they arouse my curiosity, and were often a stimulus for further exploration.