Predicting major hazard accidents by monitoring their barrier systems
A validation in retrospective

Schmitz, Peter; Reniers, Genserik; Swuste, Paul

DOI
10.1016/j.psep.2021.07.006

Publication date
2021

Document Version
Final published version

Published in
Process Safety and Environmental Protection

Citation (APA)
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

Process Safety and Environmental Protection 153 (2021) 19–28

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

Predicting major hazard accidents by monitoring their barrier systems: A validation in retrospective

Peter Schmitz[a,b,*], Genserik Reniers[a], Paul Swuste[a]

[a] Safety and Security Science Group, Faculty of Technology, Policy and Management, Technical University of Delft, Jaffalaan 5, 2628 BX, Delft, the Netherlands
[b] OCI-Nitrogen, Urmonderbaan 22, 6167 RD, Geleen, the Netherlands

ARTICLE INFO

Article history:
Received 8 March 2021
Received in revised form 14 June 2021
Accepted 2 July 2021
Available online 6 July 2021

Keywords:
Process safety
Bowtie
Indicator
Organizational factor
Management delivery system

ABSTRACT

OCI Nitrogen, one of Europe's largest fertilizer producers, is investigating the extent to which it is possible to take targeted measures at an early stage and stop the development of major hazard accident processes. An innovative model has been developed and recently explained and elaborated in a number of publications. This current paper 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 practice. 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 categorized as flaws and allocated to nine organizational 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 paper 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 organizational factors.

1. Introduction

OCI Nitrogen, one of Europe's largest fertilizer producers, faced several serious process safety related incidents in the period 2015 – 2020. According to an internal investigation they were mainly caused by incorrect choice of materials, accelerated wear, incorrect design, and unrecognized risks during work. Although no physical injuries were suffered in any of the incidents, in some cases the plant had to be shut down for a longer period and large economic costs were suffered. OCI initiated an investigation in which management asked how process safety can be monitored. The underlying aim of the internal investigation is to be able to take targeted measures at an early stage and stop the development of major accident processes. An innovative model has been developed and recently issued in a few papers (Schmitz et al., 2020, 2021a,b,c). This paper offers a validation of the model by looking in retrospect at a major hazard accident, the 2005 BP Texas city incident, using two papers in particular: Schmitz et al. (2021b,c) regarding preventive barrier indicators, and organizational factors respectively. 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 organizational 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 (Britisch Petrol (BP)., 2005) as well as externally by the U.S. Chemical Safety and Hazard Investigation Board (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 manage-

* Corresponding author at: Safety and Security Science Group, Faculty of Technology, Policy and Management, Technical University of Delft, Jaffalaan 5, 2628 BX, Delft, the Netherlands.
E-mail addresses: peter.schmitz@ocinitrogen.com (P. Schmitz), G.L.L.M.E.Reniers@tudelft.nl (G. Reniers), paul@paulswuste.nl (P. Swuste).

https://doi.org/10.1016/j.psep.2021.07.006

ment 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 organizational factors or management delivery systems which played a role in this incident. This paper investigates how and to what extent this evidence could have served as an early warning. As this investigation is focused 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 Fig. 1 (U.S. Chemical Safety and Hazard Investigation Board (CSB), 2007). During startup, 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).

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 startup, operations personnel pumped flammable liquid hydrocarbons into the tower for over three hours without any liquid being removed, which was contrary to startup 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 vapors released from the process.

The released volatile liquid evaporated as it fell to the ground and formed a flammable vapor cloud. The most likely source of ignition for the vapor 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.

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., 2005, 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 paper's validation and is elaborated in the next chapter. 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, optimize the (management of the) current safety barrier system, and improve the design of new safety barrier systems.

3. Methodology

This validation is based on a method which is described in two papers, one related to preventive barrier indicators (Schmitz et al., 2021b), and one regarding organizational factors (Schmitz et al., 2021c). The model is based on the bowtie metaphor, which is used 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., 2021b). 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;

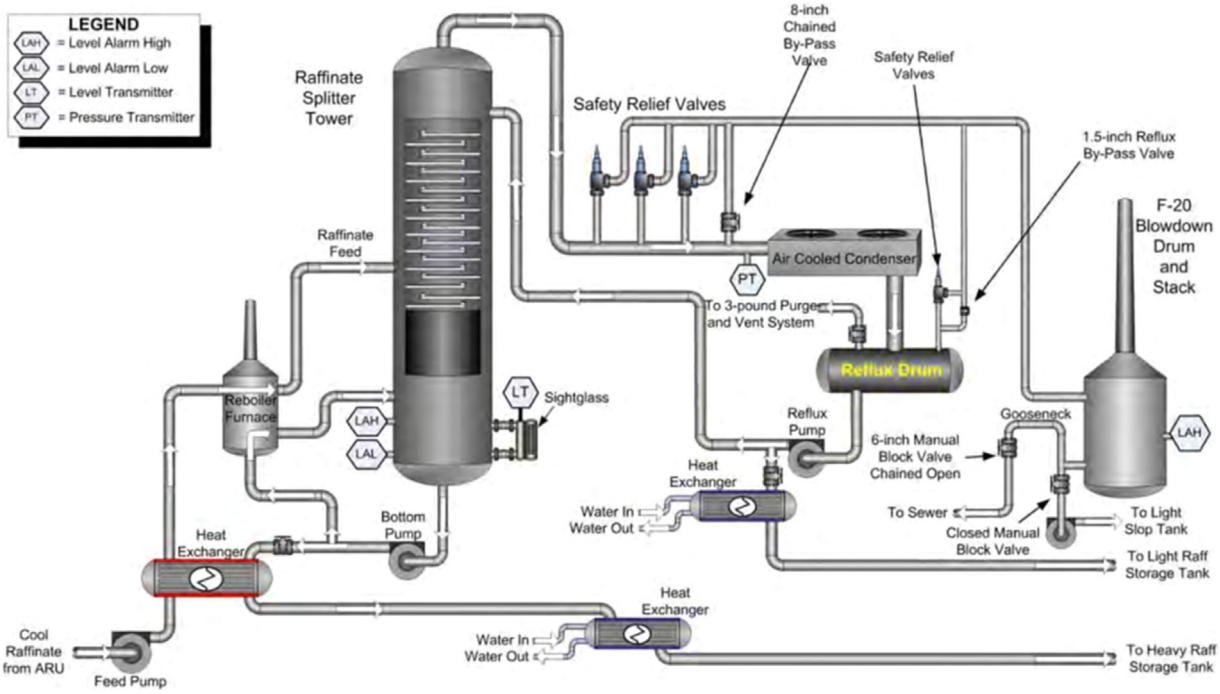

Fig. 1. Raffinate section of the ISOM unit (CSB, 2007).

2 With the preventive barrier system as perceived by the day shift control room operator on the day of the incident;
3 With the preventive barrier system according to current standards of best practice.

Secondly, we study the organizational factors or management delivery systems which can also be linked to accident processes and their barrier system (Schmitz et al., 2021c). Flaws in organizational factors may indirectly impact accident processes as organizational factors are responsible for delivering the required quality or trustworthiness of the barrier system. For each barrier, the appropriate organizational 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, organizational 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 organizational 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.

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 practice.

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

4.1. Preventive barrier indicators

Fig. 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 Fig. 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 startup procedure including some of the main following steps (Britisch Petrol (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 Fig. 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 Fig. 1) at 78 % of the transmitter value, indicating that the level in the stripper's bottom is too high. At

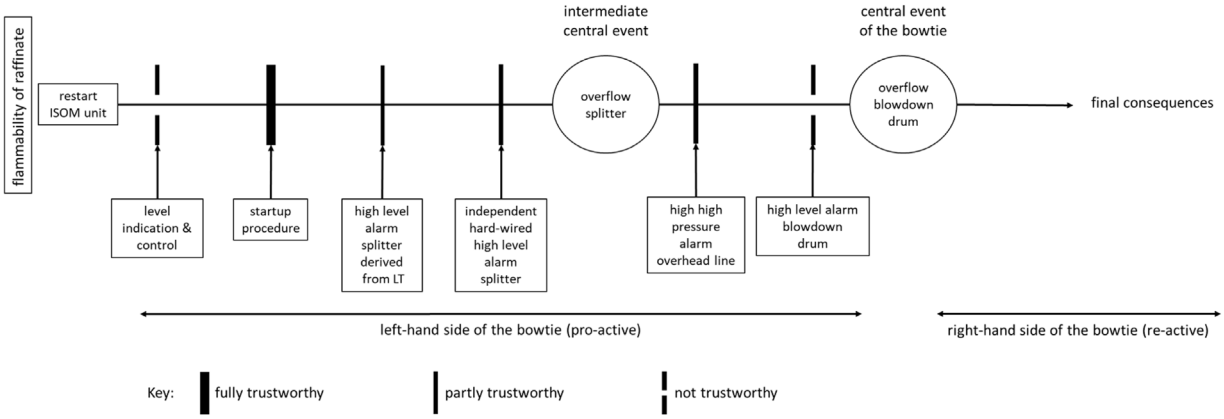

Fig. 2. The barrier system as designed on the day of the incident.

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 Fig. 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 Fig. 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.

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 (Centre for Chemical Process Safety (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 startup 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 (Britisch Petrol (BP)., 2005). If adhered to, the startup 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 (Centre for Chemical Process Safety (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 (Centre for Chemical Process Safety (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 startup 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. Fig. 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 × 100 %) and 50 % (3/6 × 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 × 100 %).

From the day shift control room operator's perspective, using the accident investigation reports (Britisch Petrol (BP)., 2005; U.S. Chemical Safety and Hazard Investigation Board (CSB), 2007; Hopkins, 2008), the barrier system looks slightly different as shown in Fig. 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 startup 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,

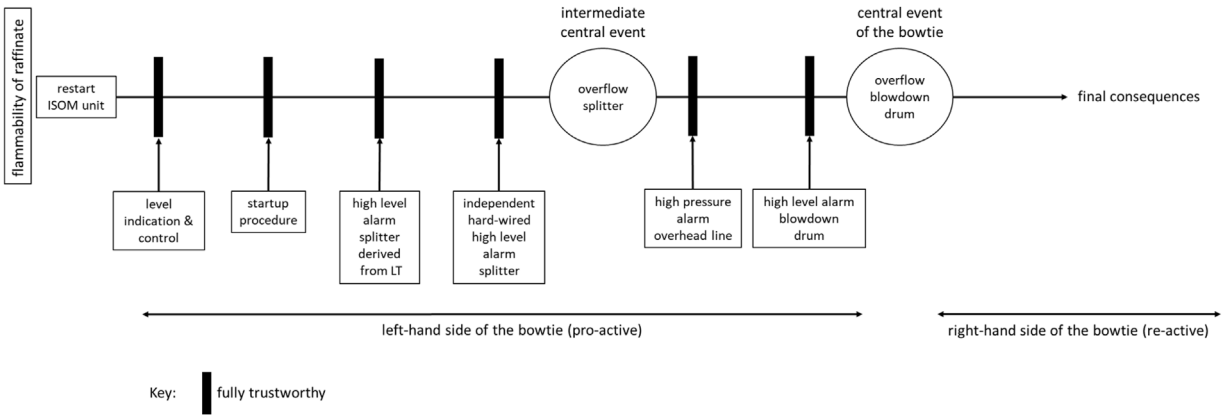

Fig. 3. The barrier system perceived by the day shift control room operator on the day of the incident.

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 startup, because he would have been told otherwise.

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 realize 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 Fig. 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 startup (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 startup, operators had a good reason for this practice. 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 startup 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 (Britisch Petrol (BP)., 2005).

From the day shift control room operator's view, all six barriers were trustworthy: the level indication and control, the startup 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 startup procedure and ignored the high level alarm, he was fully confident of his violation and did probably not realize 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 × 100 %), which means a fully active barrier system with six barriers.

The investigation reports studied (Britisch Petrol (BP)., 2005; U.S. Chemical Safety and Hazard Investigation Board (CSB), 2007; Hopkins, 2008) all indicated that the design of the splitter and blowdown drum did not meet current standards of best manufacturing practice. Fig. 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 startup 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.

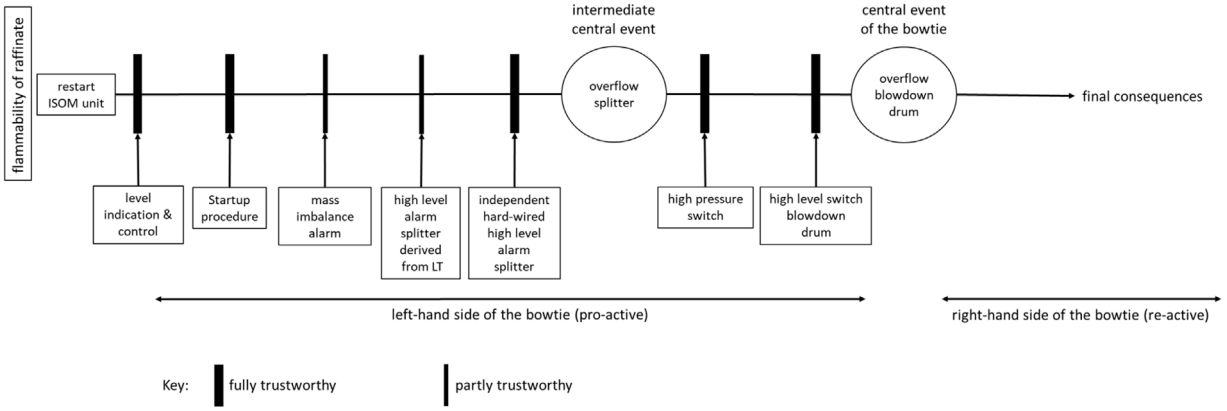

Fig. 4. A barrier system design of the splitter to protect against overfilling according to current standards.

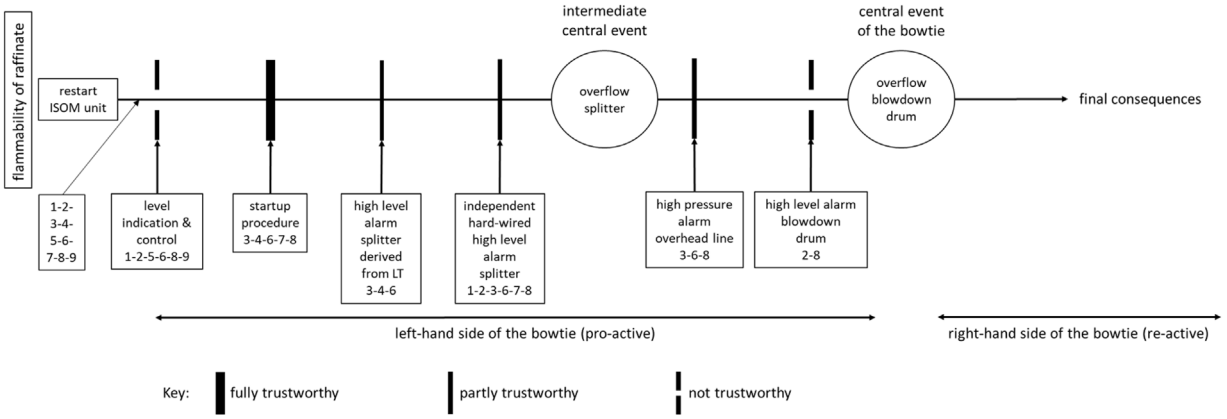

Fig. 5. The organizational factors on the day of the incident.
(1. Maintenance; 2. Inspection and testing; 3. Training & competence; 4. Management; 5. Procedures; 6. Plant documentation; 7. Communication & coordination; 8. Plant design & operations; 9. Hardware integrity).

- A hardwired high pressure switch which will automatically shut-down 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 Fig. 4.

The barrier system design in Fig. 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 startup 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 startup 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 (Centre for Chemical Process Safety (CCPS)., 2015). In short, the risk of overfilling of the splitter has reduced by 10,000–100,000 which comes down to an RRL of 4–5 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 6–7 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 Fig. 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 practice. 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 practice would have been somewhere between 29 % (2/7 × 100 %) at worst and 50 % (3/6 × 100 %) at best.

4.2. Organizational factors

Schmitz et al. compiled nine organizational factors or management delivery systems (see legend of Fig. 5). The relation of the organizational factors with the accident processes runs through the barrier systems. Fig. 5 shows the organizational factors on the day of the incident, which relate to Fig. 2. The organizational factors strongly influence the quality or trustworthiness of the barriers and are indicated in the box under each of the barriers. In addition,

Table 1
Organizational factors creating latent, dangerous conditions.

Organizational factors	General flaws in the organizational factors
Maintenance	• Maintenance details were poorly documented (eg. Instrumentation calibration).
Inspection & testing	• The startup 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 focused on lagging indicators for personal safety. • There was an inability to learn from previous startup failures as they were not investigated.
Management	• There was no fatigue prevention policy as operators worked long shifts for many days in a row. • Many steps of the startup 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 organization 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 startup review were not conducted. • Changes to the startup procedures and training actions were not closed although indicated.
Plant documentation	• The startup 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 startup. • Poor handover procedures. • Hundreds of contractors in the Ultracracker TA were unaware of the startup. • 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 startup.

malfunctioning organizational 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 organizational factors is indicated in the box on the left-hand side in Fig. 5 which directly points to the accident process or scenario.

The investigation reports provide an overwhelming amount of evidence on what went wrong at BP's refinery site in Texas City. In Table 1 relevant evidence has been included as flaws for each of the nine organizational factors which had an influence on the accident process (as indicated in the box on the left-hand side of Fig. 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 2 highlights the organizational 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 organizational factor. The evidence demonstrates not only the flaws of the organizational factor but also shows the decline of the barrier's quality.

5. Discussion

The authors retrieved their information from the three investigation reports as well as from Hopkins' book "Failure to learn". They have not been to the BP's refinery site at Texas City nor have they spoken to anyone involved in the incident or to their investigators. As a result, this article 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

Table 2
Organizational factors for each preventive barrier, on the day of the incident.

Organizational factors	Flaws in the organizational 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.
	Startup 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 startup were signed off as completed even though they were not. • The shift supervisor did not enforce, and the operators did not follow the startup procedure. • The startup 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 startup. The acting superintendent did not visit the ISOM to review progress with the operators. • The splitter startup 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 startup procedure and PHA's. • The startup procedure was not fully up to date. • Making a mass balance was not prescribed and described in the startup 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 startup 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 startup. • 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 startup. • 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.
Management	• A lack of supervision allowed the alarm to be ignored.
Plant documentation	• The relevance of the alarm was not documented in the startup 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 startup, 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 startup 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.

Table 2 (*Continued*)

Organizational factors	Flaws in the organizational factors of each preventive barrier
Plant documentation	• There was no reference of the cause of overpressurization due to overfilling of the splitter in the startup 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).

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 categorization 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 organizational factor of a barrier but to an organizational 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 organizational 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 paper 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 Centre for Chemical Process Safety (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 paper. Clearly, the lack of BP's follow-up is a cultural aspect, which could have been discovered looking at both the barrier system and organizational factors as demonstrated in this paper. 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 organizational 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, organizational 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 (Onderzoeksraad voor de Veiligheid (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 article shows that the barrier management approach can be used in a proactive way, regardless of the type of company within the (petro)chemical industry.

6. Conclusions

This paper 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 organizational 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 organizational 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 organizational 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 practices 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.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Aven, T., Sklet, S., Vinnem, J.E., 2006. Barrier and operational risk analysis of hydrocarbon releases (BORA-Release), Part I. method description. J. Hazard. Mater. A137, 681–691, http://dx.doi.org/10.1016/j.jhazmat.2006.03.027.

Baker, J., Retrieved from https://www.csb.gov/assets/1/20/baker_panel_report1.pdf?13842 2007. The Report of the BP U.S. Refineries Independent Safety Review Panel.

Britisch Petrol (BP), Retrieved from http://cip.management.dal.ca/publications/final_report.pdf 2005. Fatal Accident Investigation Report. Isomerization Unit Explosion (Final Report).

Centre for Chemical Process Safety (CCPS), 2015. Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis. Wiley, New York, U.S.

Hopkins, A., 2008. Failure to Learn. CCH Australia Ltd, Sydney, Australia.

Kalantarnia, M., Khan, F., Hawboldt, K., 2010. Modelling of BP Texas City refinery accident using dynamic risk assessment approach. Process. Saf. Environ. Prot. 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. J. Loss Prev. Process Ind. 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. Reliab. Eng. Syst. Saf. 96, 925–932, http://dx.doi.org/10.1016/j.ress.2011.03.012.

Khakzad, N., Khan, F., Amyotte, P., 2012. Dynamic risk analysis using bow-tie approach. Reliab. Eng. Syst. Saf. 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. Saf. Environ. Prot. 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. Nat. 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 Anal. 35 (7), 1336–1347, http://dx.doi.org/10.1111/risa.12337.

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

Meel, A., Seider, W.D., 2006. Plant-specific dynamic failure assessment using Bayesian theory. Chem. Eng. Sci. 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. J. Loss Prev. Process Ind. 20, 113–127, http://dx.doi.org/10.1016/j.jlp.2006.10.003.

Onderzoeksraad voor de Veiligheid (OVV), Retrieved from 2018. Chemie in Samenwerking. 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. J. Risk Res. 18 (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. Saf. Environ. Prot. 89, 151–164, http://dx.doi.org/10.1016/j.psep.2011.01.002.

Reason, J., 1990. Human Error. University Press, Cambridge, UK.

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. Eng. Fail. Anal. 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. Saf. Environ. Prot. 138, 139–147, http://dx.doi.org/10.1016/j.psep.2020.03.009.

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. J. Loss Prev. Process Ind. 70, http://dx.doi.org/10.1016/j.jlp.2021.104395, 104395.

Schmitz, P., Swuste, P., Reniers, G., Nunen van, K., 2021b. Predicting major accidents in the process industry based on the barrier status at scenario level: a practical approach. J. Loss Prev. Process Ind. 71, 104519, http://dx.doi.org/10.1016/j.jlp.2021.104519.

Schmitz, P., Reniers, G., Swuste, P., Nunen van, K., 2021c. Predicting major hazard accidents in the process industry based on organizational factors: a practical, qualitative approach. Process. Saf. Environ. Prot. 148, 1268–1278, http://dx.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. Reliab. Eng. Syst. Saf. 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. Saf. Sci. 48, 279–280, http://dx.doi.org/10.1016/j.ssci.2009.09.001.

U.S. Chemical Safety and Hazard Investigation Board (CSB), Retrieved from 2007. Investigation report, Refinery Explosion and Fire BP Texas City. 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. Reliab. Eng. Syst. Saf. 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. Proc. Inst. Mech. Eng. Part O J. Risk Reliab. 223 (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 Saf. Environ. Prot. 91, 333–342, http://dx.doi.org/10.1016/j.psep.2012.07.006.