Delft University of Technology

Mechanical integrity of process installations
Barrier alarm management based on bowties

Schmitz, Peter; Swuste, Paul; Reniers, Genserik; van Nunen, Karolien

DOI
10.1016/j.psep.2020.03.009

Publication date
2020

Document Version
Final published version

Published in
Process Safety and Environmental Protection

Citation (APA)
Schmitz, P., Swuste, P., Reniers, G., & van Nunen, 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

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.
For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.

Process Safety and Environmental Protection 138 (2020) 139–147

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

Mechanical integrity of process installations: Barrier alarm management based on bowties

Peter Schmitz[a,b,*], Paul Swuste[b], Genserik Reniers[b], Karolien van Nunen[b,c]

[a] OCI-Nitrogen, Urmonderbaan 22, 6167 RD, Geleen, The Netherlands
[b] Safety and Security Science Group, Faculty of Technology, Policy and Management, Technical University of Delft, Jaffalaan 5, 2628 BX, Delft, The Netherlands
[c] Research Chair Vandeputte, University of Antwerp, 2000, Antwerp, Belgium

ARTICLE INFO

Article history:
Received 12 January 2020
Received in revised form 8 March 2020
Accepted 10 March 2020
Available online 12 March 2020

Keywords:
Bowtie
Mechanical failure mechanism
Integrity
Process safety indicator
Ammonia
Risk-based inspections

ABSTRACT

A Safety Research project was carried out in an ammonia plant of OCI Nitrogen, located at the Chemelot site in Geleen, The Netherlands. This research focused 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 visualized using a bowtie. The research project 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.

© 2020 The Authors. Published by Elsevier B.V. on behalf of Institution of Chemical Engineers. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

Contents

1. Introduction

OCI Nitrogen, a producer of ammonia, fertilizer and melamine 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 sub-study is part of a larger study aimed at preventing major process safety incidents by early detection and targeted

* Corresponding author at: OCI-Nitrogen, Urmonderbaan 22, 6167 RD, Geleen, The Netherlands.
E-mail addresses: peter.schmitz@ocinitrogen.com (P. Schmitz), paul@paulswuste.nl (P. Swuste), G.L.L.M.E.Reniers@tudelft.nl (G. Reniers), K.L.L.vanNunen@tudelft.nl (K. van Nunen).

https://doi.org/10.1016/j.psep.2020.03.009
0957-5820/© 2020 The Authors. Published by Elsevier B.V. on behalf of Institution of Chemical Engineers. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

action. This paper 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 focused 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 paper is only focusing 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 visualized 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 monitor the quality of barriers (Guillaume, 2011; Guldenmund et al., 2006). Early warnings are investigated empirically in this paper 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 paper 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 programs 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.

2. Industrial challenge

A complete RBI program provides a consistent methodology for assessing the optimum combination of methods and frequencies of inspection. By analyzing each available inspection method, estimating its relative effectiveness in reducing failure probability and including the costs, an optimization program can be developed (API, 2016). However, an RBI program 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 program in which an inspection program 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 paper provides guidance for mapping scenarios into bowties, implementing early warnings and using barrier alarm management on scenario level.

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 (Van Nunen et al., 2018). 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). 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. The holes in the Swiss cheese correspond to the flaws in the organizational 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. 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 characterized 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 Cockshot (2005) it is ä 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 organizational 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.

In this paper three barrier elements are considered: detection by a sensor, diagnosis and action which are all three supported by management delivery systems as shown in Fig. 2. 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 Fig. 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.

In this paper primary barriers may consist of both technical and non-technical barrier elements, whereas non-technical ones are 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 focused 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 extensive discussed with the control room operators. These discussions gave insight in various process deviations.

Fig. 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). 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 Fig. 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.

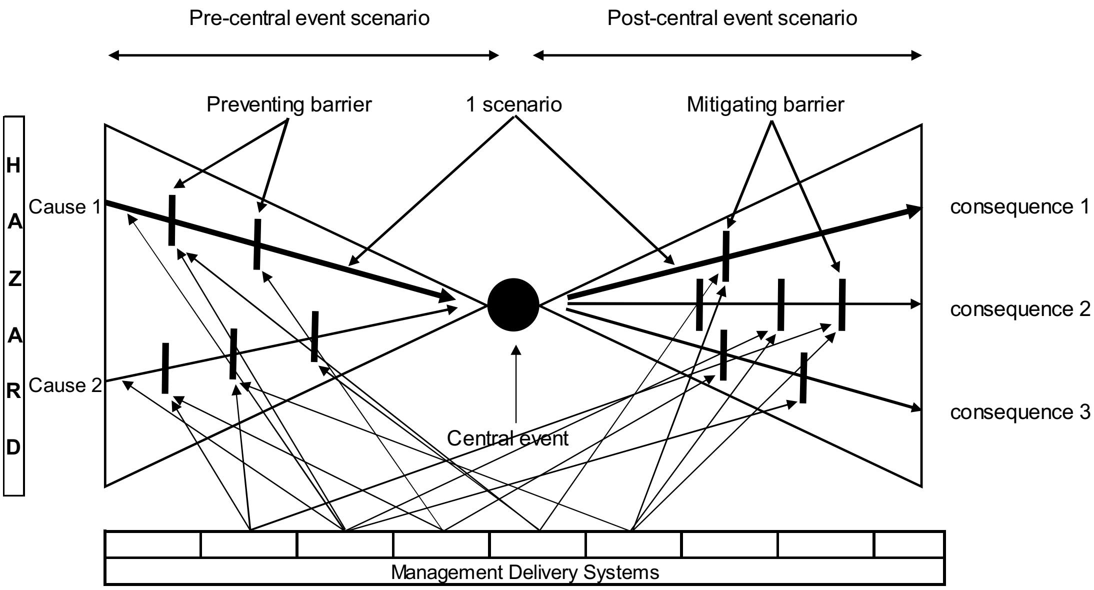

Fig. 1. Bowtie metaphor.

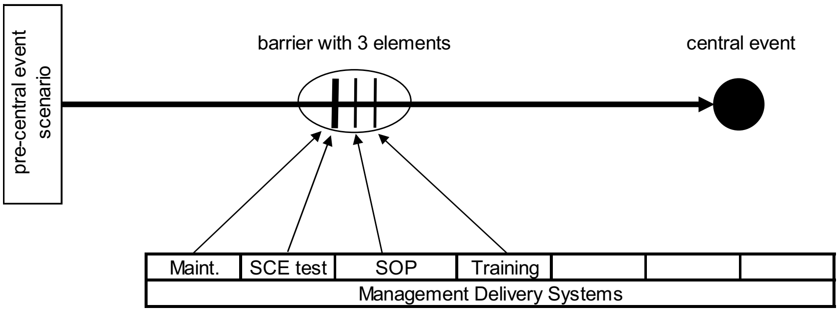

Fig. 2. Relation of management delivery systems and barriers. (Maint.: maintenance; SCE: safety critical equipment; SOP: standard operating procedure).

Table 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 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 x D x B. Table 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.

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 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 2 is a non-exhaustive list with examples of the quality (in the sense of reliability) of barriers and detections applied at

Table 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	

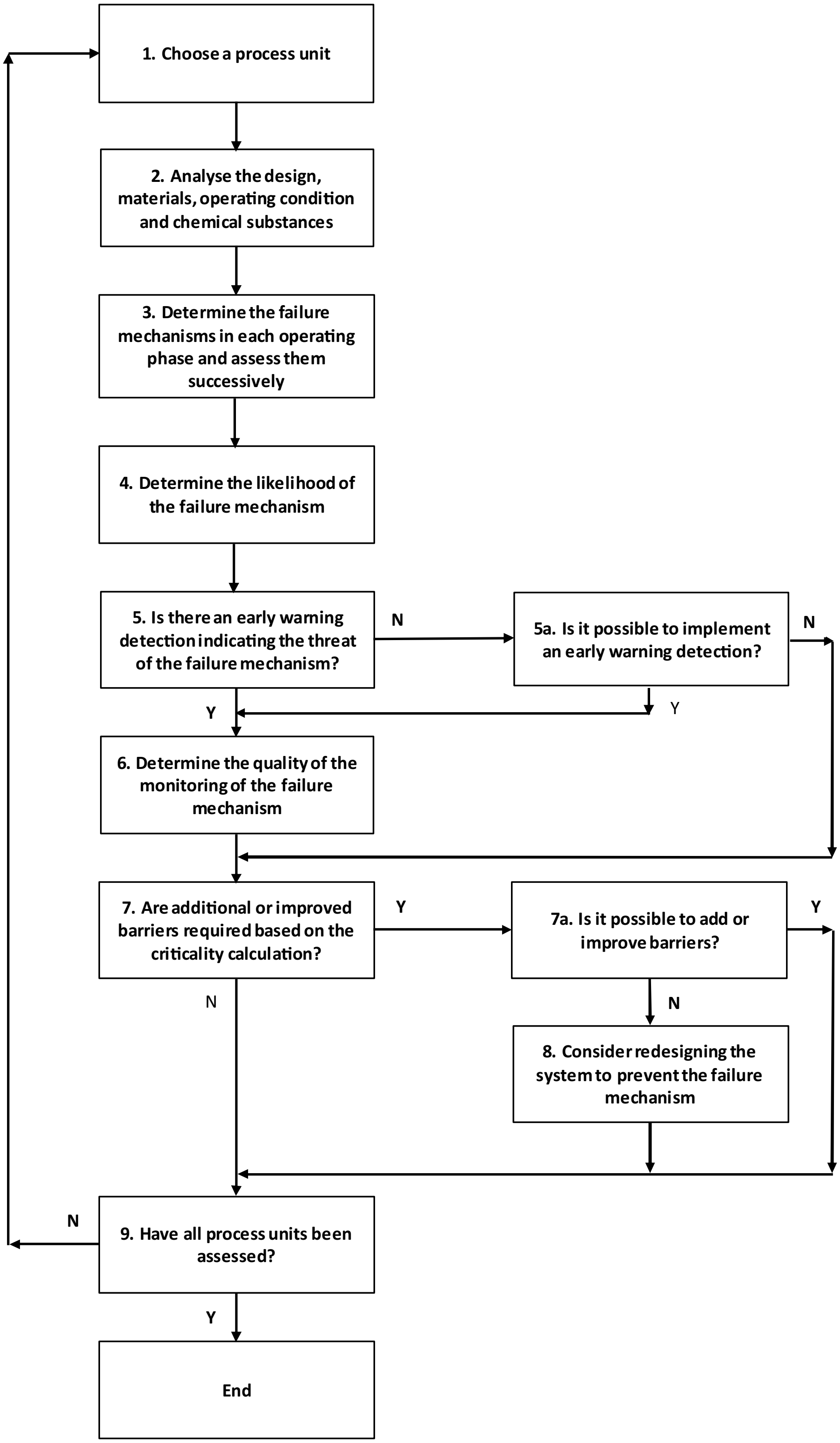
1. Choose a process unit
2. Analyse the design, materials, operating condition and chemical substances
3. Determine the failure mechanisms in each operating phase and assess them successively
4. Determine the likelihood of the failure mechanism
5. Is there an early warning detection indicating the threat of the failure mechanism?
N
5a. Is it possible to implement an early warning detection?
N
Y
Y
6. Determine the quality of the monitoring of the failure mechanism
7. Are additional or improved barriers required based on the criticality calculation?
Y
7a. Is it possible to add or improve barriers?
Y
N
N
8. Consider redesigning the system to prevent the failure mechanism
N
9. Have all process units been assessed?
Y
End

Fig. 3. Process unit assessment flow chart.

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 Fig. 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.

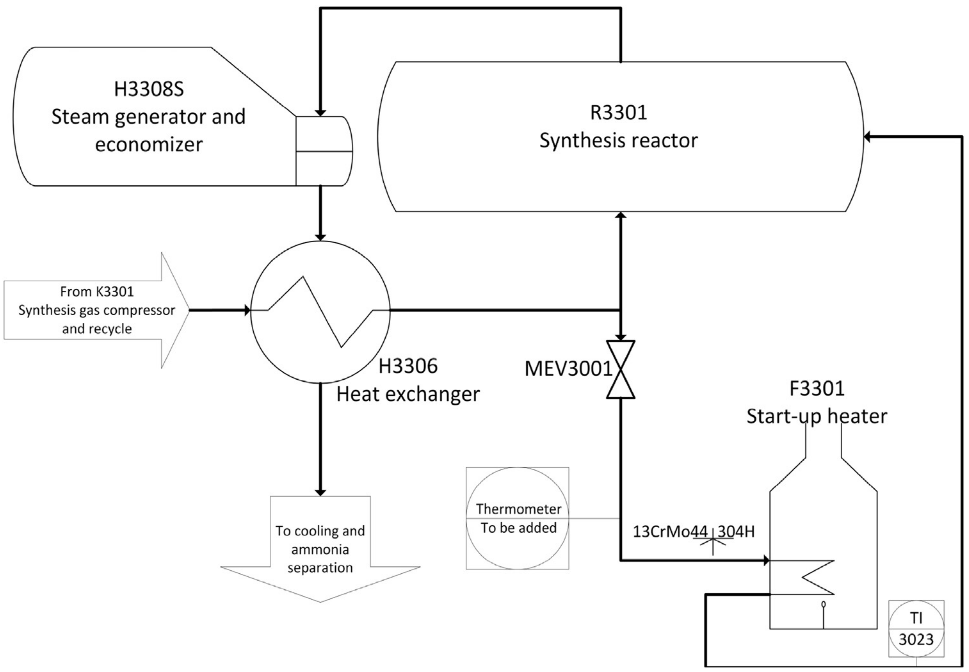

Fig. 4. Start-up heater and synthesis reactor.

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. Data collection and analysis

Two scenarios of an ammonia process unit were examined and schematically shown as the left part of the bowtie (Figs. 5 and 7). The presence and quality of barriers and early warnings (detection) was assessed, and it was determined whether improvements were necessary.

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 Fig. 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.

The supply line of the start-up heater is made of Cr-Mo steel (13CrMo44), whereas the coils are made of austenitic steel (304 H). 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 (304 H), 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 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

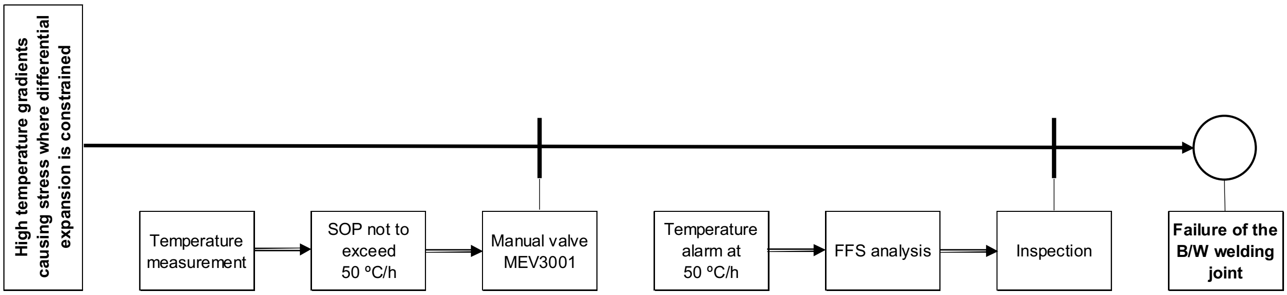
High temperature gradients causing stress where differential expansion is constrained
Temperature measurement
SOP not to exceed 50 °C/h
Manual valve MEV3001
Temperature alarm at 50 °C/h
FFS analysis
Inspection
Failure of the B/W welding joint

Fig. 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).

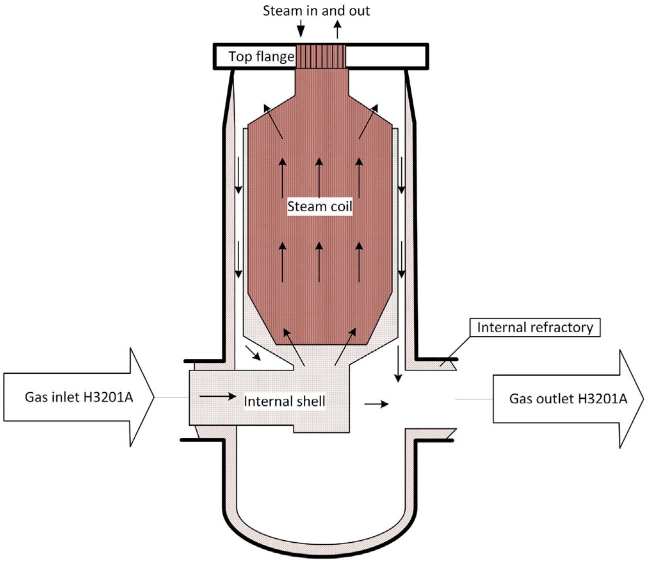

Fig. 6. Steam superheater.

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 × 2 × 4). 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 Fig. 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 × 2 × 2 = 12).

Fig. 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.

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. Fig. 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 attack 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 attack is always preceded by small, hard-to-see defects, the scenario is focused on the latter.

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 × 4 × 2). Therefore, the scenario must be provided with additional or improved barriers.

The heater can be provided with indicator paint on the outside, which discolors 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 dis-

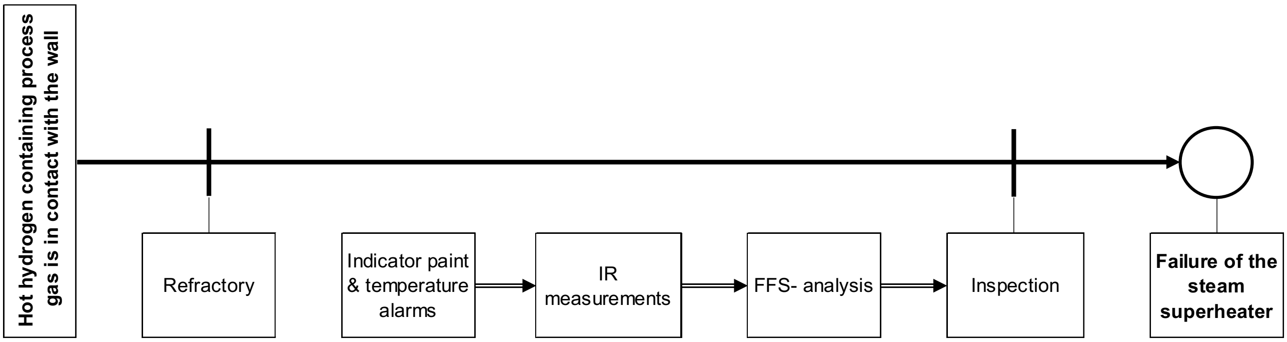
Hot hydrogen containing process gas is in contact with the wall
Refractory
Indicator paint & temperature alarms
IR measurements
FFS- analysis
Inspection
Failure of the steam superheater

Fig. 7. Left part of the bowtie regarding creep and Nelson hydrogen attack of the steam superheater (IR: infrared; FFS: fitness for service).

colored 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 ($C = L \times D \times B = 3 \times 2 \times 2$) which makes the scenario sufficiently safe. No additional barriers are required if the detection and monitoring are implemented as proposed above.

Fig. 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.

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 paper focused 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.

6. Conclusions

The main question raised in this paper 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 visualized 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 investigated further in a follow-up study.

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 program 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 paper 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.

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

API, 2016. Risk-Based Inspection. API RP 580, 3rd ed. API Publishing Services, Washington.

API, 2019. Mechanical Integrity: Fixed Equipment Standards & Recommended Practices. API Publishing Services, Washington DC 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. Reliab. Eng. Syst. Saf. 92, 735–744, http://dx.doi.org/10.1016/j.ress.2006.02.010.

CCPS, 2018. Dealing With Aging Process Facilities and Infrastructure. AIChE, New York.

Chevreau, F., Wybo, J., Cauchois, D., 2006. Organizing learning processes on risks by using the bow-tie representation. J. Hazard. Mater. 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. Saf. Environ. Prot. 83 (B4), 307–316, http://dx.doi.org/10.1205/psep.04380.

COMAH, 2010. Ageing Plant Operational Delivery Guide (accessed 22 November 2019) http://www.hse.gov.uk/comah/guidance/ageing-plant-core.pdf.

de Ruijter, A., Guldenmund, F., 2016. The bowtie method: a review. Saf. Sci. 88, 211–218, http://dx.doi.org/10.1016/j.ssci.2016.03.001.

DNV, 1996. Risk Management of Ageing Process Plants. DNV Research Report 96-2001.

Dokas, M., Feehan, J., Syed, I., 2013. EWaSAP: an early warning sign identification approach based on a systemic hazard analysis. Saf. Sci. 58, 11–26, http://dx.doi.org/10.1016/j.ssci.2013.03.013.

Groeneweg, J., 1992. Controlling the Controllable, the Management of Safety. DSWO Press, Leiden.

Guillaume, E., (Doctoral thesis) 2011. Identifying and Responding to Weak Signals to Improve Learning from Experiences in High-risk Industry.

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. J. Hazard. Mater. 130, 234–241.

Hassan, J., Khan, F., 2012. Risk-based asset integrity indicators. J. Loss Prev. Process Ind. 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? Thesis MoSHE course TU Delft 2016.

Hollnagel, Erik, 2008. Risk + barriers = safety? Saf. Sci. 46, 221–229, http://dx.doi.org/10.1016/j.ssci.2007.06.028.

HSE, 2006. Plant ageing. RR509 (accessed 22 November 2019) http://www.hse.gov.uk/research/rrhtm/rr509.htm.

HSE, 2007. Key Programme 3. Asset Integrity Programme. http://www.hse.gov.uk/offshore/kp3.pdf.

HSE, Whittle House, Warrington 2010. Managing Ageing Plant, A Summary Guide.

IAEA, 2017. Handbook on Ageing Management for Nuclear Power Plants. Safety Guide No. NP-T-3.24. 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? J. Loss Prev. Process Ind. 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. J. Loss Prev. Process Ind. 35, 352–356, http://dx.doi.org/10.1016/j.jlp.2014.10.008.

Øien, K., Utne, I., Herrera, I., 2011a. Building safety indicators I theoretical foundations. Saf. Sci. 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. Saf. Sci. 49, 162–171, http://dx.doi.org/10.1016/j.ssci.2010.05.015.

OGP, 2008. Asset Integrity – the Key to Managing Major Incident Risks. Report No. 415. https://www.scribd.com/document/391778284/OGP-Report-415-Asset-integrity-the-key-to-managing-major-incident-risks-December-2008-pdf.

OVV, https://www.onderzoeksraad.nl/nl/page/4707/ chemie-in-samenwerking—veiligheid-op-het-industriecomplex-chemelot (accessed 14 December 2019) 2018. Chemie in Samenwerking.

Perrow, C., 1984. Normal Accidents. Living With High-risk Technologies. Basic Books, New York.

Reason, J., 1987. The Chernobyl errors. Bull. Br. Psychol. Soc. 40, 201–206.

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

Reason, J., 1997. Managing the Risks of Organizational Accidents. Taylor & Francis, Abingdon.

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. Chem. Eng. Trans. 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. J. Loss Prev. Process Ind. 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. J. Loss Prev. Process Ind. 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. B + B Vakmedianet, Alphen aan den Rijn.

SZW, 2016. Ageing bij Brzo-bedrijven.

TNO, 2015. Literatuuronderzoek naar veroudering van installaties (accessed 18 November 2019) https://publications.tno.nl/publication/34626341/jB13ci/TNO-2015-R10878.pdf.

Turner, B., 1978. Man-made Disasters. Butterworth-Heinemann, Oxford.

Utne, I.B., Brurok, T., Rødseth, H., 2012. A structured approach to improved condition monitoring. J. Loss Prev. Process Ind. 25, 478–488, http://dx.doi.org/10.1016/j.jlp.2011.12.004.

Van Nunen, 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, 2–19, http://dx.doi.org/10.3390/ma11101955.

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