CHEMICAL ENGINEERING TRANSACTIONS

VOL. 91, 2022

A publication of AIDIC

The Italian Association
of Chemical Engineering
Online at www.cetjournal.it

Guest Editors: Valerio Cozzani, Bruno Fabiano, Genserik Reniers
Copyright © 2022, AIDIC Servizi S.r.l.
ISBN 978-88-95608-89-1; **ISSN** 2283-9216

DOI: 10.3303/CET2291018

Linking Barrier Indicators to Major Accident Scenarios, a First Step to Predict Major Accident Scenarios

Peter Schmitz [a], 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, Technical University of Delft, Jaffalaan 5, 2628 BX Delft, The Netherlands
[c]Research Chair Vandeputte, University of Antwerp, 2000 Antwerp, Belgium
paul@pauswuste.nl

At the OCI Nitrogen ammonia plant, located at the Chemelot site in Geleen, The Netherlands, a project has been initiated to monitor major accident processes at the site. This contribution answers the question whether indicators can be derived from the barrier system status to provide information about the development and likelihood of the major accident processes in the ammonia production process. The accident processes are visualized as scenarios in bowties. This research focuses on the status of the preventive barriers on the so called ‘left-hand side’ of the bowtie, before a hazard becomes uncontrollable. Both the quality – expressed in reliability/availability and effectiveness – and the activation of the barrier system give an indication of the development of the accident scenarios and the likelihood of the central event. This likelihood is calculated as a loss of risk reduction compared to the original design. The calculation gives in an indicator called “preventive barrier indicator”, which should initiate further action. Based on an example, it is demonstrated which actions should be taken and their urgency.

1. Introduction

Identifying process safety indicators of the ammonia production process and providing information on major accident processes is a challenge. The starting point is the ranking of the most dangerous process parts (Schmitz et al., 2020). Completed with major accident scenarios of ammonia plants internationally, a selection of most likely, hazardous scenarios has been determined. This study describes the results concerning indicators to recognise and stop the development of these “worst credible” scenarios at an early stage. The research question is:

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

There is little empirical research published on process safety indicators, but many (petro)chemical companies measure their process safety performance. Often, a distinction is made between 'leading' and 'lagging' indicators. Where the former are proxies to hazards, barriers, scenarios and management factors, the latter provide information on the loss of containment or loss of control events and their consequences. The scientific literature questions this distinction (Swuste et al., 2016, 2019).

2. Materials and methods

The bowtie model of accident processes is used in this study, starting with one or more hazards at its left side (Visser, 1998). A hazard represents an energy, e.g. a chemical substance, or an overpressure (Figure 1). Arrows represent different scenarios which will lead to a so-called central event, a situation where a hazard becomes uncontrollable. Barriers placed in the scenario pathways can prevent a central event from happening.

Paper Received: 14 January 2022; Revised: 23 March 2022; Accepted: 25 May 2022
Please cite this article as: Schmitz P., Swuste P., Reniers G., Van Nunen K., 2022, Linking Barrier Indicators to Major Accident Scenarios, a first Step to Predict Major Accident Scenarios, Chemical Engineering Transactions, 91, 103-108 DOI:10.3303/CET2291018

Barriers are generally classified in physical and non-physical barriers, and are usually made up of three elements: a sensor, a decision maker and a final element or action taker (Guldenmund et al., 2006). A barrier only works if all three elements are functioning, and can be regarded as a 3-out of-3 system.

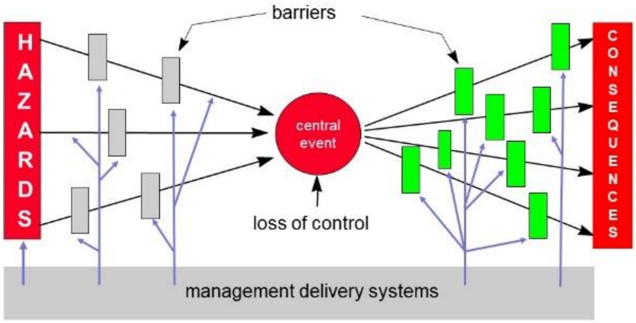


Figure 1: The bow-tie model (Visser, 1998)

The quality of a barrier is determined by various parameters, including: 1/ trustworthiness (effectiveness: functionality, reliability: performing its function, availability: functioning at any point in time), 2/ costs to keep the barrier functional, reliable and available, 3/ robustness: continue to function during incidents, 4/ response time: the time from activation to the execution of the intended function, and 5/ ''trigger": the event or condition that activates the barrier. To measure the likelihood of a scenario to develop into a central event, the decline in quality of the barriers must be monitored. The quality parameter trustworthiness is regarded as the only one that will vary sufficiently over time and can present the possible deterioration in quality of a barrier.

Preventive and corrective maintenance, inspection and test programs, and management and administrative aspects influence the trustworthiness of technical barrier systems. Sometimes a barrier is deliberately inactivated, or overridden, for example, for performing maintenance, an inspection or a test. So the status of a barriers may differ as Table 1 shows, including related symbols, used as abbreviations in this paper.

Table 1: Possible barrier statuses and associated symbols

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

Trustworthiness of a barrier and risk reduction can be calculated, using a common and generally accepted equation from the IEC (2016) of the unavailability of a barrier as a function of time: $U(t) = 1 - e^{-\lambda t}$, where λ is the barrier failure frequency and t is any moment in time. U(t) is a dimensionless number between 0 and 1, a barrier is 100% trustworthy when the barrier is new. U(t) increases as time progresses. If a barrier is never maintained, inspected and tested, and the time t runs to infinity, U(t) will go to 1, the barrier will fail with 100% certainty when it is needed and/or the barrier will not (correctly) perform its necessary function. The risk reduction RR that can be achieved with the barrier is the reciprocal value of U(t), RR equals $(1 - e^{-\lambda t})^{-1}$. The risk reduction is mostly given as a 10-, 100- or 1000-fold reduction. The risk reduction expressed in logarithm is abbreviated as RRL, where the RRL is equal to $\log(1 - e^{-\lambda t})^{-1}$. In this study the time interval in between each maintenance, inspection and test is defined as T, meaning the barrier is maintained, inspected and tested at T, 2T, 3T, etc. The barrier can be qualified as trustworthy if it is checked no later than the required period T. If it is checked later than the required period T, the RR will decrease below its designed value. Table 2 shows the effect of postponement of maintenance, inspection and testing on the risk reduction RR and the risk reduction expressed in logarithm RRL. Three different values of U(t), meaning 0.1, 0.01 and 0.001, are included in Table 2 for various time intervals. An unavailability of 0.1 means that on average, the barrier is not working in 10% of the demands. Table 2 shows, for example, the effect of a postponed check by half a period to 1.5T. U(t) increases by a factor of 1.5 to resp. 0.15, 0.015 and 0.0015 and the RR decreases by 33%. In this study, it is assumed that a barrier may not be trustworthy if the RR has decreased by 50% or more from the required design value. Table 2 shows that this is the case if a barrier has not been checked (maintained, inspected and tested) for more than a doubled period of T (from 2T upwards).

Table 2: The influence of the time interval on U(t), RR and RRL

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

The status of the barrier system determines the likelihood of the central event against which the barriers should prevent, and is therefore a suitable indicator. The preventive barrier indicator is the quotient of the current RRL and the required RRL. This is also called relative risk reduction expressed in a logarithm: RRRL. $RRRL(t) = [RRL(t) / RRL_{required}] \times 100\%$. Table 3 shows the outcome of the preventive barrier indicator representing the likelihood of the central event in four colours. This likelihood increases as the colour shifts from green to red. The boundaries are evenly distributed in this chapter and are set at 0%, 25%, 50%, 75% and 100%. For each of these classifications, management must determine how to respond and by whom.

Table 3: The colour of the preventive barrier indicator related to the RRRL

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

The preventive barrier indicator, RRRL, can be determined not only from the trustworthiness of the barrier system, but also from its activation and how many barriers still protect against the central event. The calculation of the RRRL can be applied in the same way here: $RRRL(t) = [RRL(t) / RRL_{required}] \times 100\%$, where RRL(t) is the risk reduction expressed in Briggs logarithm of the (remaining) barrier system to the central event. The RRRL shows the current risk reduction compared to what it should be according to design and has thus become a (relative) measure for the loss of quality of the barrier system. Figure 2 shows a barrier system of a total RRL of 3. The barrier system is always located on the left-hand side of the bowtie and consists of preventive barriers. This example represents for instance a high-pressure scenario, which is equipped with a SIL 1 qualified, instrumental safeguard and a (mechanical) safety valve.

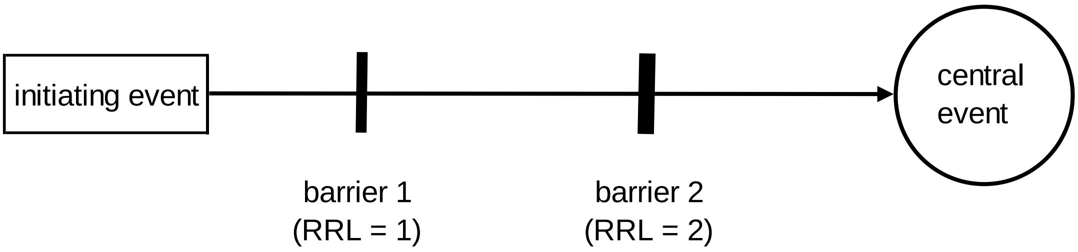


Figure 2: A scenario protected by two independent barriers with an RRL of 1 resp. 2

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

Table 4: Preventive barrier indicator of a barrier system consisting of two barriers with an RRL of 1 resp. 2

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

3 Case study

The ammonia process uses natural gas as a raw material. Gas is cracked to H_2 and combined with N_2 from the air. The synthesis reaction to form ammonia takes place in the presence of a catalyst at approx. 200 bar and 515 °C, the Haber-Bosch process. In the last part of the process the ammonia formed is cooled, separated from the unreacted and inert gases and reduced in pressure, followed by refrigeration to liquify the ammonia.

Post reformer R1 is part of the cracking process, where uncracked natural gas from the reformer is cracked at temperatures, up to 1000°C. The post reformer is equipped with a water jacket that protects the inner wall against too high temperature. The water jacket has open connections on top. As the water jacket is slowly losing its contents, water has to be supplied continuously. A disturbed water flow will raise the wall's temperature, weaken it and finally the wall will collapse under the prevailing process pressure of approx. 37 bar. Process gas will escape, creating a jet fire or explosion. The water in the water jacket comes from the feed water pumps P1A and P1B, one running, and one on a stand-by mode. Pump failure is seen as the most likely cause for failure of the water supply. If both pumps fail, a motor alarm (MA P1) is activated, after which the operator can try and start one of the feed water pumps, start one of the condensate pumps or draw in canal water to feed the water jacket (Figures 3, 4).

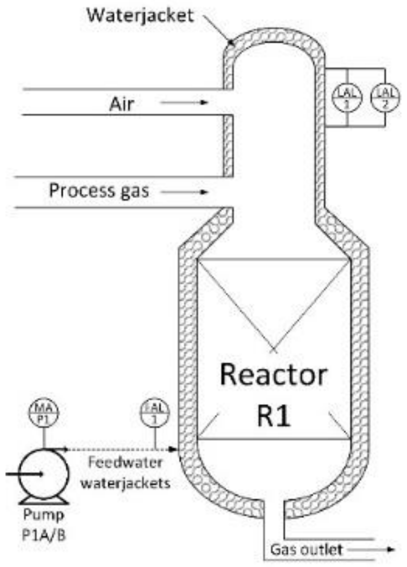


Figure 3: Post reformer R1 and alarms

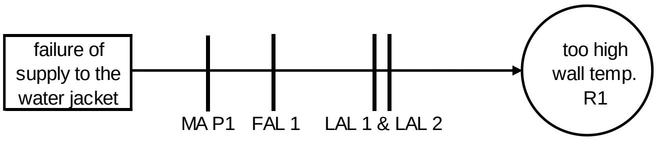
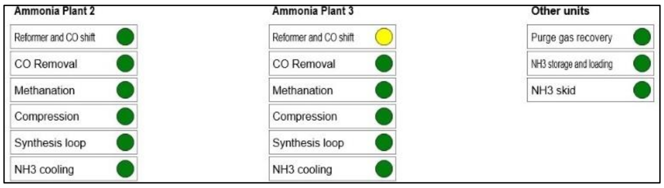


Figure 4: Scenario 'too high wall temperature R1' by failure of the water jacket cooling

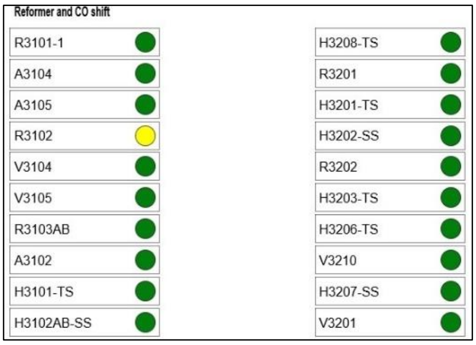
A low water supply to the water jacket is also detected by a low flow alarm (FAL1) that gives the operator enough time to act and to ensure sufficient water supply to the water jacket. This action is identical to the activated alarm MA P1: manual start of the feed water or condensate pumps or the intake of canal water. Also two (low-level) alarms (LAL) installed on the water jacket will be activated if water levels are too low. Although these two identical alarms can be considered as a 1-out of-2 system, they count in the calculation as if they were two separate alarms. In case the low-level alarms have been activated, the operator has some but limited time to identify and recover from the cause. Ultimately it can be decided to shut down the plant. All the operator actions are relatively simple and can be conducted out without much time pressure. All four alarms have a SIL a qualification and an RRL of 0.5. According to specification, the scenario is protected by a barrier system with a total RRL of 2. The status of the preventive barrier indicators is presented in dashboards.

The screenshots below show a detailed process safety dashboard, showing all ammonia production installations (Figure 5), and zooming to the installation with a problematic barrier status (Figure 6), and activated alarms (Figure 7). Installing such a process safety dashboard can provide the control room with real-time information about the status of the barrier system, but it also enables management to view the *status quo* of their production unit at a high level.



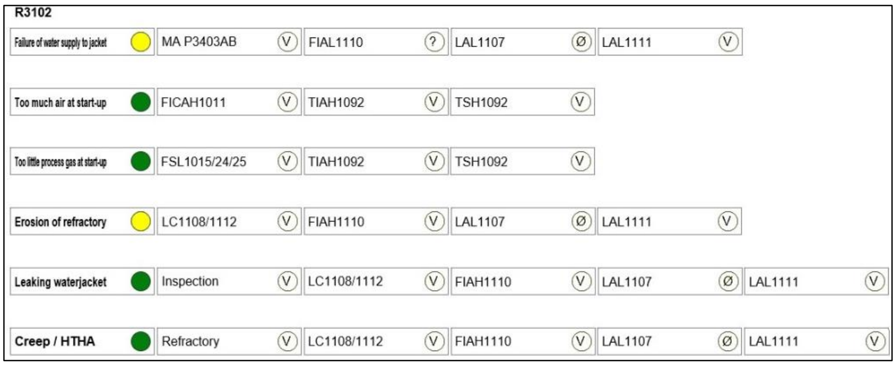
Ammonia Plant 2		Ammonia Plant 3		Other units	
Reformer and CO shift	🟢	Reformer and CO shift	🟡	Purge gas recovery	🟢
CO Removal	🟢	CO Removal	🟢	NH3 storage and loading	🟢
Methanation	🟢	Methanation	🟢	NH3 skid	🟢
Compression	🟢	Compression	🟢		
Synthesis loop	🟢	Synthesis loop	🟢		
NH3 cooling	🟢	NH3 cooling	🟢		

Figure 5: The process safety dashboard



Reformer and CO shift			
R3101-1	🟢	H3208-TS	🟢
A3104	🟢	R3201	🟢
A3105	🟢	H3201-TS	🟢
R3102	🟡	H3202-SS	🟢
V3104	🟢	R3202	🟢
V3105	🟢	H3203-TS	🟢
R3103AB	🟢	H3206-TS	🟢
A3102	🟢	V3210	🟢
H3101-TS	🟢	H3207-SS	🟢
H3102AB-SS	🟢	V3201	🟢

Figure 6: The process safety dashboard of the 'reformer and CO shift' section of ammonia plant



R3102											
Failure of water supply to jacket	🟡	MA P3403AB	Ⓥ	FIAL1110	?	LAL1107	Ø	LAL1111	Ⓥ		
Too much air at start-up	🟢	FICAH1011	Ⓥ	TIAH1092	Ⓥ	TSH1092	Ⓥ				
Too little process gas at start-up	🟢	FSL1015/24/25	Ⓥ	TIAH1092	Ⓥ	TSH1092	Ⓥ				
Erosion of refractory	🟡	LC1108/1112	Ⓥ	FIAH1110	Ⓥ	LAL1107	Ø	LAL1111	Ⓥ		
Leaking waterjacket	🟢	Inspection	Ⓥ	LC1108/1112	Ⓥ	FIAH1110	Ⓥ	LAL1107	Ø	LAL1111	Ⓥ
Creep / HTHA	🟢	Refractory	Ⓥ	LC1108/1112	Ⓥ	FIAH1110	Ⓥ	LAL1107	Ø	LAL1111	Ⓥ

Figure 7:The process safety dashboard of the post reformer with multiple scenarios

4. Discussion

This chapter shows that it is possible to give a qualitative estimate of the likelihood of the central event based on the preventive barrier status. However, the presented model has a few limitations. Barriers usually consist of 3 elements: a sensor, a decision maker, and a final element.

All three must be monitored to determine the status of the (preventive) barrier. In particular, the final element does not always have self-diagnosis, so it cannot be foreseen whether this barrier element is overridden or defective.

If a barrier consists of an alarm, a (safety-critical) instruction and an operator intervention, a similar problem occurs. The trustworthiness of the operator is difficult to measure. Has the operator seen the alarm and understood the problem? Does he/she know how to act? Is he/she not too busy with other tasks? The failure rate regarding operator intervention is usually much higher than the failure rate of sensors. Hence, the reduction of equation $U(t) = 1 - e^{-\lambda t}$ to a widely used, simplified sawtooth of λt can not be applied as λt is not smaller than 0.01. In other words, when applying Table 2 to human intervention, care should be taken

Proper and timely maintenance, inspection and testing may not always guarantee the trustworthiness of barriers. Clearly, maintenance should be performed according to the manufacturer's guidelines and by competent personnel, but that does not mean a 100% safe barrier system. It is recommended to set up a registration system for safety critical equipment that records the findings of its maintenance, inspection and testing.

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

5. Conclusions

A barrier system is defined as a set of existing barriers that must prevent causes from developing into consequences. The barrier system's status can be derived from the parameters reliability/availability and effectiveness. Both parameters are sensitive to change, which is considered as an important indicator criterion. An indicator – called preventive barrier indicator – has been developed from these parameters. From the example the preventive barrier indicator has proven to monitor the level of safety, and enable the operators to decide where and which action is necessary. The preventive barrier indicator shows the development and likelihood of the scenario, which is not an absolute value, but rather an indication of the change in the *status quo* that should initiate further action.

Many incidents did not happen because a process value was extremely out of range, but rather because of a rare combination of deviating values. That is perhaps one of the reasons that the number of major process safety incidents in the process industry is low. It is better to look at the more frequent "precursor" incidents to measure safety (Hopkins, 2009). If the quality parameters of the barriers are incorporated in an automated system, the preventive barrier indicator can be calculated and displayed in real time. This is different for technical changes which are not automatically notified as they will have to be entered manually. A future validation, performed through retrospective research based on several (near) incidents, will have to show to what extent the preventive barrier indicator provides timely insight into the likelihood and development of the accident scenarios. Further research is needed to design indicators at other levels that can provide information on major accident processes, starting with the management delivery system as the first higher aggregation level.

References

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

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

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

Schmitz, P. (2020). Preventing major hazard accidents through barrier performance. Doctoral thesis, Delft University of Technology, https://repository.tudelft.nl/islandora/object/uuid%3A782fcd3e-0db4-42ee-965a-c180586759f4.

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

Swuste, P., Nunen, K. van., Schmitz, P., Reniers, G. (2019). Process safety indicators, how solid is the concept Chemical Engineering Transactions 77, 85-90.

Visser K., (1998). Developments in HSE management in oil and gas exploration and production, in: Hale A.,Baram M., (Eds.). Safety management, the challenge of change, p. 43-66. Pergamon, Amsterdam.