CHEMICAL ENGINEERING TRANSACTIONS
VOL. 86, 2021
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Sauro Pierucci, Jiří Jaromír Klemeš

ISBN 978-88-95608-84-6; **ISSN** 2283-9216
DOI: 10.3303/CET2186045

Dynamic Risk Analysis from the Perspective of Life Cycle Approach in IEC 61508 and IEC 61511

Shenae Lee[a],* Mary Ann Lundteigen[b], Nicola Paltrinieri[a]

[a]Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, Trondheim, Norway
[b] Department of Engineering Cybernetics, Norwegian University of Science and Technology, Trondheim, Norway
shenae.lee@ntnu.no

Dynamic risk analysis (DRA) aims to provide updated risk levels during operations of a hazardous facility. One of the main objectives of performing a DRA is to support day-to-day operational decisions, primarily for preventing major accidents. For this reason, many DRA methods have been developed to include information about the status of the safety barriers whose failures can increase the likelihood of a major accident. However, DRA is not widely used in industry, and there is no standard that describes DRA approaches and their applications. It may therefore be of interest to consider similar concepts and methods addressed in the existing standards. This paper focuses on a specific type of safety barriers, safety instrumented systems (SISs), and recognized functional standards IEC 61508 and IEC 61511 that give performance requirements to a SIS. In particular, SIS performance monitoring in the operational phase according to IEC 61508/61511 can provide valuable inputs to DRA applications.

1. Introduction

Experience of process accidents such as the explosion at the Buncefield oil depot in 2005 (HSE, 2005) and the blowout on the Deepwater Horizon drilling rig in 2010 (BP, 2010) increased the focus on risk and safety management of hazardous processing facilities. EU Directive on safety of offshore oil and gas operations (EU, 2013), introduced as a response to the Deepwater Horizon accident, requires the use of risk analysis as a basis to achieve an acceptable level of major accident risks throughout all the life-cycle phases of offshore installations. In the design phase of an offshore facility, risk analyses primarily aim to support decisions related to design issues and operating procedures. An example of such an analysis is quantitative risk analysis (QRA) for Norwegian offshore facilities (Vatn and Haugen, 2013), and a facility QRA is suited to estimate the long-term average risk for a specific installation, typically averaged per year (Yang and Haugen, 2015).
On the other hand, the risk level can change with time in the operational phase due to the different activities and decisions that can affect the facility's risk level (Hauge et al., 2015). In terms of supporting day-to-day operational decisions with short-term risk effect, averaging risk over a long period is not relevant, and in practical cases, the use of the facility QRA is limited. Such operational decisions may be supported by qualitative methods (e.g. job safety analysis) (Yang and Haugen, 2016), but these types of studies have a weak link to the facility's overall risk picture (Vatn and Haugen, 2013). In addition, qualitative studies may not be suitable for judging the risk tolerability in complex risk management situations, and in these cases, a quantitative analysis is useful for decision-making (Oil and Gas UK, 2012). For this reason, the focus has been given to provide a better quantitative basis for risk management during the operational phase, and this includes developing improved risk models that can quantify the relative change in the major hazard risk in real-time (Haugen and Edwin, 2017). This is in line with Dynamic risk analysis (DRA) methods aimed at updating the risk picture when needed, as opposed to traditional QRAs that are updated infrequently (e.g. every five years) (Paltrinieri and Khan, 2020).
Many of DRA methods and models have been developed to update the risk level in the period of interest or to predict future risk based on accident precursors (Lee et al., 2019). An example of DRA method is the Risk Barometer approach (RB), aimed at real-time monitoring of risk level during the day-to-day operation of an

Paper Received: 13 August 2020; Revised: 8 March 2021; Accepted: 30 April 2021
Please cite this article as: Lee S., Lundteigen M.A., Paltrinieri N., 2021, Dynamic Risk Analysis from the Perspective of Life Cycle Approach in Iec 61508 and Iec 61511, Chemical Engineering Transactions, 86, 265-270 DOI:10.3303/CET2186045

offshore installation. RB can quantify the change in the risk level by using a set of indicators that can measure the status of critical barriers (Hauge et al., 2015). However, most of DRA methodologies are ongoing studies, and no standard and tools for the application of DRAs exist (Paltrinieri and Reniers, 2017). Therefore, it can be of interest to understand concepts and methods related to DRA in the existing standards. For example, ISO 31000 (ISO 31000, 2018) states that effective risk management should adapt to risk changes. NORSOK Z-013 (NORSOK, 2010) specifies the need for updating the existing QRAs based on operational experiences. Such requirements pertain to updating of risk analysis for reflecting significant modifications or major changes to the organization (Paltrinieri and Khan, 2016).
On the other hand, functional safety standards IEC 61508 (IEC 61508, 2010) and IEC 61511 (IEC 61511, 2016) uses the safety life-cycle concept to achieve a risk-based level of safety in all the operating phases of a safety instrumented system (SIS) (Rausand, 2014). SISs are based on electrical, electronic, and/or programmable electronics (E/E/PE) technology, and they are an important sub-type of safety barriers at a facility. According to the safety life-cycle approach in IEC 61508/61511, performance requirements for a SIS are determined in design, and the actual performance of the SIS is monitored during operations. This paper highlights the potential to integrate information from SIS performance monitoring into DRAs, in order to update the risk level in real-time and improve day-to-day decision support.

2. Safety integrity in IEC 61508 and IEC 61511

2.1 Risk-based performance requirement for a SIF

A safety instrumented system (SIS) consists of input elements (e.g. sensors), logic solvers, and final elements (e.g. safety valve) (Rausand, 2014). A SIS is intended to respond to a specific process demand and to bring the process back to a safe state. The safety function performed by a SIS is called safety instrumented functions (SIF). General principles for specifying the performance requirements to a SIS are described in the standard IEC 61508, and IEC 61511 is the standard for specific applications of IEC 61508 for the process sectors.
According to IEC 61511, the required SIFs are determined based on a hazard and risk analysis. A process risk is defined as a reference point risk arising from abnormal events in a specified process system and its basic process control system (BPCS) without considering any safety barriers. The risk may be defined in relation to a specific hazardous event (e.g. process leak), and a typical tolerability criterion is its maximum frequency per year. In such a case, the difference between the estimated frequency and the target frequency is the necessary risk reduction that may be allocated to SIS and non-SIS barriers, as illustrated in Figure 1.

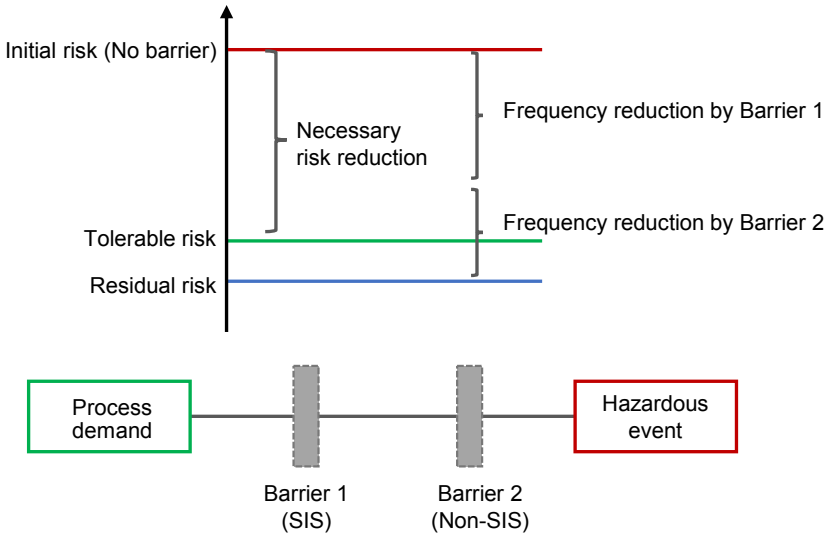

Figure 1: The risk reduction of frequency-reducing barriers against a specific process demand.

The risk reduction (e.g. frequency reduction) allocated to a SIS is achieved by its associated SIFs, and the amount of the risk reduction provided by a SIF is its reliability target. The most commonly used reliability measure for a SIF operated on a low demanded mode (e.g. demand for the SIF is less than once per year) is the average probability of failure on demand (PFD) (Rausand, 2014). IEC 61508 uses safety integrity level (SILs) to give a target PFD range. SILs are divided into four levels, from SIL 1 to SIL 4. A SIF with SIL 1 is the

least reliable and, and a SIF with SIL 4 is the most reliable. If the PFD value is lower than 10^{-1}, but not less than 10^{-2} and, it corresponds to SIL1. If the PFD is lower than 10^{-2} but not less than 10^{-3}, it corresponds to SIL 2 (IEC 61508, 2010).
According to IEC 61511, a layer of protection analysis (LOPA) is one of the methods used to decide if SISs are needed as barriers in relation to process deviations. In a LOPA study, possible initiating events (e.g. abnormal high pressure) and the associated accident scenarios are identified. Several scenarios may give rise to the same end event (e.g. a vessel rupture due to overpressure). The end event with no significant consequences will be excluded from the analysis (Rausand, 2011). For each scenario, its frequency is calculated by multiplying the frequency of the initiating event and the PFD of the barriers. The sum of a specified end event can then be the sum of the frequencies of all the scenarios that result in this event. If the estimated frequency of a specific end event is higher than the tolerable frequency, implementing a SIF is one option for risk reduction. The SIL of the SIF can be determined from the amount of risk reduction required.

2.2 SIS life-cycle phases

In IEC 61508, the safety life cycle concept is used to maintain the required performance of a SIS throughout all the operating phases. The life cycle is a sequence of 16 phases that includes hazard and risk analysis, planning, design, development, installation, operation, maintenance, and decommissioning. Risk assessment (phase 1-5) will define what a SIS is required to do and its SIL target. These requirements and the relevant assumptions will be documented in the safety requirements specification (SRS) (Lundteigen, 2009). The SRS provides a basis for design, but it should be updated during operation to reflect major changes to assumptions such as new SIL requirements and updated failure rates (NOGA, 2004).
In SIS operating phases, SIS follow-up activities such as testing and maintenance, performance monitoring, and modification are carried out to assure compliance to the SRS. Hauge and Lundteigen (2008) demonstrate how the SIL target can be verified during operation on the basis of performance indicators for SIS components. A suitable indicator can be the number of observed dangerous undetected (DU) failures of identical components during an observation period. The number of observed DU failures can be compared with the target value (e.g. two per year) to check the validity of the PFD estimate obtained in design. The target number can be calculated from the generic failure rate that is used to predict the PFD. If the number of DU failures for the studied component exceeds the target value, a failure cause analysis is required. Furthermore, measures to reduce the number of failures should be considered, for instance, shortening the test interval. If, on the other hand, the number of failures is below the target, extending the test interval may be considered, as illustrated in Figure 2 (Lundteigen and Hauge, 2008).

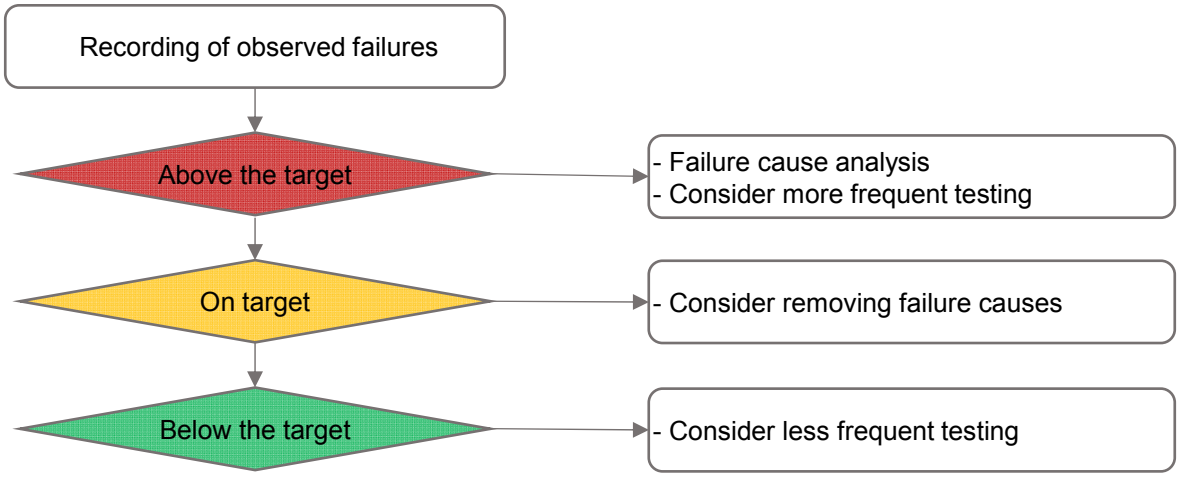

Figure 2: An example on how to use a performance indicator (e.g. observed number of DU failures) for verifying SIL requirements in the operational phase. Adapted from (Hauge et al., 2008).

2.3 Implication for dynamic risk analysis and barrier management

IEC 61508 and IEC 61511 address performance requirements for SISs in different operating phases, but non-SIS barriers are not covered by these standards, and the management of functional safety of a SIS can be considered as a subset of barrier management (NOGA, 2004). The purpose of barrier management is to maintain the desired barrier performance over the facility's lifetime in achieving the required risk reduction (PSAN, 2017). Øien et al. (2015) affirm that SIL management needs to be integrated into barrier management,

and barrier management activities should be in principle linked to the risk management process. However, barrier management tends to focus on the status of individual barriers, but not the overall risk level. It may therefore be necessary to develop DRA methods and models that can consider risk-inducing activities and conditions at the plant, together with the information from barrier management and the existing QRAs (Haugen and Edwin, 2017).

In addition, it may be useful to specify the requirements to how often barrier status information should be updated, taking into account the use of a DRA method. Hauge et al. (2015) address that DRA can be categorized into three different levels with respect to how often the analysis is updated. The first type is a DRA updated in months and years, which means reliability parameters are updated based on activities like analyses, surveys, interviews. The benefit from such activities is to gain insights on root causes, safety culture, and additional information from historical data (Øien, 2001). The second type is a DRA that is updated on a daily and weekly basis. The strength of this approach is the capability for measuring the changes in risk in the period of interest. The last type is a DRA updated in the range of minutes and hours, such that instantaneous information such as process parameters and weather conditions are used to update the risk picture.

An example of reliability parameters updated on a less frequent basis is DU failure rate and PFD of a SIS. They are recalculated based on new information obtained from testing campaigns that may be carried out, for example, once per year. For this reason, the result of SIS performance monitoring with respect to DU failures can be inputs for a DRA updated on a yearly basis. On the other hand, SIS provides diagnostic alarms for dangerous detected (DD) failures, which is real-time information about the current status of SIS barrier functions. Such information can be inputs for a DRA updated on a daily basis, together with other risk influencing factors at the plant.

3. Case study

This case study briefly illustrates how SIS performance monitoring may provide input to DRA applications, using a bulk oil storage tank as an example. Overfilling of an atmospheric storage tank containing hazardous substances (e.g. flammable liquids) may lead to a major accident. An example of such an accident is the vapor cloud explosion (VCE) at Buncefield oil depot in 2005, which was caused by the gasoline release from an overfilled tank. The release gave rise to the spreading of the vapor cloud and generated a VCE. The overflowed tank was equipped with barriers to prevent a tank overfill, including an automatic gauging system (ATG), level alarms, and an independent high-level switch (IHLS). On the day of the Buncefield accident, the ATG stopped registering the tank's rising level during the receipt of the fuel. Subsequently, the tank level reached above an abnormally high level, but the alarms were not triggered. The IHLS, a mechanical switch, did not activate the shutdown, and the tank exceeded its maximum capacity, resulting in the loss of containment (i.e. petrol releases) (HSE, 2005). Typical event sequences to a tank overfill or a release are shown in the simple barrier block diagram in Figure 3.

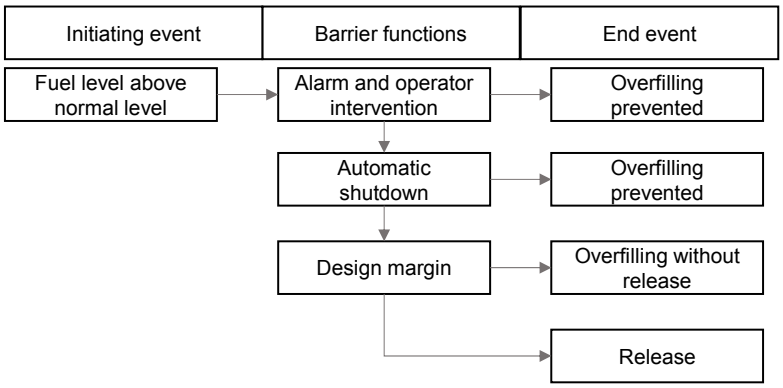

Figure 3. A barrier block diagram for release from the tank due to overfilling.

In response to the Buncefield accident, a number of recommendations were made for improving the safety in a Buncefield-like facility. This includes SIS applications for automatic overfill protection systems (AOPS) and the systematic assessment of SIL requirements for such an AOPS according to IEC 61511 (MIIB, 2008). In light of this, this case study focuses on an AOPS that is a SIS, which is a key barrier to prevent tank overfills. An AOPS is designed to automatically shut down the fuel inflow upon a critical high level, and it consists of

level sensors, logic solvers, and final elements such as shut-off valves (API 2350, 2020). To determine the SIL requirements for an AOPS within the scope of IEC 61511, a LOPA is a suitable risk assessment method (PSLG, 2009). As explained in section 2.1, various accident scenarios with significant consequences are considered in a LOPA. An example of such a scenario in a storage tank is an event sequence where the initiating event 'the failure of the ATG' results in the end event 'VCE' (Chambers et al., 2009).
A LOPA can be used in the design phase of a new tank to determine the reliability target for the AOPS. For an existing tank in operation, a LOPA can be performed in conjunction with a hazard and operability (HAZOP) review or revalidation (Rausand, 2011). This may imply that a LOPA can be updated to reflect new knowledge about potential accidents and to ensure that all the relevant accident scenarios are included. For this reason, it may be relevant to apply DRA methods that are suited to update the hazard identification process. One such method is Dynamic Procedure for Atypical Scenario Identification (DyPASI). DyPASI is suited to discover new scenarios based on new accident data, early warnings, and other relevant knowledge (Paltrinieri et al., 2012).
On the other hand, SIL verification for the AOPS during operation can trigger updating of the frequency calculation in the LOPA. For instance, the elements of an AOPS, such as level sensors and the shut-off valves, are proof-tested at regular intervals (PSLG, 2009). New information from the periodic tests will be used as important inputs to recalculate the PFD and, accordingly, the frequency of a specific end event in the LOPA. It may be noted that updating of LOPA by using DyPASI method or updating PFD can be understood as a DRA updated on a less frequent basis, as mentioned in section 2.3.
Finally, information from daily monitoring of the AOPS can be used as input for a DRA that is updated on a day-to-day basis. Examples of such information are diagnostic alarms raised due to the DD failures in level sensors and the inhibition of an input signal from a sensor. They are relevant input for DRA aimed at monitoring day-to-day changes in the risk level. DRA applications and SIS performance monitoring can provide additional information to the existing LOPA, as illustrated in Figure 4.

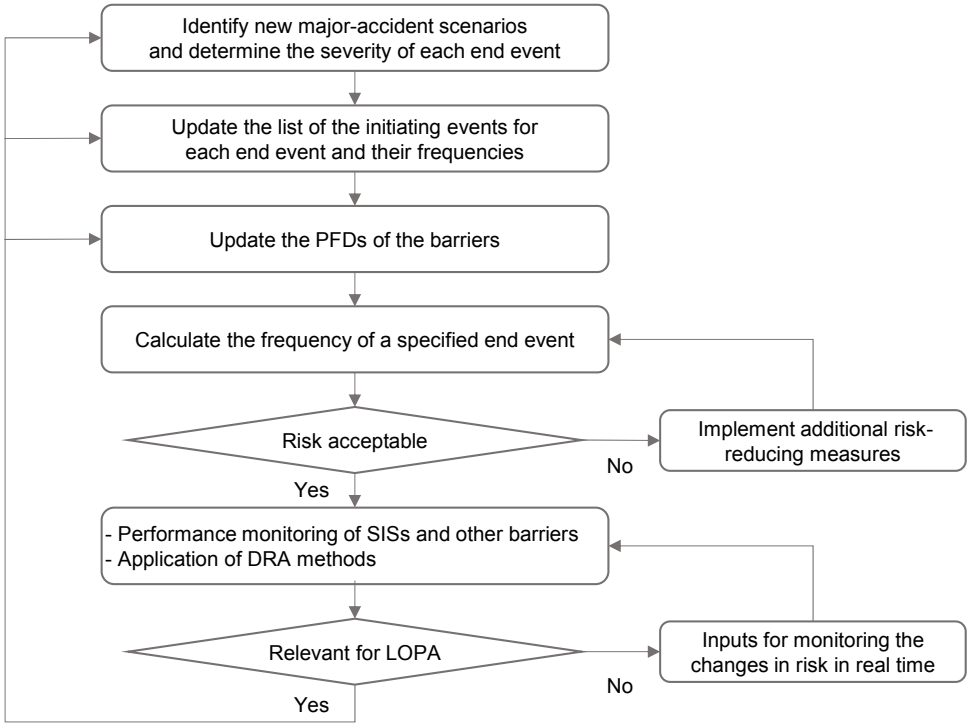

Figure 4: LOPA and performance monitoring of SISs during the operational phase

4. Conclusion

This paper highlights how to incorporate the information from performance monitoring of SIS into DRA applications. Updated information about SIS performance with respect to DU failures can be inputs for the DRAs updated on a less frequent basis. On the other hand, daily monitoring of SIS status gives immediate new information about an existing degradation of the SIS. Such information is valuable inputs to DRA methods aimed at supporting day-to-day operational decisions.

References

API 2350, 2020. Overfill Protection for Storage Tanks in Petroleum Facilities, 5th edition. Washington, DC.
BP, 2010. Deepwater Horizon Accident Investigation Report, Internal BP Report.
Chambers, C., Wilday, J., Turner, S., 2009. A review of Layers of Protection Analysis (LOPA) analyses of overfill of fuel storage tanks, Report on the Internet.
EU, 2013. Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on safety of offshore oil and gas operations and amending Directive 2004/35/EC Text with EEA relevance. Official Journal of the European Union, L178/66.
Hauge, S., Lundteigen, M.A., 2008. Guidelines for follow-up of safety-instrumented systems (SIS) in the operating phase.
Hauge, S., Lundteigen, M.A., Onshus, T., Bodsberg, L., 2008. Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase PDS -multiclient Safety Sikkerhet Operation Drift, SINTEF.
Hauge, S., Okstad, E., Paltrinieri, N., Edwin, N., Vatn, J., Bodsberg, L., 2015. Handbook for monitoring of barrier status and associated risk in the operational phase. SINTEF F27045. Center for Integrated Operations in the Petroleum Industry, Trondheim, Norway , Norway.
Haugen, S., Edwin, N.J., 2017. Dynamic risk analysis for operational decision support. EURO J. Decis. Process. 5, 41–63. https://doi.org/10.1007/s40070-017-0067-y
HSE, 2005. Buncefield: Why did it happen? Control Major Accid. Hazards 36.
IEC 61508, 2010. IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.
IEC 61511, 2016. Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Part 1-3., 2.1. ed. International Electrotechnical Commission, Geneva.
ISO 31000, 2018. Risk Management. ISO 31000:2018.
Lee, S., Landucci, G., Reniers, G., Paltrinieri, N., 2019. Validation of dynamic risk analysis supporting integrated operations across systems. Sustain. https://doi.org/10.3390/su11236745
Lundteigen, M.A., 2009. Safety instrumented systems in the oil and gas industry: Concepts and methods for safety and reliability assessments in design and operation.
Lundteigen, M.A., Hauge, S., 2008. A new approach for follow-up of safety instrumented systems in the oil and gas industry, in: Safety, Reliability and Risk Analysis : Theory, Methods and Applications : Proceedings of the European Safety and Reliability Conference, ESREL 2008.
MIIB, 2008. The Buncefield Incident 11 December 2005, Volume 2.
NOGA, 2004. 070 – Norwegian Oil and Gas Application of Iec 61508 and Iec 61511 in the Norwegian Petroleum.
NORSOK, 2010. Risk and emergency preparedness assessment. Z-013. Oslo, norway, Norway.
Øien, K., 2001. Risk indicators as a tool for risk control. Reliab. Eng. Syst. Saf. https://doi.org/10.1016/S0951-8320(01)00067-9
Øien, K., Hauge, S., Størseth, F., Tinmannsvik, R., 2015. Towards a holistic approach for barrier. https://doi.org/SINTEF A26845
Oil and Gas UK, 2012. Guidance on the Conduct and Management of Operational Risk Assessment for UKCS Offshore Oil and Gas Operations Issue 1. Oil Gas UK.
Paltrinieri, N., Dechy, N., Salzano, E., Wardman, M., Cozzani, V., 2012. Lessons Learned from Toulouse and Buncefield Disasters: From Risk Analysis Failures to the Identification of Atypical Scenarios Through a Better Knowledge Management. Risk Anal. 32. https://doi.org/10.1111/j.1539-6924.2011.01749.x
Paltrinieri, N., Khan, F., 2016. Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application, 1st ed. Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-803765-2.01001-5
Paltrinieri, N., Khan, F.I., 2020. Dynamic risk analysis—Fundamentals, in: Methods in Chemical Process Safety. Elsevier, pp. 35–60. https://doi.org/10.1016/bs.mcps.2020.04.001
Paltrinieri, N., Reniers, G., 2017. Dynamic risk analysis for Seveso sites. J. Loss Prev. Process Ind. 49. https://doi.org/10.1016/j.jlp.2017.03.023
PSAN, 2017. Barrier Memorandum.
PSLG, 2009. Safety and environmental standards for fuel storage sites, Health and Safety Executive.
Rausand, M., 2014. Reliability of Safety-Critical Systems, Wiley. Wiley, Hoboken,NJ.
Rausand, M., 2011. Risk assessment - theory, methods and applications, Statistics in practice. Wiley, Hoboken,NJ.
Vatn, J., Haugen, S., 2013. On the usefulness of risk analysis in the light of deepwater horizon and Gullfaks C, in: Oil and Gas, Technology and Humans: Assessing the Human Factors of Technological Change.
Yang, X., Haugen, S., 2016. Risk information for operational decision-making in the offshore oil and gas industry. Saf. Sci. https://doi.org/10.1016/j.ssci.2016.02.022
Yang, X., Haugen, S., 2015. Classification of risk to support decision-making in hazardous processes. Saf. Sci. 80, 115–126. https://doi.org/10.1016/j.ssci.2015.07.011