

# Digital Twin Concept for Risk Analysis of Oil Storage Tanks in Operations: a Systems Engineering Approach

Shenae Lee<sup>a,b\*</sup>, Cecilia Haskins<sup>b</sup>, Nicola Paltrinieri<sup>b</sup>

<sup>a</sup> Dept. of Software Engineering, Safety and Security, SINTEF Digital, Trondheim, Norway

<sup>b</sup> Dept. of Mechanical and industrial engineering, NTNU, Trondheim, Norway

[Shenae.lee@ntnu.no](mailto:Shenae.lee@ntnu.no)

This paper presents an approach to develop a risk monitoring tool for oil storage facilities. The suggested approach is derived from the existing dynamic risk analysis (DRA) methods and the digital twin concepts. One of the main challenges in practical applications of DRA methods is insufficient amount of relevant data, and it seems that digital twin models can overcome this challenge by offering increased availability of real-time data. It can be interesting to judge if their combination can provide the intended advantages with a structured and more holistic viewpoint. Therefore, this paper demonstrates how a representative systems engineering (SE) methodology may be used to facilitate the process of developing an improved risk monitoring tool.

## 1. Introduction

Recent history of accidents resulting from the operations of bulk oil storage facilities such as the vapor cloud explosion (VCE) in Buncefield oil depot (2005) (MIIB, 2008), the explosion in Bayamon terminal (2009), and the VCE in Jaipur (2009) (Sharma et al., 2013) motivate the need to prevent similar accidents. Oil storage facilities handling a large amount of dangerous substances such as gasoline, diesel, and gas oil pose risks arising from unpredicted releases (European commission, 2008). Such a release can result in a severe accident that may harm workers, the residents around the site, and the environment. Moreover, the volume of materials to be stored and transported in an oil depot can change depending on the market demands, while the storage capacity of the existing tanks remains limited (Fernandes et al., 2013). It is therefore important to carry out tank operations in an affordable way, while maintaining the focus on the safety and risk management (Bubbico et al., 2020).

Onshore processing plants and storage facilities in Europe where hazardous materials are present in quantities above a certain threshold are defined as Seveso sites (EU, 2012). The operating company of a Seveso site has a general obligation to implement necessary measures to prevent major accidents, which includes establishing an adequate safety management system. The safety management system can be understood as a part of risk control during the operations, and it includes procedures for the identification of major hazards arising from normal and abnormal operations, operational control (e.g. procedure for safe operation and maintenance), and monitoring of safety performance (e.g. follow-up of near-misses). However, risk assessments performed in the design phase are not fully adequate for capturing all these aspects, because they are suited for providing the average risk at the facility or a static risk picture (Yang et al., 2018). This implies the need for more suitable risk analysis methods to update the risk picture, which are often referred to as dynamic risk analysis (DRA) in the process industry (Paltrinieri and Reniers, 2017).

Examples of DRA methods are organizational risk influence model (ORIM) (Øien and Sklet, 2001) and the risk modelling through integration of organizational, human and technical factors (Risk-OMT) (Gran et al., 2012). The latter focus on updating important quantitative risk analysis (QRA) parameters (e.g. leak frequencies), which they developed primarily for the Norwegian offshore industry. The Risk-OMT model can be used to calculate and periodically update the frequency of specified hydrocarbon release scenarios during the operational phase of an installation. The model establishes quantitative relationships between the failure probabilities of operational barriers and the installation-specific factors that can affect the barrier performance.

The states of the factors are measured by the associated indicators. However, one of the challenges of using these methods was the increased efforts for data collection and analysis.

More recently, a DRA method denoted as Risk Barometer (RB), was developed as a pragmatic approach for updating risk analysis on daily basis, using the data that can be retrieved from existing information management systems (e.g. maintenance management) (Paltrinieri and Haskins, 2018). However, the RB uses simple risk models that may not include detailed causal factors for changes in risk level. Another limitation was found to be an insufficient availability of the needed quantity of real-time data about safety barriers to support analysis (Hauge et al., 2015). Nonetheless, it seems that improvements against these practical limitations of current DRA methods can be made, by means of the digital twin concept (Pasman, 2020). Digital twin models can offer the increased availability of real-time data from the systems and the possibility of using data-driven models as a part of risk analyses (Paltrinieri et al., 2019).

As a digital replica of physical systems, a digital twin should be updated in real-time by collecting and processing the large amount of sensor data related to the system, and its external environment. Real time synchronization between the digital model and physical system is enabled by the internet of thing (IoT). A digital twin can predict the future behaviours of the system using different what-if scenarios, with no adverse impact on its physical counterpart (Rasheed et al., 2020). Digital twins can be used for supporting a variety of decisions at any life cycle phase of a system. In the operational phase, decisions regarding maintenance may be based on the information from digital twins, for instance, current technical condition of an item and its remaining useful life (Boschert and Rosen, 2016).

Therefore, it follows that the information from digital twins can supplement existing risk analyses for major hazard facilities by providing a more real-time and dynamic risk picture (DNV GL, 2018). Furthermore, it is important that digital twin models are customized for improved decision support in safety and risk management (Lee et al., 2019). However, both DRA and digital twin concepts are relatively new in risk analysis, and it may be of great interest to judge their practical benefits in a structured way. The main objective of this paper is to address heterogeneous aspects of combining digital twin concepts with a DRA, using a systems engineering (SE) methodology. A simple case study of oil storage facilities is used for illustration.

## **2. A representative SE methodology**

Systems engineering (SE) is defined as a transdisciplinary and integrative approach to enable the successful realization, use, and retirement of engineered systems using systems principles and concepts, and scientific, technological and management methods (INCOSE, 2018). A SE methodology called SPADE, proposed by Haskins (2008), is catered for the application of SE principles through executing a set of five essential SE activities: Stakeholder identification, Problem formulation, Alternatives and analysis, Decision-making and Evaluation. Each task can be accomplished by using a set of relevant models and methods. The ordering of the acronym SPADE reflects the logical sequence of performing these activities. A stakeholder is defined as any individual or organization with a legitimate interest in the safety and risk management of the site, and the stakeholders' need should be continuously validated (Haskins et al., 2011). For example, new requirements from a stakeholder influence the problem definition. According to the framed problem, suitable alternative solutions to the problems should be considered and analyzed for feasibility and risk mitigation. The analysis results provide a basis for decision-making. Evaluation is a continuous activity that is conducted to judge if the requirements for these tasks are fulfilled, such that any of these four activities are iterated whenever better information becomes available.

## **3. Case study**

This case study illustrates how the SPADE methodology may be applied to in a hypothetical situation where an improved risk monitoring tool is developed for Buncefield-type oil storage sites located in Europe that fall under the upper-tier establishment under the scope of the Seveso directive. The accident at the Buncefield oil depot in December 2005 have created a number of recommendations for improving safety in Buncefield-type oil storage sites, with the emphasis on strengthening the performance of safety barriers and risk control. Typically, an oil depot consists of atmospheric storage tanks, loading facilities for product dispatch by road tankers, and unloading facilities for ships. According to European Commission (2008), the technical complexity of storage facilities is relatively low and technical options are limited, compared to other types of Seveso sites in the petrochemical industry. For this reason, the activities in the oil depot can easily be standardized, which implies that these sites can possibility agree upon necessary means for controlling major hazard risks.

**3.1 Stakeholders and problems**

Aven and Renn (2012) state that a stakeholder is any individual, group or organization that may affect or be affected by decisions. The stakeholders have strategies and plans for meeting their visions and goals, which reflect the stakeholders' values. The relevant stakeholders involved in improving risk monitoring tools have the shared interest of preventing major accidents, for example, the regulatory authorities, the company management, risk analysts (safety and risk management). The regulatory authority is responsible for the implementing the Seveso directive in a country (e.g. Health and safety executive in England), and their interest is basically to ensure that the level of protection against major hazards remain constant or increase during the entire lifetime of the Seveso site. At a fairly high level, the safety management system is intended to provide continuous risk monitoring and safety improvement. The company management allocates resources into different management areas in the company and ensures that the company complies with the regulations and laws, including the Seveso directive. The management may determine a tolerable level of risk and safety targets based on company values, budget, and various factors. Risk analysts are the main actors who develop a risk monitoring tool, and the problem is further refined by eliciting their needs by using the following questions:

-What are you trying to do? Answer: To develop a tool to monitor risk during operations of oil storage facilities, which can be used for planning purposes on a daily basis.

-What is the problem? How is it done today? Answer: DRA methods that are suited for updating the risk picture may be a good basis for developing a risk monitoring approach. A DRA approach may be differentiated based on the input data for the analysis. On one hand, an analysis may focus on incorporating data directly related to past experiences with the studied systems, for instance, past incidents and failure recordings from the systems. Historical data can be used as suitable input for updating the probability estimates for potential accidents(Khakzad et al., 2014).On the other hand, an analysis may focus on deriving possible risk changes from risk indicators (Landucci and Paltrinieri, 2018). If risk indicators can be measured based on real-time data, the risk level can be updated in real time. In this regard, a risk monitoring approach called Risk Barometer (RB) is developed to reflect the changes in risk by means of indicators that provide information on a daily status of safety barriers.

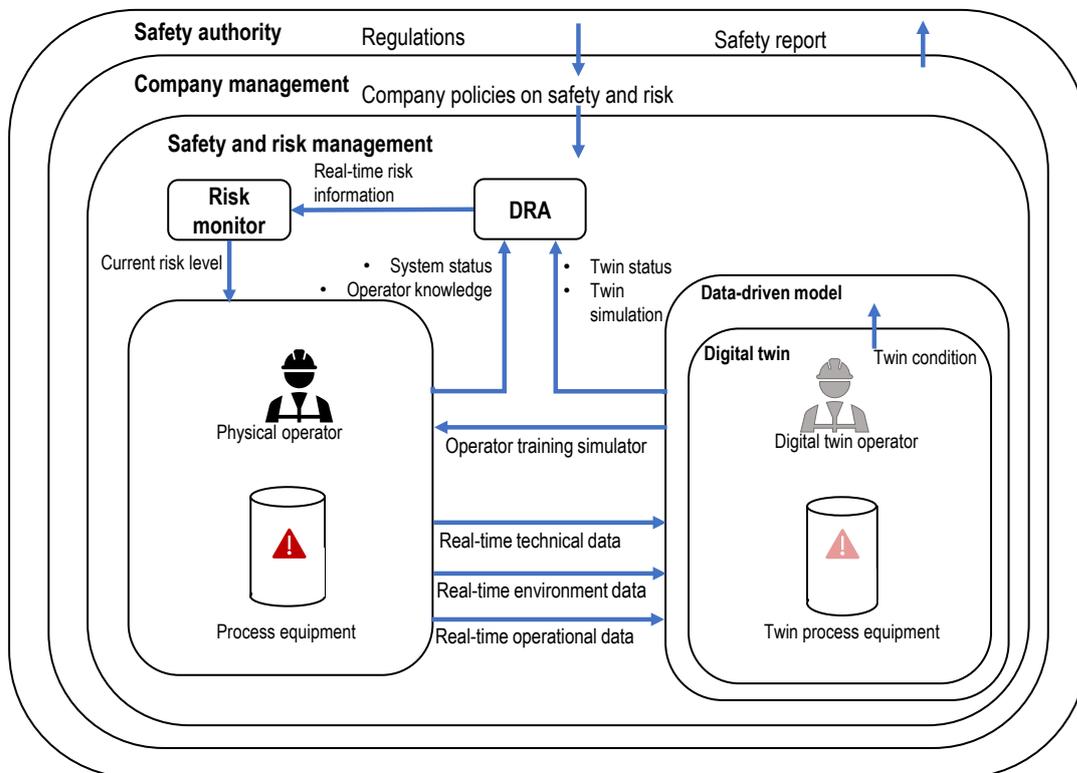


Figure 1: Context diagram for the use of digital twin and DRA in the operations phase of a tank filling operation.

-What is new in your approach and why do you think it will be successful? Answer: The updating frequency of the RB approach is currently in the range of days and weeks, and one reason for this is insufficient amount of relevant instantaneous information about the barrier status. Thus, the combination of RB and digital twin concepts are proposed, where digital twins can collect a large amount of real-time data from system. In addition, digital twins can offer simulations, which can be used as part of the risk analysis. Testing digital twin concepts seem to be relatively easier for Buncefield-type oil storage sites, due to the low technical complexity and standardized operational activities in the storage sites. In addition, various what-if analyses can be simulated by digital twin models to predict the risk impact of operational and maintenance activities without perturbing those activities. Moreover, the implementation of digital twins can possibly allow for remotely monitoring real-time data about the system and for inspecting the systems in the offshore industry (Herrera, 2018). If a similar concept is implemented for the onshore oil storage facilities, it can facilitate remote participation of third parties in operation and maintenance. For instance, after the Buncefield accident, it was recommended that third parties verify the tank dips prior to transfer of fuel (PSLG, 2009).

### 3.2 Analysis

Once the stakeholders and problem formulation activities are underway, it is possible to define the system boundary and visualize it by the simplified context diagram as shown in the figure 1. The arrows are used to indicate information flow between the elements. After the system boundary is established, the models and methods for analysis activities can be chosen. According to Haskins et al. (2011) models can be based on two approaches: representations and simulations. A representation model uses some mathematical rules to express the logical dependence between system elements, but do not necessarily mimic the physical system structure. Simulations mimic the detailed physical phenomena, composing components that are connected as in the real system. For this case study, simulations may be executed by the digital twin models for critical barriers for a storage tank. For example, digital twin model for maintenance can be updated in real time by utilizing the instantaneous information (e.g. degradation level of a barrier) that are collected automatically (Lee et al., 2019).

On the other hand, representations models can be established by using the Risk Barometer (RB) methodology. The RB proposes seven steps for developing risk models that are suited to capture the changes in risk, which includes definition of hazardous events and accident scenarios, identifying the relevant barrier functions, establishing barrier performance indicators, and developing an underlying risk model based on barrier indicators (Hauge et al., 2015). For this case study, the hazardous event to be analysed is the overfilling of an atmospheric storage tank, which may contribute significantly to the risk of an oil depot (PSLG, 2009). Then, the underlying risk model can be developed to establish the logical dependency between the barrier performance indicators and the probability of the specified hazardous event. The barrier relevant to the hazardous event can be identified in light of Buncefield accident in 2005 (MIIB, 2008).

On the day of Buncefield accident, unleaded petrol was transferred from an oil refinery to the Buncefield oil storage, and the level of tank 912 continued to rise, exceeding the maximum capacity of the tank. The overfilling of the tank led to a large vapor release which escalated to a VCE (HSE, 2005). Abnormal tank level may be caused by the unplanned increase of flow rate or incorrect valve line-up before the tank fill operation (PSLG, 2009). To control the inflow and to prevent an abnormally high tank level, various safety barriers are used. Primarily, automatic gauging system continuously monitor the level to maintain the normal operating level and to notify if the level deviates from this pre-set normal level by raising the 'alarm abnormal level'. Operators should be able to respond to this alarm within the stipulated response time. Failing a timely response, the tank level would reach high level, and a high-level alarm is triggered, and this also requires appropriate human intervention within the recommended response time. Should this barrier fail, the automatic shutdown should be activated to stop the tank filling operation and to prevent the overfill. Therefore, it is essential that these barriers achieve the required performance to reduce the probability of the overfilling of a storage tank (MIIB, 2008).

To establish the link between the barrier performance and the probability of a tank overfill, the indicator-based approach developed under the Risk-OMT project (Gran et al., 2012) may be chosen. The Risk-OMT model focuses mainly on factors that influence the barrier performance, denoted as risk influencing factors (RIFs). The influence of these RIFs to the barrier failures are modeled by Bayesian Networks (BNs). In the Risk-OMT, RIFs are structured in two levels in BNs: RIFs on Level 1 are organizational conditions, and RIFs on Level 2 are management aspects. Furthermore, indicators are used to measure the status of such RIFs and included as the observations (for details about the Risk-OMT project, see Gran et al., (2012)). In this case study, we present a simple BN model that include the influencing factors at the same level. As shown in Figure 2, the BN is constructed to represent the causal relationships between the hazardous event (specified as overfilling in Figure 2) and the states of the barriers installed to prevent this event. This BN also includes the influencing factors to the operational barriers, as well as the indicators to these factors. To perform a quantitative analysis

of this constructed BN, the prior distribution of each root node and the conditional probability distributions of the non-root nodes should be specified (Rausand, 2011). The probability distributions of the BN can be updated whenever we obtain new values for the indicators.

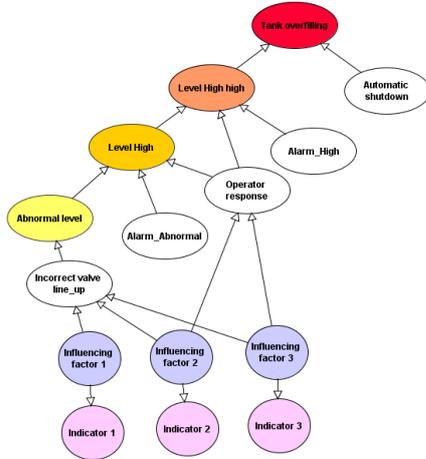


Figure 2. A simple BN for the specified hazardous event including factors for the barrier performance and the associated indicators.

### 3.3 Decision-making and evaluation

Spores (Spores, 2001) stipulated that measures of effectiveness (MOE) are the core of the evaluation of a proposed solution. He defines an MOE as the “standard to judge the capability of a solution to meet the needs of a problem.” The standard is a set of specific properties that any potential solution must exhibit to be considered fit for purpose. However, MOEs are given independently of any solution and do not specify performance criteria. MOE view the solution from the stakeholder's viewpoint, and in this case MOEs can be refined by using safety performance indicators relevant for the site, and examples are given in table 1. Creating a solution and collecting data that supports these measurements becomes the driving factors for designing and implementing a digital twin. Monitoring the site for potential overfill events should provide the desired result of a safe storage facility.

Table 1: Example of MOEs for company organization

Number of faults detected before the operation
Number of unwanted events (e.g. near misses) in a specified period
Fraction of operational activities considered for risk analysis
Percentage of correct maintenance on safety critical items
Fraction of sensible data related to a unique process line controlled by one supervisor

## 4. Conclusions

This paper illustrates the application of a representative SE methodology called SPADE in the early phase of designing a new risk monitoring tool based on DRA methods and the digital twins. The use of SPADE allows for clarifying the problems and provides a structured approach for proposing potential solutions to the problems, as well as MOEs for evaluating proposed solution. Although the case study uses a hypothetical situation for oil storage facilities, it can be anticipated that developing a common approach for monitoring major hazard risks is viable, and likely to benefit many operators of these sites. In contrast, the lower technologies of the Buncefield-type oil storage sites demands a structured approach to preventing overfill events and major accidents. Systems engineering methods are proposed here as an effective means to designing monitoring systems using digital twin solutions.

## References

- Aven, T., Renn, O., 2012. On the risk management and risk governance of petroleum operations in the Barents Sea area. *Risk Anal.* 32, 1561–75. <https://doi.org/10.1111/j.1539-6924.2011.01777.x>
- Boschert, S., Rosen, R., 2016. Digital Twin—The Simulation Aspect, in: *Mechatronic Futures*. [https://doi.org/10.1007/978-3-319-32156-1\\_5](https://doi.org/10.1007/978-3-319-32156-1_5)

- Bubbico, R., Lee, S., Moscati, D., Paltrinieri, N., 2020. Dynamic assessment of safety barriers preventing escalation in offshore Oil&Gas. *Saf. Sci.* <https://doi.org/10.1016/j.ssci.2019.09.011>
- EU, 2012. European Parliament And Council, 2012. Directive 2012/18/EU of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC - Seveso III. *Off. J. Eur.Union* 1e37 1–37. [https://doi.org/doi:10.3000/19770677.L\\_2013.124.eng](https://doi.org/doi:10.3000/19770677.L_2013.124.eng)
- European commission, 2008. Necessary Measures for Preventing Major accidents at Petroleum Storage depots. Key Points and conclusions, Labour.
- Fernandes, L.J., Relvas, S., Barbosa-Póvoa, A.P., 2013. Strategic network design of downstream petroleum supply chains: Single versus multi-entity participation. *Chem. Eng. Res. Des.* <https://doi.org/10.1016/j.cherd.2013.05.028>
- Gran, B.A., Bye, R., Nyheim, O.M., Okstad, E.H., Seljelid, J., Sklet, S., Vatn, J., Vinnem, J.E., 2012. Evaluation of the Risk OMT model for maintenance work on major offshore process equipment. *J. Loss Prev. Process Ind.* 25, 582–593.
- Haskins, C., 2008. Systems engineering analyzed, synthesized, and applied to sustainable industrial park development. Thesis NTNU Trondheim, Norway. 2008175.
- Haskins, C., Krueger, M., Forsberg, K., Walden, D., Hamelin, R.D., 2011. *Systems Engineering Handbook V3.2.2*. International Council on Systems Engineering (INCOSE).
- Haskins, C., Ruud, K.S., 2018. Systems engineering: Making people talk! *Discip. Converg. Syst. Eng. Res.* 1081–1093. [https://doi.org/10.1007/978-3-319-62217-0\\_75](https://doi.org/10.1007/978-3-319-62217-0_75)
- 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.
- Herrera, E., 2018. Digital Twins' Role in an Ever-increasing Remote Workforce [WWW Document]. URL <https://www.rtinsights.com/digital-twins-role-in-an-ever-increasing-remote-workforce/>
- HSE, 2005. Buncefield: Why did it happen? Control Major Accid. Hazards 36.
- INCOSE, 2018. What is systems engineering [WWW Document]. URL <https://www.incose.org/systems-engineering> (accessed 1.25.21).
- Khakzad, N., Khan, F., Paltrinieri, N., 2014. On the application of near accident data to risk analysis of major accidents. *Reliab. Eng. Syst. Saf.* 126, 116–125. <https://doi.org/10.1016/j.res.2014.01.015>
- Landucci, G., Paltrinieri, N., 2018. Proactive monitoring of risk-based indicators: Example of application in the Oil & Gas integrated operations, in: *Institution of Chemical Engineers Symposium Series*.
- Lee, J., Cameron, I., Hassall, M., 2019. Improving process safety: What roles for digitalization and industry 4.0? *Process Saf. Environ. Prot.* <https://doi.org/10.1016/j.psep.2019.10.021>
- MIIIB, 2008. The Buncefield Incident 11 December 2005, Volume 2.
- Øien, K., Sklet, S., 2001. Metodikk for utarbeidelse av organisatoriske risikoindikatorer. Trondheim, Norway.
- Paltrinieri, N., Haskins, C., 2018. Chapter 7: Dynamic Security Assessment: Benefits and Limitations. In: Reniers, G., Khakzad, N., Van Gelder, P. (eds). "Security Risk Assessment – in the chemical and process industry", DeGruyter, ISBN: (978-3-11-050052-3).
- Paltrinieri, N., Landucci, G., Rossi, P.S., 2019. An integrated approach to support the dynamic risk assessment of complex industrial accidents. *Chem. Eng. Trans.* 77, 265–270. <https://doi.org/10.3303/CET1977045>
- 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>
- Pasman, H.J., 2020. Early warning signals noticed, but management doesn't act adequately or not at all: a brief analysis and direction of possible improvement. *J. Loss Prev. Process Ind.* <https://doi.org/10.1016/j.jlp.2020.104272>
- PSLG, 2009. Safety and environmental standards for fuel storage sites, Health and Safety Executive.
- Rasheed, A., San, O., Kvamsdal, T., 2020. Digital twin: Values, challenges and enablers from a modeling perspective. *IEEE Access.* <https://doi.org/10.1109/ACCESS.2020.2970143>
- Rausand, M., 2011. Risk assessment - theory, methods and applications, Statistics in practice. Wiley, Hoboken,NJ.
- Sharma, R.K., Gurjar, B.R., Wate, S.R., Ghuge, S.P., Agrawal, R., 2013. Assessment of an accidental vapour cloud explosion: Lessons from the Indian Oil Corporation Ltd. accident at Jaipur, India. *J. Loss Prev. Process Ind.* <https://doi.org/10.1016/j.jlp.2012.09.009>
- Sproles, N., 2001. The difficult problem of establishing measures of effectiveness for command and control: A systems engineering perspective. *Syst. Eng.* <https://doi.org/10.1002/sys.1012>
- Yang, X., Haugen, S., Paltrinieri, N., 2018. Clarifying the concept of operational risk assessment in the oil and gas industry. *Saf. Sci.* <https://doi.org/10.1016/j.ssci.2017.12.019>