CHEMICAL ENGINEERING TRANSACTIONS
VOL. 90, 2022
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Aleš Bernatík, Bruno Fabiano

ISBN 978-88-95608-88-4; **ISSN** 2283-9216
DOI: 10.3303/CET2290026

An Approach to Update the Failure Rates of Safety Barriers Based on Operating Experience

Shenae Lee[ad]*, Nima Khakzad[b], Peter Schmitz[c], Genserik Reniers[c], Solfrid Håbrekke[d], Nicola Paltrinieri[a]

[a] Dept. of Mechanical and industrial engineering, NTNU, Trondheim, Norway
[b] School of Occupational and Public Health, Ryerson University, Toronto, Canada
[c] Safety and Security Science Group, Faculty of Technology, Policy and Management, TU Delft, the Netherlands
[d] Dept. of Software Engineering, Safety and Security, SINTEF Digital, Trondheim, Norway
Shenae.lee@sintef.no

Hazardous events in process plants like the leakage of dangerous substances can result in severe damage, and such an event is often defined as the TOP event of a fault tree analysis (FTA) in a quantitative risk analysis. The TOP event probability can then be calculated if the basic events probabilities are provided. These probabilities are often determined based on generic reliability data which do not necessarily reflect the operational and environmental characteristics of a plant of interest. This paper presents an approach based on Bayesian network (BN) analysis to explicitly include experience data collected during the plant operation to make the generic probabilities more plant specific. The approach is illustrated via a pressure vessel containing a toxic substance in an Ammonia production plant. In this case study, the failure rate distribution in the BN is updated as the new information becomes available during plant operation. The results show that the suggested approach effectively reflects the operating experience of a specific plant.

1. Introduction

Process plants have the inherent potential to cause major accidents (Kletz, 2009). The release of toxic gas in Bhopal in 1984 (Kalelkar and Little, 1988), the explosion in Toulouse in 2001 (Dechy et al., 2004), and the explosion in Buncefield in 2005 (MIIB, 2008) are some examples of such accidents. Such accidents have been a driving force for the development of risk assessment in the process industry. This is reflected in the regulations related to major process accidents, like the Seveso directive of the European Union that is imposed on the operators of facilities handling dangerous substances. The directive requires the operators of the Seveso site categorized as upper-tier sites to perform risk analysis and to implement all the necessary risk-reducing measures (EU, 2012). To meet this requirement, quantitative risk analyses (QRAs) is typically carried out in the design phase of a facility (Paltrinieri and Reniers, 2017).
Conventional QRA studies focuses on the quantification of the risk related to major accident scenarios (Haugen, 2018). A major accident scenario in the process industry generally involves a loss of containment (LOC) event like a leakage from a vessel, which can be referred to as a central event (bowtie), TOP event (fault tree) or hazardous event. To estimate the risk related to a specific hazardous event, the frequency or probability of this event should be obtained (Delvosalle et al., 2006). The frequency estimates for representative hazardous events in process plants can be found in the literature sources, for example the HSE UK failure rate and event data for land use planning (HSE, 2012) and the Dutch Purple book published as a guideline for QRA in the process industry (Uijt de Haag and Ale, 2005). Such frequency estimates are usually derived from historical data and various QRA studies for typical process systems, and are intended to be a default value that can be either a conservative or nonconservative approximation for the studied system (Beerens et al., 2006). It may therefore be necessary to calculate the probability/frequency of a specific hazardous event, for instance, using a fault tree analysis (FTA).
FTA has been extensively applied in the QRAs of process systems (Khakzad et al., 2011; Pasman, 2015).

Paper Received: 14 January 2022; Revised: 16 March 2022; Accepted: 22 April 2022
Please cite this article as: Lee S., Khakzad N., Schmitz P., Reniers G., Håbrekke S., Paltrinieri N., 2022, An approach to update the failure rates of safety barriers based on operating experience, Chemical Engineering Transactions, 90, 151-156 DOI:10.3303/CET2290026

When the probability of the TOP event is to be calculated for a FTA, first the probability of each basic event in the FT must be determined, for example, failure probabilities for technical barriers and human error probabilities. An example of a basic event is a pressure relief valve that does not open upon demand. For such a technical component, the time to failure distribution is often assumed to be an exponential distribution with a constant failure rate. Then, the basic event probability is determined by the probability of failure on demand that is calculated from the failure rate and test interval (Vesely et al., 1981). Component test intervals are usually known from the maintenance system, while failure rates are uncertain parameters. Thus, to provide the failure rate vales, generic reliability data are often used in FTA. However, if possible and reasonable, plant-specific failure rates should ideally be used to reflect the plant characteristics (such as usage and environment), rather than generic failure rates representing the average data for a whole industry. In this respect, the use of generic reliability data in a FTA contributes to parameter uncertainty, which in turn may influence the validity of the frequency of the TOP event (Hauptmanns, 2008).
Several approaches have been suggested to handle the parameter uncertainty in FTA, e.g. where a component failure rate is treated as a random variable with a probability distribution (Brissaud et al. (2010), Flage et al. (2013)). In addition, the failure rate distributions can be updated based on the actual performance of a component (Kaplan (1983), Siu and Kelly (1998), Vatn (2006), Khakzad et al.,(2014)). Based on these studies, this paper suggests an approach based on Bayesian network (BN) analysis where the barrier failure rates are updated based on operating experience. In the suggested approach, a FT model for a hazardous event is converted to a BN, and then this BN model is extended with a hierarchical Bayesian analysis where generic reliability data are used to define the prior distribution of the failure rate, and plant-specific data are used to update the failure rate distribution. A case study of a pressure vessel in an Ammonia production plant is used to demonstrate the approach. In this case study, the failure rate of an important barrier is updated based on the incidence reports and maintenance data.

2. Theoretical background

Bayesian network (BN) analysis is becoming increasingly popular in risk and reliability studies for process systems, and is used as an alternative to FTA (Khakzad et al., 2011). BN can overcome some of the limitations of FTA, and an advantage with a BN analysis is that the probabilities of the nodes in the BN can be updated as new information becomes available.

2.1 Bayesian networks in relation to fault trees

A BN is a directed acyclic graph built with nodes and arcs. Each node represents a random variable with a probability distribution that can be discrete or continuous (Charniak, 1991). An arc denotes the causal relationship between two variables, such that one variable is interpreted as a cause and another variable is interpreted as an effect. An effect variable is often referred to as a child and has a set of parent nodes that represent the cause variables. For any node with the parent(s), a conditional probability distribution needs to be specified to indicate the strength of the casual relationships between the variables (Kjærulff and Madsen, 2013). A node with no parents is called a root node, and for such nodes a marginal probability distribution needs to be specified. Any fault tree in a risk analysis can easily be converted to a BN where the basic events of a FT are represented by the root nodes. It should be noted that a basic event may appear more than once in a FT, but the same root node is presented only once in the BN (Rausand, 2011). The intermediate events and the TOP event of a FT are converted to non-root nodes, and the conditional probability table (CPT) of each non-root node should be specified such that it corresponds to the OR-gate and AND-gate, respectively, from the FT.

2.2 Hierarchical Bayesian analysis

The prior probabilities of the root nodes in the BN can be assigned in the same way as for the basic events in the fault tree, which means that parameter values (e.g. failure rates) are identified from available data. If generic data are applied, the BN analysis will give the same generic result for the leaf node as for the corresponding t TOP event in the FTA (Khakzad et al., 2011). The available data for a node may however be associated with uncertainty, and this uncertainty is described by using a prior distribution for the node (e.g. component). In this case, the component under consideration can be regarded as a sample of a population of similar components. Then, the failure rate λ_i of component *i*, is considered as a sample from a distribution, and this distribution is governed by uncertain hyperparameters (Kelly and Smith, 2009). Then, the prior distribution for each hyperparameter can be specified independently, and we can use vague prior distributions – e.g., uniform distribution – when no information exists. If there is available information such as expert opinion and relevant reliability data, these should be reflected in the prior distribution of the hyperparameters (Fenton and Neil, 2012). The prior distribution of a hyperparameter can be updated to a posterior distribution by using e.g., data from similar systems. As a result, an informative prior distribution for the failure rate can be determined, and this prior

distribution can be further updated to a posterior distribution in the light of the plant-specific data obtained during operation (Khakzad et al., 2014).

3. Proposed approach

This section presents the approach that is suited for establishing a BN model where the distribution of uncertain parameters (i.e., failure rates) can be updated by using Hierarchical Bayesian analysis. The approach consists of five steps as illustrated in Figure 1.

- Step 1 Construct the fault tree: It is essential to identify relevant hazardous events in risk analysis of a system or process. The relevant hazardous events can be identified by taking into account the type of the system and the properties of the substances contained in the system (ARAMIS, 2004). Each hazardous event is defined as the TOP event of a FT, such that the FT is used to model the causal sequences to the event, including barrier failures.

-Step 2 Convert the fault tree structure to a BN: The conversion is straight forward (see Section 2.1.)

-Step 3 Evaluate the data sources for selecting prior distributions: As mentioned in Section 2.2, the prior probability for each node may be assigned in the same way as for the FTA. Then, we can carry out a sensitivity analysis to obtain the ranking of important nodes (variables) that have significant influence on the hazardous event, and such variables require better quantification (Rausand, 2011). In this step, it is proposed to search for plant-specific data, at least for the important components. However, plant-specific data are usually sparse, and it is therefore suggested to use the performance data from similar systems by using Hierarchical Bayesian analysis.

-Step 4 Hierarchical Bayesian analysis: Hierarchical Bayesian approach can be graphically represented in the BN by extending the BN with the nodes for the hyperparameters, and this requires that the prior distributions for the hyperparameters be determined. In cases where additional information about the hyperparameters is available, this information can be incorporated to obtain an informative prior distribution for the parameter of interest (see Section 2.2).

-Step 5 Obtain a posterior distribution given the new plant-specific data: During the operation of the studied system, we can obtain new information (e.g. maintenance data) that can be used to update a prior distribution for the parameter of interest in the BN (Khakzad et al., 2014). Such information is referred to as evidence, and the BN is extended by adding the evidence nodes.

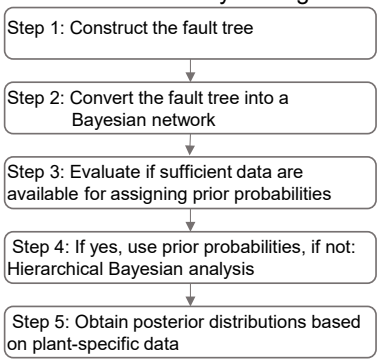

Figure 1: The proposed procedure for hierarchical Bayesian analysis

4. Case study

4.1 Construction of the fault tree and Bayesian network

The proposed approach is demonstrated by a simple case study of a pressure vessel containing a toxic material, installed in an Ammonia production plant. The documentation and the drawing of the vessel is provided by the operator of an anonymous Ammonia production plant. The vessel is used to vaporize Anhydrous ammonia (NH_3) coming from a separator where NH_3 is in a liquid state. At start-up, the level of liquid NH_3 in the separator is controlled by a level control valve (LCV) that is operated manually by the human operator. If a large amount of NH_3 fluid enter the vessel, the pressure in the vessel will increase quickly, which can lead to the overpressure. The overpressure may in turn result in a rupture of the vessel. The hazardous event to be analyzed is specified as ‘overpressure in the expansion vessel due to the loss of liquid in the separator’.

The FT for the specified hazardous event is constructed as shown in Figure 2a, using the software CARA FaultTree (Sydvest, 1999). In the FT, the failures of the barrier elements (components) installed to prevent the overpressure are defined as basic events. A pressure relief valve (PSV) is a key barrier to relieve the excessive

pressure when the vessel pressure reaches the PSV set pressure. A flow orifice (FO) is used to regulate the pressure, such that the relief load on PSV will not increase over its relieving capacity. The PSV is designed as a 2 out of 2 system with the flow orifice. The level alarm called level alarm low (LAL) is sounded if the liquid level is too low in the separator, which will lead to the increase of the pressure in the expansion vessel. The operator should respond to LALs by operating the LCV manually. There are two redundant level alarms, denoted LAL1 and LAL2. There is also a pressure alarm, called pressure alarm high (PAH) that is redundant to the level alarms. PAH will be activated when the vessel pressure increases beyond a specified high pressure, and the operator should respond operating the LCV manually. However, the LCV with mechanical failures cannot perform correctly, even if the operator response is proper. Each node in the BN has two states, i) The component has failed ii) The component is functioning. It is noted that all the components included in the BN are barriers,. A barrier can fail in different ways or have several failure modes. For this case study, only the failure modes of a barrier that can impede the required safety function are considered. For PSVs, fail to open on demand (FTO) is the failure mode that includes the inability of a PSV to open at the set pressure, and thus the two states for PSV are specified as follows: i) FTO, ii) Functioning on demand.

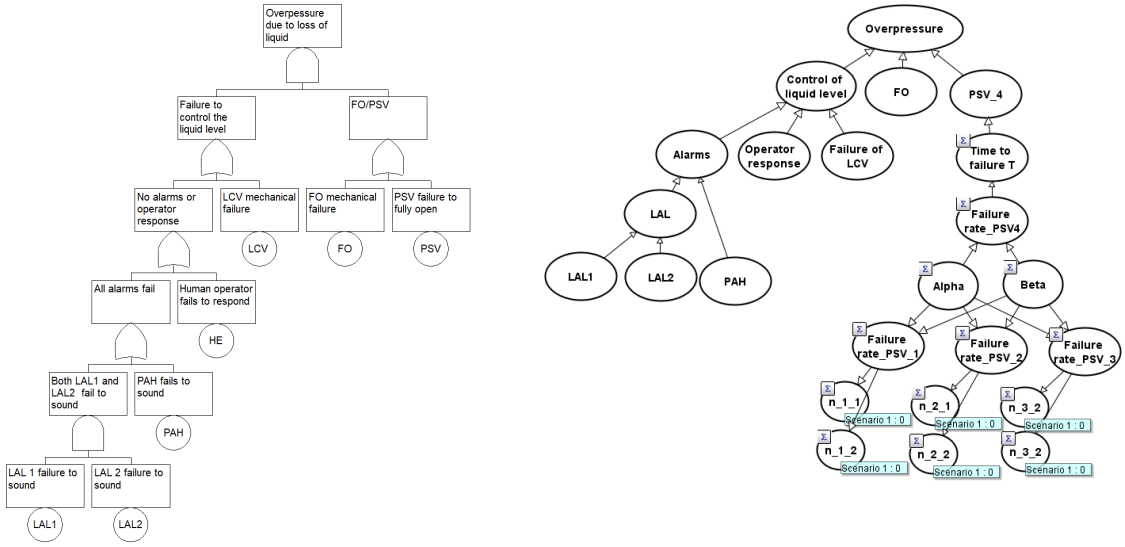

Figure 2a: The fault tree for the overpressure in the expansion vessel. Figure 2b: The BN extended by including hierarchical Bayesian analysis

4.2 Informative prior distribution

The FT model established in Step 1 is converted to a BN, and the prior probabilities for the nodes in the BN are determined. The failure probabilities of components assumed based on both generic reliability data from the Offshore and Onshore Reliability Data (OREDA) (OREDA, 2009), as well as the company database. For the human error probabilities, are based on the risk analyses by the company. A sensitive analysis revealed that the PSV is the most critical among the technical components, and therefore a hierarchical Bayesian analysis is carried out for the PSV.

For this case study, historical performance data from three other PSVs installed in a similar Ammonia plant are used to generate an informative prior distribution for the failure rate of the PSV. The three other PSVs are denoted as PSV_1 PSV_2 and PSV_3 respectively, and the given PSV is denoted as PSV_4. These PSVs are used in similar operating conditions with PSV_4 and are deemed to have similar failure characteristic. Therefore, λ_i of PSV_i is considered as a sample of the random variable Λ that is Gamma distributed with α and β. The time to failure T_i of PSV_i is assumed to be exponentially distributed with the failure rate λ_i. As shown in Figure 2b, the BN is extended with the hyper parameter nodes for α and β (the nodes named Alpha and Beta), which is connected to the nodes for λ_i. To choose the prior distributions for the hyperparameters α and β, we use PSV data obtained from OREDA. The PSV data from OREDA are relevant for PSV_4, because it reflects the industry-average failure rate for PSVs. The lower, mean, and upper values for the estimate of the failure rate (per 10^6 hours) for the conventional PSVs are 0.02, 1.17, and 3.69 per 10^6 hours respectively (OREDA, 2009). To reflect this information, a Triangular distribution (0, 1, 4) is selected for the hyperparameter α, where 1 is the most likely value, and 0 and 4 are the minimum and maximum values, respectively. The interpretation can be that the modal value for the number of failures within the accumulated time in service is 1. On the other hand, the exponent of hyperparameter β, $\log_{10}\beta$ is assumed to have a triangular distribution (-8, -7, -6), which may be interpreted as

the accumulated time in service is 10^6 to 10^8 hours. This method for defining hyper priors using Triangular distributions is suggested by Fenton and Neil (2012), to utilize observed performance of similar components or to use expert opinions, instead of using vague prior distributions for the hyper parameters.
The prior distribution is then updated to the informative prior distribution for the PSV in the BN, denoted PSV_4, using the performance data from the similar PSVs. This requires addition of evidence nodes for λ_i in BN representation. The evidence is the number of failures of PSV_i within the time interval $[t_j, t_j + v]$, n_{ij}, which is assumed to be Poisson distributed with mean $\lambda_i v$. In the BN, the arc is directed from the node λ_i (named as the failure rate node PSV_i) toward the evidence nodes. The construction and the calculation of the BN is carried out by using the software AgenaRisk (Agenarisk, 2018). According to the plant data collected from 2000-2008, PSVs opened on demand (i.e. at set pressure) during operation. A successful opening of a PSV indicates that the PSV is in a functioning state when a demand occurs. PSV_1 opened on demand twice, in 2000 and in 2008. PSV_2 also opened twice, in 2004 and 2007. PSV_3 opened once in 2007. To be able to use this information, it is assumed that the three PSVs are taken out of service every 4^{th} year for testing, which means that the length of observation period is 4 years for each PSV. If a demand occur within 4 years and the PSV is in FTO state, the PSV will not open successfully. It is therefore considered that the number of failures in the period 2000-2004 and the period 2004-2008 for these three PSVs is 0, which are entered as evidence, as shown in Figure 2b.

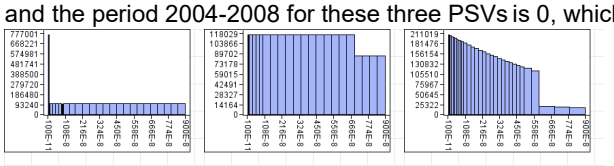

Figure 3a: Prior distribution, Figure 3b: informative distribution, Figure 3c: posterior distribution

4.3 Posterior distribution

The informative prior distribution of λ_4 is updated to a posterior distribution by using plant-specific data for PSV_4, that is the maintenance data from 2007 to 2016. The maintenance record shows that PSV_4 is subject to an inspection/overhaul, and pressure testing every 4^{th} year, and no failure of PSV_4 was detected. Therefore, number of failures = 0 is entered as evidence in period 2004-2008, 2008-2012, 2008-2016. FTO can only be detected by pressure testing or real demands, thus it can be classified as dangerous undetected (DU) failures. The mean downtime of a DU failure within a test interval is approximately the half of the test interval, given that a DU failure has occurred (Rausand, 2014). For this reason, PSV_4 is considered in failed state if its time to failure is less than 2 years (17520 hours). By this logic, the probability distribution of PSV_4 node is defined by implementing the expression 'if (T>17520, "Functioning", "FTO") 'in AgenaRisk software. The prior distribution, informative prior distribution, and posterior distribution of λ_4 are shown in Figures 3a, 3b, and 3c, respectively, and the mean and standard deviation of these distributions are reported in Table 1. The result shows that the mean value of the posterior distribution determined based on generic data is lower than the mean of the prior distribution, which may imply that the generic failure rate estimates for PSVs may be conservative values for the given plant.

Table 1: The updated mean and standard deviation (SD) of the failure rate distributions

	Prior distribution	Informative prior distribution	Posterior distribution
Mean	$4.35 \cdot 10^{-6}$	$4.29 \cdot 10^{-6}$	$2.97 \cdot 10^{-6}$
SD	$2.68 \cdot 10^{-6}$	$2.52 \cdot 10^{-6}$	$2.02 \cdot 10^{-6}$

5. Conclusions

The suggested approach is based on BN analysis where the BN model for a specified hazardous event is extended with hierarchical Bayesian analysis for updating the failure rate distributions. The case study demonstrates how the failure rate distribution of a key barrier, a PSV, can be updated based on operating experience. The performance data from the similar PSVs are incorporated to obtain the informative prior distribution, and then experience data from the given plant are used to obtain the posterior distribution. This approach is directed at practical application of hierarchical Bayesian analysis to handle parameter uncertainty in a risk analysis.

Acknowledgments

The first author is grateful for the hospitality during her visit to Safety and Security Science Group at TU Delft.

References

Agenarisk, 2018. AgenaRisk: Bayesian network and simulation software for risk analysis and decision support.

ARAMIS, 2004. Accidental risk assessment methodology for industries in the context of the Seveso II directive. Technical report EVSGI-CT-2001-00036, Fifth Framework Programme of the European Community, Energy, Environment and Sustainable Development, http://aramis . jr.

Beerens, H.I., Post, J.G., Uijt De Haag, P.A.M., 2006. The use of generic failure frequencies in QRA: The quality and use of failure frequencies and how to bring them up-to-date. J. Hazard. Mater. https://doi.org/10.1016/j.jhazmat.2005.07.013

Brissaud, F., Barros, A., Bérenguer, C., Troffaes, M., 2010. Handling parameter and model uncertainties by continuous gates in fault tree analyses. Proc. Inst. Mech. Eng. Part O J. Risk Reliab. https://doi.org/10.1243/1748006XJRR313

Charniak, E., 1991. Bayesian networks without tears.

Dechy, N., Bourdeaux, T., Ayrault, N., Kordek, M.A., Le Coze, J.C., 2004. First lessons of the Toulouse ammonium nitrate disaster, 21st September 2001, AZF plant, France, in: Journal of Hazardous Materials. https://doi.org/10.1016/j.jhazmat.2004.02.039

Delvosalle, C., Fievez, C., Pipart, A., Debray, B., 2006. ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries. J. Hazard. Mater. 130, 200–219.

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

Fenton, N., Neil, M., 2012. Risk assessment and decision analysis with bayesian networks, Risk Assessment and Decision Analysis with Bayesian Networks. https://doi.org/10.1201/b21982

Flage, R., Baraldi, P., Zio, E., Aven, T., 2013. Probability and Possibility-Based Representations of Uncertainty in Fault Tree Analysis. Risk Anal. https://doi.org/10.1111/j.1539-6924.2012.01873.x

Haugen, S., 2018. Safety in Offshore Platforms—Use of QRA in the Norwegian Offshore Industry. https://doi.org/10.1016/bs.mcps.2018.05.001

HSE, 2012. Failure Rate and Event Data for use within Risk Assessments (FRED) 1–96.

Kalelkar, A.S., Little, A.D., 1988. Investigation of large-magnitude incidents: Bhopal as a case study.

Kaplan, S., 1983. ON A “TWO-STAGE” BAYESIAN PROCEDURE FOR DETERMINING FAILURE RATES FROM EXPERIENTIAL DATA. IEEE Trans. Power Appar. Syst. Vol. PAS-1, 195–202.

Kelly, D.L., Smith, C.L., 2009. Bayesian inference in probabilistic risk assessment-The current state of the art. Reliab. Eng. Syst. Saf. https://doi.org/10.1016/j.ress.2008.07.002

Khakzad, N., Khan, F., Amyotte, P., 2011. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. Reliab. Eng. Syst. Saf. 96, 925–932. https://doi.org/10.1016/j.ress.2011.03.012

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.ress.2014.01.015

Kjærulff, U.B., Madsen, A.L., 2013. Bayesian Networks and Influence Diagrams: A Guide to Construction and Analysis (Second Edition), Information Science and Statistics. https://doi.org/10.1007/978-3-642-46890-2_1

Kletz, T., 2009. What Went Wrong?, What Went Wrong? https://doi.org/10.1016/B978-1-85617-531-9.X0001-7

MIIB, 2008. The Buncefield Incident 11 December 2005, Volume 2.

OREDA, 2009. Offshore reliability data handbook, 6th editio. ed. OREDA Participants, Available from: Det Norske Veritas, NO 1322 Høvik, Norway.

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., 2015. Risk Analysis and Control for Industrial Processes - Gas, Oil and Chemicals: A System Perspective for Assessing and Avoiding Low-Probability, High-Consequence Events, Risk Analysis and Control for Industrial Processes - Gas, Oil and Chemicals: A System Perspective for Assessing and Avoiding Low-Probability, High-Consequence Events. https://doi.org/10.1016/C2013-0-14379-6

Rausand, M., 2011. Risk assessment - theory, methods and applications, Statistics in practice. Wiley, Hoboken,NJ.

Siu, N.O., Kelly, D.L., 1998. Bayesian parameter estimation in probabilistic risk assessment. Reliab. Eng. Syst. Saf. https://doi.org/10.1016/S0951-8320(97)00159-2

Sydvest, 1999. CARA-FaultTree: Software tool for fault tree analysis. http://www.sydvest.com/Products/Cara/.

Uijt de Haag, P.A.M., Ale, B.J.M., 2005. PSG3: Guidelines for Quantitative risk assessment (purple book). Publ. Ser. Danger. Subst.

Vatn, J., 2006. Procedures for updating test intervals based on experience data, in: Proceedings of the 30th ESReDA Seminar. European Commision, Joint Reserach Center, Ispra, Italy, pp. 185–196.

Vesely, W.E., Goldberg, F.F., Roberts, N.H., Haasl, D.F., 1981. Fault Tree Handbook (NUREG-0492). U.S. Nucl. Regul. Com.