CHEMICAL ENGINEERING TRANSACTIONS
VOL. 82, 2020
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Bruno Fabiano, Valerio Cozzani, Genserik Reniers

ISBN 978-88-95608-80-8; **ISSN** 2283-9216
DOI: 10.3303/CET2082026

From Risk Assessment to Resilience Assessment. An Application to a HazMat Storage Plant

Tomaso Vairo[a]*, Andrea P. Reverberi[b], Bruno Fabiano[a]

[a] DICCA - Civil, Chemical and Environmental Engineering Dept. – Genoa University, via Opera Pia 15 - 16145 Genoa, Italy
[b] DCCI - Chemistry and Industrial Chemistry Dept., Genoa University, via Dodecaneso 31 - 16145 Genoa, Italy
tomaso.vairo@edu.unige.it

The purpose of this work is to outline a framework for assessing the resilience of a petrochemical storage plant, through the construction of a dynamic hierarchical Bayesian network. The BN approach allows keeping memory of the states, in order to manage the actual safety and reliability evidences during the petrol transfer operation from storage tank to trucks in a repository of oil products. The proposed framework aims at assessing risk in process plants by analysing continuous process hazard data from a Bayesian point of view. A sequence of hazard functions derived for the FTAs, is modelled with a hidden Markov chain. The capability of the model implemented by means of Markov Chain Monte Carlo methods are tested at a real scale plant.

Keywords: data driven model, hidden Markov models, resilience, semi-supervised learning,.

1. Introduction

The main objective of risk assessment within industrial settings is the minimization of accident probability or, at least, the preservation of this probability below an acceptable value. QRA is a legislative mandatory requirement in a wide range of industrial plants according to specific Seveso Directives used as the basis of regulations, also outside of the European Union (Fabiano et al., 2017). As commented by Genserik and Pasman (2014), the obtained risk picture of the system is however static, being fully developed at the design stage. The Bayesian approach is currently widely recognised as a proper framework for analysing risk in industrial plants (Vairo et al. 2019, Yang et al. 2013, Kantalarmia et al. 2009). However, the traditional Bayesian approach is unable to keep memory of the previous states of the plant components and thus is unable to catch the transition from “safe” to “unsafe” states, identifying the trend exclusively on the basis of the current state of the system. On these grounds, several studies were performed focusing on a dynamic risk assessment by use of the BN in the process industries. As amply reported, even when performing an accurate risk analysis, it is not possible to rule out uncertainty completely, mainly due to lack of knowledge about the system and the physical variability of a system response (Markowski et al., 2009). Additionally, from a survey on his personal experience in 92 QRAs over a time span of 36 years, Taylor (2016) evidenced that the 26 major accidents were related to uncompleted hazard identification and management not correctly implementing HazId. In this paper, a detailed comparison between the traditional risk analysis and the proposed resilience assessment is carried out, referring selected scenarios involving a significant loss of containment (LOC). Different databases including Lloyds’ Register allow concluding that human error is the main cause of a lot of operational mishaps causing LOCs: they are either covered by the previous HazId phase, or they appear in ageing plants as new causes (e.g. Vairo et al., 2018). On these grounds, the resilience of the system was analysed, i.e. the capacity of the system to respond to disturbances that may occur during the ongoing operations, maintaining a dynamic stability. For each precursor event, resilience analysis was carried out using dynamic Bayesian networks. A priori probabilities obtained from conventional risk analysis procedure are updated on the basis of the evidence gathered in the plant during the operations, then stochastically disturbed by inserting them in Markov-Monte Carlo chains. As recently proposed by Don & Khan, (2019) integrated data driven techniques, including HMM and Bayesian network (BN), allows a successful approach to Abnormal Event Management (AEM) which includes the detection, diagnosis, and

Paper Received: 20 December 2019; Revised: 16 April 2020; Accepted: 28 August 2020
Please cite this article as: Vairo T., Reverberi A., Fabiano B., 2020, From Risk Assessment to Resilience Assessment. an Application to a Hazmat Storage Plant, Chemical Engineering Transactions, 82, 151-156 DOI:10.3303/CET2082026

correction of abnormal conditions of faults in a process. Four main cases were selected to test the correction capability of the approach based on new evidence, namely safe operation, hard disrupted operation, human error disrupted operation, event escalation. The overall system resilience is evaluated by a dynamic safety indicator, in relation to the posterior probability density function of the disruptive events. At last, the overall study under development will consider critical comparison of results with the outputs of conventional risk assessment.

2. Methodology

As detailed in the following, the development of the model includes a customized implementation of Hidden Markov Model (HMM) coupled with Bayesian inference applied to dynamic fault trees.

2.1 Theoretical approach

HMM is a statistical Markov model in which the system being modelled is assumed to be a Markov process with unobservable (i.e. hidden) states, which in the given context represent the transitions between the “safe” and “unsafe” states of the system. The focus of this work is to evaluate the results that HMM semi-supervised learning models could achieve to perform a reliable forecasting of states sequences during critical operations in a Seveso upper tier plant, starting from operational experience and field data. Basic assumption in defining the space of probable sequences is that only pairwise dependencies over hidden states are assumed. HMM generates a sequence of T output variables y_t conditioned on a parallel sequence of latent categorical state variables$z_t \in \{1, \dots K\}$. These hidden state variables are assumed to form a Markov chain (MC) so that z_t is conditionally independent of other variables, once given z_{t-1}. MC is parameterized by a transition matrix θ where θ_k is a K-simplex for $k \in \{1, \dots K\}$. The probability of transitioning to state z_t from state z_{t-1} is:

$$z_t \sim Categorical\left(\theta_{z\,[t-1]}\right) \tag{1}$$

The output y_t at time t is generated conditionally independently based on the latent state z_t (Munkhammar et al. 2018). It is possible describing HMMs with a simple categorical model for outputs $y_t \in \{1,\dots,V\}$.
The categorical distribution for latent state k is parameterized by a V-simplex ϕ_k. The observed output y_t at time t is generated based on the hidden state indicator z_t at time t:

$$y_t \sim Categorical\left(\emptyset_{z\,[t]}\right) \tag{2}$$

So HMMs form a discrete mixture model where the mixture component indicators form a latent Markov chain.
Given the transition and emission parameters, $\theta_{k,k'}$ and $\phi_{k,v}$ and an observation sequence $u_1, \dots, u_T \in \{1,\dots,V\}$, the *Viterbi algorithm* computes the state sequence which is most likely to have generated the observed output u (Blasiak et al. 2011). As widely discussed (Vairo et al. 2019, Meel et al. 2006), fault tree analysis (FTA) can be effectively transposed into dynamic Bayesian Networks. The latter however, can perform forward analysis, being the inference process based on the naive assumption of conditional independence between basic events. In order to overcome this limitation it is possible building a hierarchical network; following the original reasoning by Chatzis et al. (2011), the Bayesian structure was developed starting from the Markov Chain of hidden states.

2.2 Model development

The model is developed according to the conceptual scheme depicted in Figure 1. As the failure frequencies of root events are transposed into probability distribution, the first stage consists in performing MCMC sampling (with the conditional rules coming from the fault trees) and obtaining the distributions of intermediate events. The second stage is considering the intermediate distributions (whose observation are the data, related to the root events), and perform a second MCMC sampling from the intermediate (i.e. the posterior of root events) to obtain the Top Event distribution. The third stage aims at identifying the “*hidden states*” between safe state and failure by applying the customized Hidden Markov Model in which only the first and the last states are known, and the intermediate can be inferred from the observation and the probability distributions. In this way, the probability of correctly classifying the states sequence has a maximum a posterior probability (MAP) probability. From Bayes' rule we obtain:

$$P(Z|T) = \frac{P(Z)P(T|Z)}{P(T)} \tag{3}$$

where, Z is the sequence of states and T the emissions (observations). Since P(T) is independent of the sequence Z , the discriminant function to be maximized is:

$$g_c(T) = P(T|Z)P(Z) \quad (4)$$

Following assumptions are made in order to reduce the problem down to manageable size:

- The size of the sequence of observations is not very large. Let n be the size of a word. Then P(C) is the frequency of occurrence of words.
- Conditional independence among the features vectors. The shape of a character, which generates a given feature vector, is independent of the shapes of neighboring characters, depending only on the character in question.

Under these assumptions, from Eq. (4), one can write:

$$g_c(T) = \sum_{i=1}^{n} logP\,(t_i|z_i) + logP(z_1, \ldots, z_n) \quad (5)$$

For the case of the Viterbi algorithm, if we assume that the process is first-order Markov, it follows:

$$g_c(T) = \sum_{i=1}^{n} logP\,(t_i|z_i) + log[P(z_1|z_0) + P(z_2|z_1) + \ldots + P(z_n|z_{n-1})] \quad (6)$$

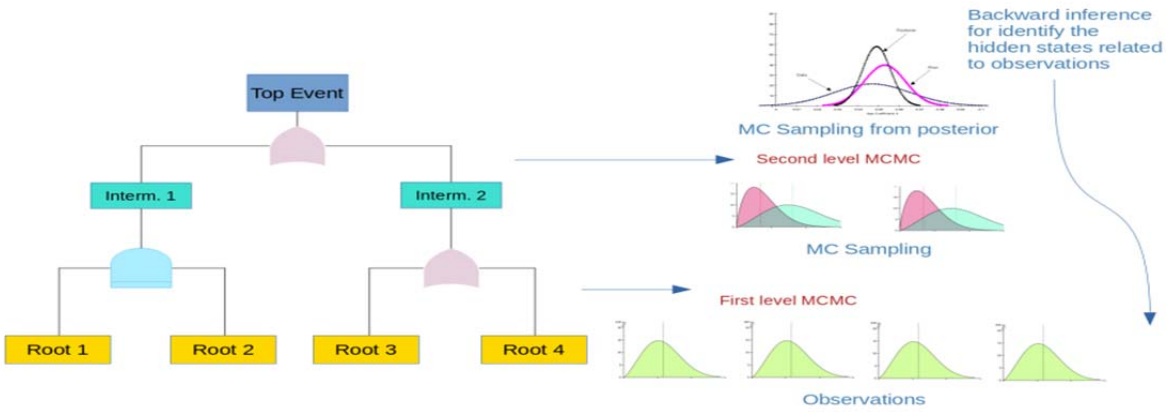

Figure 1: Model conceptual scheme.

3. Model validation

The case study is based on a petroleum products coastal storage facility located in Northern Italy, close to environmental sensitive areas, thus requiring safety protection priorities (Vairo et al., 2017). The facility is characterized by a storage capacity of about 200,000 cubic meters divided into 21 tanks and covers an area of 62.000 square meters. The facility is connected to the oil terminal pumping station via two 10" and one 16" oil pipelines, through which it is possible to both receive and ship the product by sea. The depot can also transfer product to nearby depots connected with two 6" pipelines. The products handled are mostly finished products (gasoline and diesel) of foreign and national origin; they can be received both by sea, through the equipment of the oil terminal and by pipelines (Figure 2).

Figure 2: The coastal storage facility (Italy).

3.1 Case-study

The operation on which the present study is focused, is the transfer of product from storage tank to tank truck (ATB), with associated Top Event is the product leakage in the loading area. As amply reported, in case of onshore hydrocarbon release of flammable hydrocarbons to the surrounding, environment several types of hazards and different evolving scenarios may be considered, with pool fire covering an approximate figure of 42% of all accidents (Palazzi et al., 2017). As discussed in detail in Pesce et al. (2012), the overall ignition probability should consider conditional probabilities for immediate and delayed ignition accounting for the release rate and the number of ignition sources within the LFL envelope. According to conventional risk analysis approach, the loss of product (including very minor leaks) in the loading area was cautiously estimated at an occurrence frequency equal to 10^{-3} occasions per year. The preliminary validation relies on a limited set of identified root events resulting also from operating experience: product loss from valves / flanges, error in tank truck positioning, human error in hardware connections. According to the outlined approach, a resilience assessment is conducted and the overall safety of the operation is measured by means of a dynamic safety indicator. We consider one of the key aspect of the resilience, i.e. the system's ability to respond to disturbances that may occur during operations, while maintaining dynamic stability. For each of the identified deviations, the analysis of system safety was carried out using dynamic BNs. The prior probabilities are those of the traditional risk analysis of the safety report, which were subsequently updated on the basis of the evidence collected in the plant during the course of the operations, then stochastically disturbed by inserting them in MMCC (generation random of independent events following a given probability distribution). Four possible system conditions are identified to test the capability of the model, i.e. normal (safe) conduct of operations; disturbed conduct of operations: valve failures; disturbed conduct of operations: errors in the positioning of the tank; disturbed conduct of operations: human error in observing and escalating events.

4. Results and discussion

In the following, we outline in form of immediate readability results obtained by sampling from posterior distributions (red dots) in terms of mean posterior probability of occurrence. As depicted in Fig. 3 (a), the trend of the posterior probability of leakage during steady-state operation decreases: DRA takes into account operational evidence (occurrence of malfunctions, near-misses, etc.), absent in this case, properly updating the likelihood of the given hypotheses. The probability density function depicted in Fig. 3 (b) represents the safety indicator of the system connected to a valve failure. In this case, the probability initially increases, as there is evidence of an actual malfunction. However, the system detects it, therefore corrective measures (for example a replacement intervention) can be put in place before the system fails. After the intervention, the system dynamically resumes stability and the probability is lowered. Fig. 4 (a) shows the safety indicator in case of human error during tank truck load. Analogously, the probability initially increases, because there is evidence of an actual ATB positioning error (detected by the system and corrective measures are enforced before system failure and accident escalation. After the intervention, the system dynamically resumes stability, and the probability is lowered. Fig. 4(b) shows the safety indicator in case of ATB positioning errors. In this case, the probability increases, because there is evidence of a human error in highlighting the malfunctions, which can thus cause an escalation of events. Human error is distributed stochastically, but the system itself, once it has evidence of a loss of containment, can activate the protections. The subsequent identification of Hidden States is performed by stochastically distributing not only the errors, but all the events, inserting them as well as random evidence of the HMM and then performing Montecarlo simulations.

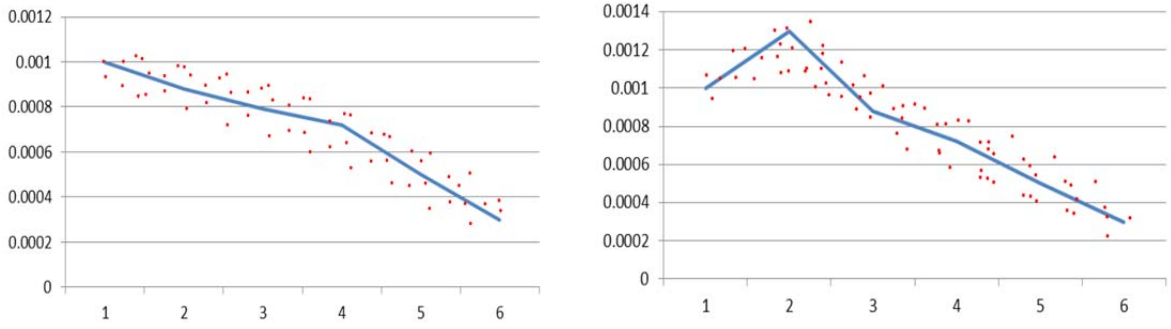

Figure 3: (a) Safe operation, leakage on loading area *(b) Perturbed operation, leakage on loading area*

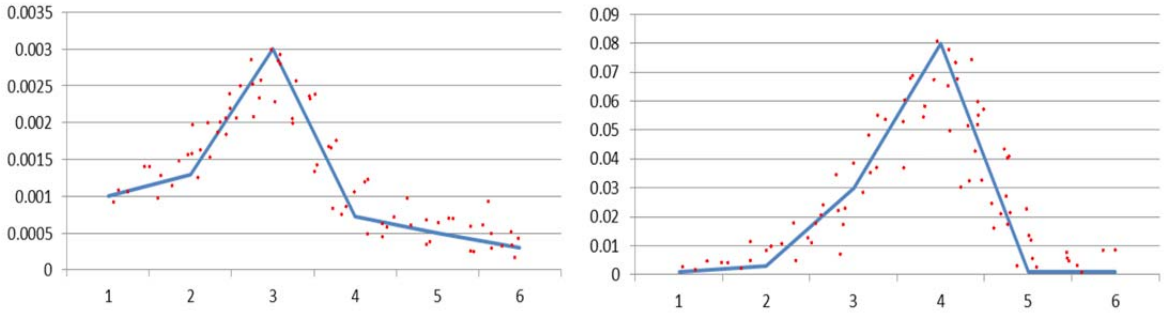

Figure 4: Posterior pdf : (a) perturbed operation, leakage on loading area (b) leakage on loading area, escalation.

Figures 5 and 6 clearly evidence the pdf of the cumulative errors and the MCMC trace respectively. After performing the posterior pdf analysis, it is possible emphasizing the most probable sequence of states of the system, visualizing the results as shown in Figure 7. According to this strategy, it is possible observing the overall transitions of the system and deriving quantitative safety indicators.

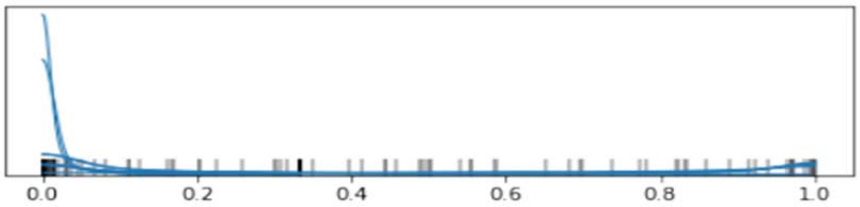

Figure 5: Pdf of cumulative errors.

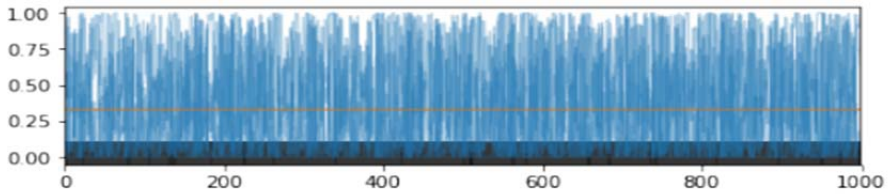

Figure 6: MCMC overall trace.

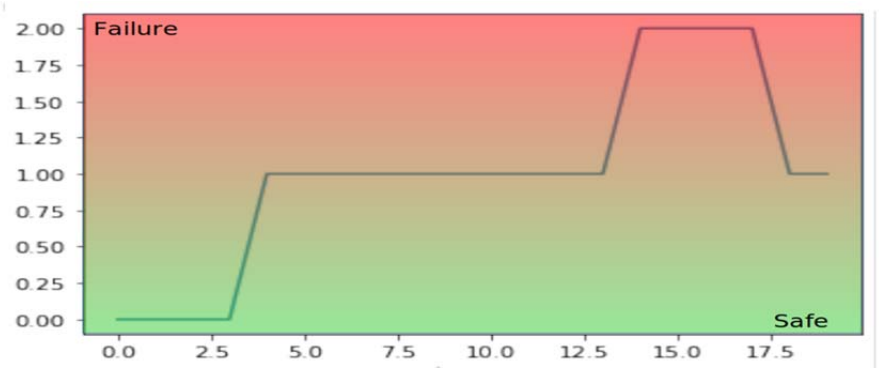

Figure 7: Overall most probable (>94%) sequence of states (transitions) vs. operation time (min).

5. Conclusions

Novel dynamic risk approaches are intended to capture the changes and deviations in operations based on collected data. We present a scheme relying on HHM to update the risk level during operation starting from sequence data. Additionally, the method allows extracting precise information on likelihood evidence from HMM towards actual BN updating. From the comparison between the PDF of minor LOCs, it is shown the

system ability in resuming dynamic stability, without hazardous consequences, improving as well overall safety performance. The possible states of the system resulting according to the performed tests are as follows, starting from safe conditions in the operation absence.

1. When carrying out operations without disturbances, the system is considered at steady-state safe and the leak posterior probability corresponds to 0.0003.
2. In case of operation disturbances absorbed by hard or soft barriers, the system is safe. The leak posterior probability rises to 0.003 and suddenly returns to 0.0005.
3. When operations with disturbances are performed without preventive barriers actions, but proper protection systems intervene, the system is safe. The leak posterior probability rises to 0.08 due to event escalation, but following protection systems intervention, go back to 0.0002.

The benchmark exercise shows that in the given cases, the process resilience is able to ensure the stability of the operations, in case of deviations from steady-state. Under the considered hypotheses, the oscillations of the dynamic safety indicator are contained within 0.3%, with 0-0.12% as 95-98% HPD (Highest Posterior Density). By setting up a dynamic system in which periodically the values are updated and statistically treated, coupled with Bayesian network ability, may enable monitoring resilience trends. Proper validation is still under development by extending a benchmark exercise starting from conventional risk analysis on the same installation. As a further development, the implementation will cover all plant sections, integrating a sensitivity analysis into the dynamic simulation, in order to quantify inputs uncertainties and output uncertainty range.

References

Blasiak S., Rangwala H., 2011, A Hidden Markov Model variant for sequence classification. IJCAI Proceedings-International Joint Conference on Artificial Intelligence, 22, 1192-1197.

Chatzis S., Kosmopoulos D., 2011, A variational Bayesian methodology for hidden Markov models utilizing Student's-t mixtures, Pattern Recognition, 44, 295–306.

Don M.G., Khan, F., 2019, Dynamic process fault detection and diagnosis based on a combined approach of hidden Markov and Bayesian network model, Chemical Engineering Science, 201, 82-96.

Fabiano B., Vianello C., Reverberi A.P., Lunghi E., Maschio G. 2016, A perspective on Seveso accident based on cause-consequences analysis by three different methods, J. Loss Preven. Process Ind. 49, 18-35.

Jain P., Rogers W.J., Pasman, H.J., Mannan M.S. 2018, A resilience-based integrated process systems analysis. Part II management system layer, Process Safety and Environmental Protection, 118, 115-124.

Kalantarnia M., Khan F., Hawboldt K. 2009, Dynamic risk assessment using failure assessment and Bayesian theory, Journal of Loss Prevention in the Process Industries, 22, 600-606.

Leveson N. 2004. A new accident model for engineering safer systems, Safety Science, 42, 237-270.

Markowski A. S., Mannan, M. S., Bigoszewska, A., 2009, Fuzzy logic for process safety analysis, Journal of Loss Prevention in the Process Industries, 22, 695–702.

Meel, A., Seider, W. 2006, Plant-specific dynamic failure assessment using Bayesian theory, Chemical Engineering Science, 61, 7036-7056.

Palazzi E., Caviglione C., Reverberi A.P., Fabiano B., 2017, A short-cut analytical model of hydrocarbon pool fire of different geometries, with enhanced view factor evaluation, Process Safety and Environmental Protection, 110, 89-101.

Pasman H.J., Reniers G., 2014, Past, present and future of Quantitative Risk Assessment (QRA) and the incentive it obtained from Land-Use Planning (LUP), J. Loss Preven. Process Ind., 28, 2–9.

Pesce M., Paci P., Garrone S., Pastorino R., Fabiano B., 2012, Modelling ignition probabilities in the framework of quantitative risk assessments, Chemical Engineering Transactions, 26, 141-146.

Munkhammar J. Widén J. 2018, An N-state Markov-chain mixture distribution model of the clear-sky index, Solar Energy 173, 487-495.

Taylor J.R., 2016, Can process plant QRA reduce risk? – Experience of ALARP from 92 QRA studies over 36 years, Chemical Engineering Transactions, 48, 811-816.

Vairo T., Del Giudice T., Quagliati M., Barbucci A., Fabiano B., 2017, From land- to water-use-planning: A consequence-based case-study related to cruise ship risk, Safety Science 97, 120-133.

Vairo T., Reverberi A.P., Milazzo M.F., Fabiano B., 2018, Ageing and creeping management in major accident plants according to Seveso III Directive, Chemical Engineering Transactions, 67, 403-408.

Vairo T., Milazzo M.F., Bragatto P., Fabiano B., 2019, A dynamic approach to fault tree analysis based on Bayesian Beliefs Networks, Chemical Engineering Transactions, 77, 829-834.

Wang H., Khan F., Abimbola M. 2018, A new method to study the performance of safety alarm system in process operations, Journal of Loss Prevention in the Process Industries, 56, 104-118.

Yang M. Kahn F., Lye L., 2013, Precursor-based hierarchical Bayesian approach for rare event estimation: a case of oil spill accident, Process Safety and Environmental Protection, 91, 333-342.