CHEMICAL ENGINEERING TRANSACTIONS

VOL. 83, 2020

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

Guest Editors: Bruno Fabiano, Valerio Cozzani, Genserik Reniers
Copyright © 2020, AIDIC Servizi S.r.l.
ISBN 978-88-95608-81-5; **ISSN** 2283-9216

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 assess the resilience of a petrochemical storage plant, through the construction of a dynamic hierarchical Bayesian network, which keeps memory of the states, in order to manage the evidence that gradually presents itself during the petrol transfer operation from tank to ATB in a repository of oil products.

The proposed framework represents a credible approach for assessing risk in Chemical plants by analizing continuous hazard data from a Bayesian point of view. A sequence of hazard functions, taken from the FTAs, is modeled with a hidden Markov chain. It is explained how the resultant model is implemented trough Markov Chain Monte Carlo (MCMC) methods.

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

1. Introduction

For some industrial systems, the main objective of the risk assessment is the minimization of accident probability or, at least, the preservation of this probability under an acceptable value.

The Bayesian approach is now 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 (posterior pdf) based exclusively on 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). In this paper, a detailed comparison between the traditional risk analysis and the proposed resilience assessment is carried out, referring to a selected scenario 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 LOC: they are either covered by the previous HazId phase or they appear in ageing plants as new causes. 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. The a priori probabilities are those of the traditional risk analysis process, which subsequently have been updated based on the evidence gathered in the plant during the operations, then stochastically disturbed by inserting them in Markov-Monte Carlo chains.

Four main cases have been identified, 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 results are critically compared to the outputs of the conventional risk assessment.

1. Methodology

The development of the model includes:

- Hidden Markov Model (HMM)
- Bayesian inference in dynamic fault trees

1.1 Hidden Markov Model

A hidden Markov model (HMM) is a statistical Markov model in which the system being modeled is assumed to be a Markov process with unobservable (i.e. hidden) states, which exactly represent the transitions between the “safe” and “unsafe” states.
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 ina high risk plant.
A hidden Markov model (HMM) generates a sequence of T output variables y_t conditioned on a parallel sequence of latent categorical state variables $z_t \in \{1, \ldots, K\}$. These hidden state variables are assumed to form a Markov chain so that z_t is conditionally independent of other variables given z_{t-1}. This Markov chain is parameterized by a transition matrix θ where θ_k is a K-simplex for $k \in \{1, \ldots, K\}$.
The probability of transitioning to state z_t from state z_{t-1} is

$$z_t \sim \text{Categorical } (\theta_{z[t-1]}).$$

The output y_t at time t is generated conditionally independently based on the latent state z_t (Munkhammar et al. 2018).
It,s possible to describe HMMs with a simple categorical model for outputs $y_t \in \{1, \ldots, V\}$.
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:

$$y_t \sim \text{Categorical}(\phi_{z[t]}).$$

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 $u_1, \ldots, u_T \in \{1, \ldots, V\}$, the *Viterbi algorithm* computes the state sequence which is most likely to have generated the observed output u (Blasiak et al. 2011).

1.2 Dynamic Fault Trees

As widely discussed (Vairo et al. 2019, Meel et al. 2006), the FTA can easily be transposed in dynamic Bayesian Networks.
Bayesian Networks. However, can perform forward analysis, being the inference process based on the naive assumption of conditional independence between basic events. This assumption can be overcome by buildin a hierarchical network
So, in the present paper, the Bayesian structure is built starting from the Markov Chain of hidden states (Chatzis et al. 2011).

1.3 The model

The model is built following the scheme in fig. 1.
The failure frequencies of root events are transposed in probability distribution.
The first stage is 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 is identifying the “*hidden states*” between safe state and failure by a 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, as described in § 1.1.

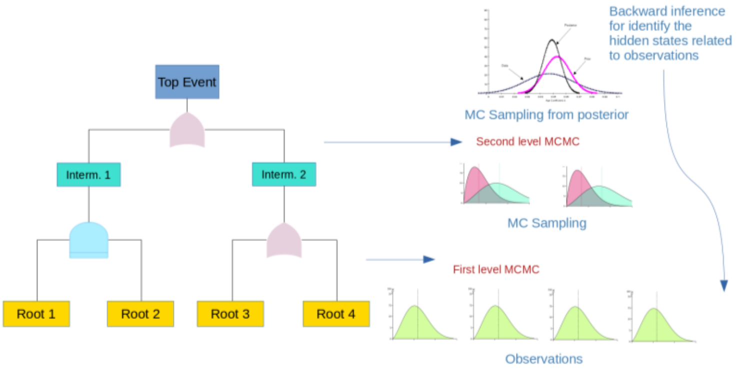

Fig. 1: Model scheme

2. The case study

the plant is a petroleum products coastal storage facility. It is spread over an area of 62.000 square meters and a storage capacity of about 200,000 cubic meters divided into 21 tanks.

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 pipeline.

Fig. 2: the storage facility

2.1 The operation

The operation on which the present study is focused, is the transfer of product from tank to ATB. And the associated Top Event is the product loss on the loading area.

The traditional risk analysis, included in the Safety Report, relating to the loss of product in the loading area, indicates a probability of occurrence equal to 1E-3 occasions per year.

The identified root events are:

- product loss from valves / flanges
- error in positioning ATB
- human error in connection

In the traditional risk assessment, the frequency of the Top Event remains constant. This is because such risk analysis is static, and, by definition, it is always the worst case.

In the present paper, a resilience assessment is conducted, and the overall safety of the operation is measured by a dynamic safety indicator, which represents one of the central 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 cases, the analysis of system safety was carried out using Bayesian dynamic networks. 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 Markov-Monte Carlo chains (generation random of independent events following a given probability distribution).

4 cases have been identified:

1. Normal (safe) conduct of operations
2. Disturbed conduct of operations: valve failures
3. Disturbed conduct of operations: errors in the positioning of the ATB
4. Disturbed conduct of operations: human error in observing and escalating events

The following figures show the sampling from posterior distributions (red dots) and the trend of the mean posterior probability of occurrence of the top event.

Case 1: Safe operation

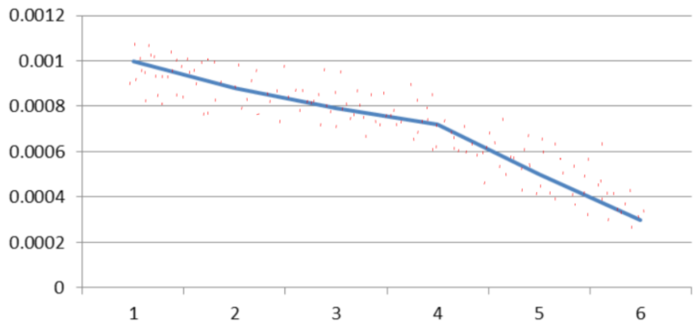

Fig. 3: Case 1 – safe operation, leakage on loading area, posterior pdf

In this case, the trend of the posterior probability of leakage during the operation decreases because the dynamic risk analysis takes into account the evidence during the operation (occurrence of malfunctions, anomalies, ...), absent in this case, which inevitably change the likelihood of the hypothesis being considered. The probability density function in Fig. 3 represent the safety indicator of the system.

Case 2: Valve failures

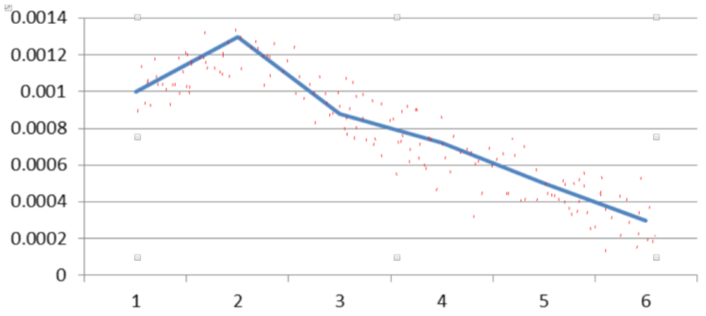

Fig. 4: Case 2 – perturbed operation, leakage on loading area, posterior pdf

In this case, the probability initially increases, because there is evidence of a malfunction (which, in this case, is no longer statistical, but real). 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 shows the safety indicator in case of valve failures.

Case 3: ATB positioning errors

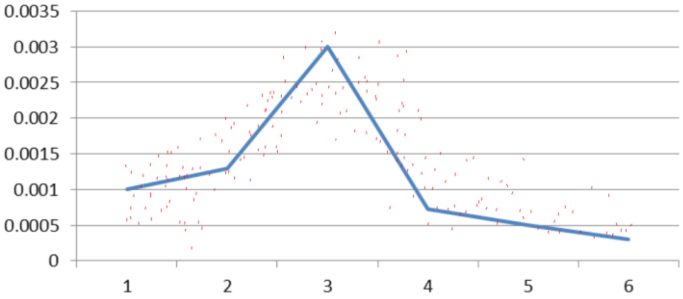

Fig. 5: Case 3 – perturbed operation, leakage on loading area, posterior pdf

In this case, the probability initially increases, because there is evidence of an ATB positioning error (which, in this case, is no longer statistical, but real). However, the system detects it, therefore corrective measures (for example positioning it correctly) can be put in place before the system fails. After the intervention, the system dynamically resumes stability, and the probability is lowered. Fig. 5 shows the safety indicator in case of ATB positioning errors.

Case 4: Event escalation

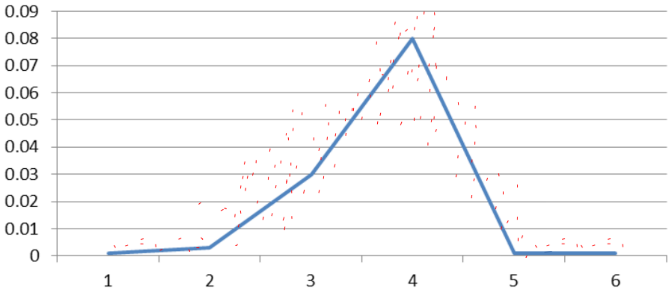

Fig. 6: Case 3 – perturbed operation, leakage on loading area, posterior pdf

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. Fig. 6 shows the safety indicator in case of event escalation.

Finally, the last stage: the identification of Hidden States.

This is done by stochastically distributing not only the errors, but all the events, inserting them as well as random evidence of the HMM, and performing Montecarlo simulations. So, it is possible to see the overall transitions of the system. the following figs 7 and 8 show the pdf of the cumulative errors and the MCMC trace. After the posterior pdf analysis, it is possible to determine the most probable sequence of states of the system. The most probable sequence is shown in fig 9.

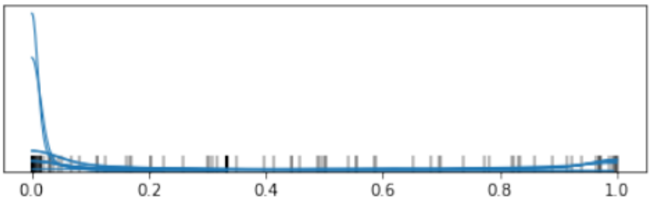

Fig. 7: pdf of cumulative errors

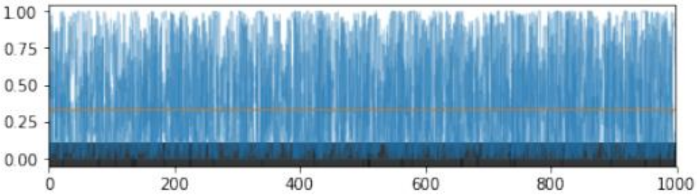

Fig. 8: MCMC overall trace

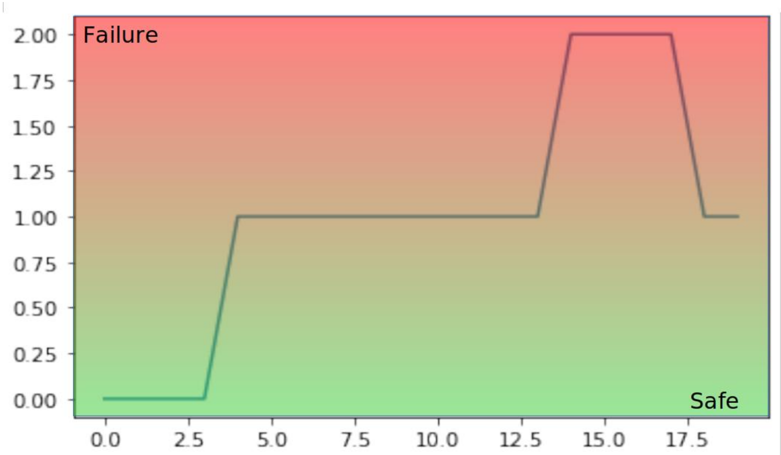

Fig. 9: overall most probable (>94%) sequence of states (transitions) vs. operation time (min)

3. Conclusions

From the comparison between the density functions of probability of having containment losses in the cases considered, it is clear how in all the cases analyzed, the system is able not only to resume dynamic stability without consequences, but to improve performance, expressed as overall safety index.

The results of the dynamic risk analysis can therefore be expressed considering frequency and impact trends.

The possible states of the system are as follows:

1. When no operations are performed, the system is secure
2. When carrying out operations without disturbances, the system is safe
3. When operations with disturbances are carried out which are absorbed during the operation, the system is safe
4. When operations with disturbances are carried out which are not absorbed during the operation, but protection systems intervene, the system is safe.

It is evident that, in all analyzed cases, the system is able to ensure the stability of the operations even in the event of disturbances in the normal course.

In the hypotheses analyzed (the same as in the valid Safety Report), the oscillations of the dynamic safety indicator are contained within 0.3%, with 0-0.12% as 95-98% HPD (Highest Posterior Density).

References

Blasiak, S.; Rangwala, H. (2011). "A Hidden Markov Model Variant for Sequence Classification". IJCAI Proceedings-International Joint Conference on Artificial Intelligence. 22: 1192.

Chatzis, Sotirios P.; Kosmopoulos, Dimitrios I. (2011). A variational Bayesian methodology for hidden Markov models utilizing Student's-t mixtures. Pattern Recognition. 44 (2): 295–306.

Jain P., Rogers W.J., Pasman, H.J., Mannan M.S., (2018). A resilience-based integrated process systems analysis. Process Safety and Environmental Protection, 118

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

Leveson, N., (2004). A new accident model for engineering safer systems, Safety Science, 42

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

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

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

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, vol. 77

Vairo T., Pettinato M., Fabiano B., (2019). A predictive operating control system based on Data Driven Bayesian Networks. Proceedings of ECCE12, The 12th European Congress Of Chemical Engineering

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

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