Journal of Loss Prevention in the Process Industries 26 (2013) 434–442

Contents lists available at SciVerse ScienceDirect

Journal of Loss Prevention in the Process Industries

journal homepage: www.elsevier.com/locate/jlp

Bayesian networks make LOPA more effective, QRA more transparent and flexible, and thus safety more definable!

Hans Pasman*, William Rogers

Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX 77843-3122, USA

ARTICLE INFO

Article history:
Received 19 February 2012
Received in revised form
20 May 2012
Accepted 4 July 2012

Keywords:
Process safety
Risk analysis
Bayesian networks
Cost–benefit
Software tools

ABSTRACT

Quantitative risk analysis is in principle an ideal method to map one's risks, but it has limitations due to the complexity of models, scarcity of data, remaining uncertainties, and above all because effort, cost, and time requirements are heavy. Also, software is not cheap, the calculations are not quite transparent, and the flexibility to look at various scenarios and at preventive and protective options is limited. So, the method is considered as a last resort for determination of risks. Simpler methods such as LOPA that focus on a particular scenario and assessment of protection for a defined initiating event are more popular. LOPA may however not cover the whole range of credible scenarios, and calamitous surprises may emerge.

In the past few decades, Artificial Intelligence university groups, such as the Decision Systems Laboratory of the University of Pittsburgh, have developed Bayesian approaches to support decision making in situations where one has to weigh gains and costs versus risks. This paper will describe details of such an approach and will provide some examples of both discrete random variables, such as the probability values in a LOPA, and continuous distributions, which can better reflect the uncertainty in data.

1. Introduction

Most successful tools in analyzing technical aspects of process safety over the years have shown to be HAZOP and LOPA, where in fact LOPA scenarios have been emerging from HAZOP studies. Protective barriers, layers of defense, and more specifically layers of protection have become a corner stone for achieving safe operations in process industry. Where HAZOP has been already with us since the seventies, LOPA's breakthrough was early in 2000 after it had been presented as a method in the second half of 90s. Of course, the thinking is older, is quite intuitive, and has been applied for a long time by the nuclear industry and the military, but the striking, eye-catching presentation in the form of the leaves of an onion and more technically as the branches of an event tree with at its root the initiating event made it immediately comprehensible and so successful. Contributing to LOPA's success was the practice of joint thinking and brainstorming in a multidisciplinary team focused on a particular scenario.

Usually after a qualitative start, further development of a method leads to quantification. Quantification sharpens the mind and makes the method more predictive and therefore more useful for risk management. Quantification has also been stimulated by the development of highly reliable safety instrumented systems. In the middle of 90s it became possible to test electronic devices to such an extent that a high reliability could be guaranteed. This technology initiated the development of international standards such as IEC 61508 on functional safety of electrical/electronic/programmable electronic safety-related systems, and its follow-on for process industry IEC 61511. Safety Integrity levels were defined as well as extensive requirements for equipment providing these levels and methods of analysis. These standards promoted the use of a risk matrix with attached consequence matrix and quantitative risk acceptance criteria.

Safety gained by layers of protection is the result of the extent in which, given the case, the assumed scenario of initiating event and follow-on events of functioning of protection layers, covers with sufficient accuracy what will happen in reality. This gained safety will be with respect to time history and severity of events, reliability of start of functioning of the layers and their protective effectiveness with all its aspects on the one hand, but what can be afforded on the other. Hence what limitation of investment and maintenance cost will allow, and thus the question of how safe is safe enough, has to be solved early on, and in that case quantification becomes a necessity. Quantification creates the need for expected frequency data of an initiating event and reliability of the

* Corresponding author.
E-mail address: hjpasman@gmail.com (H. Pasman).

0950-4230/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jlp.2012.07.016

layers and hence reliability of components. Collecting these data is not a negligible task to say the least, but reliability engineering and fault tree methodology, already developed for a number of decades is available, while event tree analysis was a known approach from quantitative risk analysis. A first attempt in quantifying was focused on failure frequencies by assuming the layers in a certain scenario function one by one successively while the functioning of a later layer is not affected by the failing of the earlier ones, hence the layers are expected to act independently. By knowing the probability values of failure on demand, the overall failure frequency can easily be calculated as the product of initiating event frequency and the assumed independent probability values. And doing this by the rounded logarithms one could do this even by heart. However, successful functioning of a layer does not mean there will be no cost consequence: the least cost will be an interruption of the process, but with failure on demand of one or more layer functions, the damage will increase from equipment clean-up, to small fire damage, large fire and possibly explosion damage, and because of potential extensive equipment damage, costs will include business interruption. A full cost–benefit analysis would encompass these potential damages as well as costs of investments in layers, testing and maintenance, and spurious false alarms.

Process industry installations and their operations are complex, which leads to a myriad of possibilities that something can go wrong. It means that for analysis one has to resort to a limited number of scenarios covering a range of possibilities represented by a probability distribution rather than dealing with each possible scenario individually. It also causes one to easily lose overview when considering scenarios of developing mishaps. Scenario development including probability of occurrence of an unwanted event has been an Achilles heel of QRA. Painstaking analysis such as HAZOP and FMEA are helpful but do not provide overview. A great step forward in methodology, initiated in Shell, to obtain better overview is a bow-tie combination of a fault tree on the left and an event tree on the right. An example with one of the possible scenarios indicated is shown in Fig. 1. The 90° clockwise rotated fault tree is connected via the top event, the initiating or critical event of an imminent hazardous material spill, to the base of an event tree. The latter is branching out from the initiating critical event to potential consequences of explosion, fire, and toxic dispersion. In the fault tree the preventive barriers and in the event tree the protective layers can be shown. The connecting lines from a fault tree basic fault to any event tree branch end consequence form a scenario, so one bow-tie can show many scenarios. Quantitative risk analysis (QRA) is an ultimate tool to cope with complexity and to obtain a resulting spectrum of plant risks based on defined scenarios. Its results are however afflicted with uncertainty due to underlying uncertainty in data and models without making uncertainty explicitly visible (Pasman, Jung, Prem, Rogers, & Yang, 2009). Specialized QRA software packages are not very transparent and not sufficiently flexible to model the effects of preventive and protective devices. So, ways to improve and better support decision making shall be investigated.

Lately Bayesian statistics and Bayesian Networks became more available for practical use. The crux of the Bayesian approach is building on existing data and absorbing new knowledge to lower uncertainty and to improve understanding of complex systems. As learning from the past is a must to improve safety, a Bayesian approach deserves a close look. We shall here show some possibilities of applying these new methods.

2. Bayesian statistics and Bayesian networks

The statistical theorem named after Bayes tells us how to update a probability distribution of values of a parameter. If applied to a failure rate, λ, we don't consider it as a single value variable but as a random variable expressed in the form of a probability density function (pdf). We then determine a posterior pdf given E, which is newly observed evidence. This posterior distribution can be derived from the product of a prior distribution of failure rate values, $f(\lambda)$, and the new information as a likelihood function, $L(E|\lambda)$ according to:

$$f(\lambda|E) = \frac{f(\lambda)\cdot L(E|\lambda)}{\int_0^\infty f(\lambda)\cdot L(E|\lambda)\,\mathrm{d}\lambda}$$

The likelihood function represents the probability that E is observed given a value of λ, and the denominator integral serves to normalize the result of the product to keep probability values between 0 and 1. With little information to start with as a prior distribution, a uniform distribution can be assumed, while for a likelihood function, in case of a constant failure rate, a Poisson distribution is suited. A derivation of the Bayes theorem can be found in, e.g., Jaynes (2007) and applications on failure frequencies in, e.g., Modarres, Kaminskiy, and Krivtsov (2010) and Hauptmanns (2011).

Updating, inference, and diagnosis are features of Bayesian Networks, also called Bayesian Belief Nets, BNs or BBNs, which makes it a very attractive graphic tool to organize one's knowledge on causal chains. BNs belong to the family of Directed Acyclic Graphs, DAGs, shorter called acyclic digraphs. Also Fault Tree, Event Tree, Bow-tie, and Master Logic Diagram known in process safety for representing cause-consequence event chains, belong to this family. As shown in Fig. 4 the BN-structure consists of nodes, usually drawn as ellipses, and connecting arcs, represented as arrows. BNs feature a number of advantages over the mentioned traditional methods. The nodes contain (random) variables with their probability information or operations between functions, while the directional arcs represent causal influence relationships. One distinguishes discrete probability distribution nets, Gaussian distribution nets, and mixed discrete/continuous nets, the latter can even be non-parametric. Starter nodes, independent of other nodes, in Fig. 4, e.g., the node named 'initiating event', are called parents, while nodes further down the structure are called children: a child can be the source for a connected follow-on child, also called sink node. The structure does not need to have one parent or one child at the end as a target node but there can be many, while also cross connections are possible as long as it does not lead to cycles. The net is therefore highly flexible. Nodes can be also just functional, while others can contain expert opinion, hence subjective information. Because of the latter the structures are called belief nets.

The discrete nets calculate conditional probability value tables (joint distributions) of the random variables corresponding to linked nodes, each variable representing, e.g., states of a process component. These tables are conditional on the marginal distributions of the variables of the connected source nodes. This is an accurate process. With binary variables (success/fail) as in many LOPA cases, this kind of net is very well suited. Practical software called SMILE with the graphical network interface GeNIe running under the Windows operating system, has been developed by the Decision Systems Laboratory of the University of Pittsburgh and is freely available from there for personal use (DSL, 2010). It can be used at different levels of detail depending on the problem at hand. It is built for Excel, so the tabled results can be further used in spreadsheets. In each node the variable and its values have to be defined while after arcing and updating, the resulting conditional probability tables can be viewed. Decision analysis is carried out by