Reliability Engineering and System Safety 154 (2016) 127–136

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Vulnerability analysis of process plants subject to domino effects

Nima Khakzad [a,*], Genserik Reniers [a], Rouzbeh Abbassi [b], Faisal Khan [b,c]

[a] Safety and Security Science Group, Delft University of Technology, The Netherlands
[b] Australian Maritime College, University of Tasmania, Australia
[c] Centre for Risk, Integrity, and Safety Engineering (C-RISE), Memorial University of Newfoundland, Canada

ARTICLE INFO

Article history:
Received 26 December 2015
Received in revised form
7 May 2016
Accepted 5 June 2016
Available online 7 June 2016

Keywords:
Domino effect
Dynamic Bayesian network
Graph metrics
Process plant

ABSTRACT

In the context of domino effects, vulnerability analysis of chemical and process plants aims to identify and protect installations which are relatively more susceptible to damage and thus contribute more to the initiation or propagation of domino effects. In the present study, we have developed a methodology based on graph theory for domino vulnerability analysis of hazardous installations within process plants, where owning to the large number of installations or complex interdependencies, the application of sophisticated reasoning approaches such as Bayesian network is limited. We have taken advantage of a hypothetical chemical storage plant to develop the methodology and validated the results using a dynamic Bayesian network approach. The efficacy and out-performance of the developed methodology have been demonstrated via a real-life complex case study.

1. Introduction

Severity of consequences of potential hazards in a system is a function of both the magnitude of hazards and the vulnerability of the system. In other words, exposed to the same level of hazard a system with higher vulnerability is susceptible to larger damages and thus suffering higher levels of risk. Johansson et al. [1] use the term vulnerability to address the inability of a system to withstand the failures. In the context of domino effect modeling, Khakzad and Reniers [2] defined the domino effect vulnerability as the capability of a plant to escalate a primary accident (fire or explosion) to higher order accidents (e.g., secondary fires and explosions). For the purpose of the present study, we adopt the definition by Khakzad and Reniers [2] and define domino vulnerability as the susceptability of a plant which allows a primary accident to spread throughout the plant via cascading effects, triggering secondary accidents, and so on. Compared to traditional risk analysis which is aimed at identification of hazards and estimation of the system failure probabilities, vulnerability analysis is usually performed to pinpoint the system components the failures of which contribute most to the cascading of failures not only within the system of interest but also across other interdependent systems. As such, the emphasis of vulnerability analysis is more on the extent of failures rather than the probabilities thereof although the incorporation of the vulnerability analysis in the probabilistic risk analysis can address both.

Over the past two decades, the issue of cascading effects in complex and interdependent systems such as water distribution networks [3], power grids [4,5], and process plants [6–15] has drawn much attention. The increasing trend in modeling and risk analysis of cascading effects – better known as domino effects in hazardous industries such as process plants – mainly lies in the fact that such cascading failures, although rare, can result in catastrophic consequences. Compared to other infrastructures, however, the potential consequences of domino effects in process plants[1] can be much more severe owing to the presence of hazardous materials such as flammable, explosive, and toxic substances. For example, a series of explosions in a LPG[2] storage plant in Mexico in November 1984 left around 600 deaths and 7000 severe injuries; similarly, a series of fires and explosions in Buncefield oil storage depot in the U.K in December 2005 led to the largest fire in peace time Europe, leaving 43 injuries and incredible property damages.

Compared to long-established methods for accident modeling and risk analysis of domino effects in process plants, relevant work in the field of vulnerability analysis has been relatively few [13,15,16]. In most previous work, however, either a full simulation of potential domino effects has been performed to identify the units contributing the most to the vulnerability of the plant or an iterative deterministic analysis has been carried out with one

* Corresponding author.
E-mail address: n.khakzadrostami@tudelft.nl (N. Khakzad).

[1] In the present work we use the term process plant as a general expression to refer to a wide variety of plants including but not limited to chemical plants, petrochemical plants, and oil and gas refineries.

[2] Liquified Petroleum Gas.

http://dx.doi.org/10.1016/j.ress.2016.06.004
0951-8320/

failure at a time to evaluate the extent of the failure cascade. Regardless of which aforementioned approaches is used, simulations can turn out too time-consuming and even intractable in case of large process plants containing many process installations and equipment.

Many infrastructures such as water distribution networks, power grids, process plants, and communication networks can be displayed as graphs in an abstract form, where the components of the infrastructure are represented as nodes, and the flows of materials, energy, or information among the nodes are denoted as edges. Accordingly, some graph metrics have been suggested to infer about the attributes of the graph (infrastructure) under consideration. In this regard, graph metrics have been used to investigate the robustness of (single) communication networks with regard to technological errors or man-made attacks [17], vulnerability of (joint) interdependent networks (power network and Internet communication network) to the cascading effect of random node failures [18], vulnerability analysis of water distribution networks [19], and vulnerability analysis of process plants in the context of domino effects triggered by terrorist attacks [20] or random failures [2].

Following the work of Khakzad and Reniers [2], in the present study we examine the reliability and efficacy of graph theory (graph metrics) in domino vulnerability analysis of process plants under multiple accident scenarios and varying environmental conditions. We validate the results obtained from graph theory using a dynamic Bayesian network (DBN) methodology developed by Khakzad [15]. The efficacy of the developed methodology is demonstrated via a real case study. To this end, a short review of Bayesian networks is given in Section 2. The graph theory and graph metrics are presented in Section 3, while the development, validation, and application of the methodology are demonstrated in Section 4. The main conclusions drawn from this work are presented in Section 5.

2. Bayesian networks

2.1. Ordinary Bayesian networks

Bayesian network (BN) is a probabilistic tool for reasoning under uncertainty, where the nodes represent random variables and directed arcs imply local conditional dependencies between parent and child nodes [21,22]. The type and strength of such conditional dependencies are defined by means of conditional probabilities assigned to the nodes. Those parent nodes which are not children of other parent nodes – so-called root nodes – are assigned marginal probabilities. satisfying the Markov condition,[3] BN factorizes the joint probability distribution of a set of random variables $U = \{X_1, X_2, \ldots, X_n\}$ as the product of marginal and conditional probabilities of nodes:

$$P(U)=P(X_1, X_2,\ldots, X_n)=\prod_{i=1}^{n} P(X_i \mid pa(X_i)) \tag{1}$$

where $P(U)$ is the joint probability distribution of variables and $pa(X_i)$ is the parent set of variable X_i. For example, considering the BN of Fig. 1, the joint probability distribution of the variables can be defined as $P(X1,X2,X3,X4) = P(X1)\cdot P(X2 \mid X1)\cdot P(X3 \mid X1,X2)\cdot P(X4 \mid X2)$.

BN takes advantage of Bayes' theorem to update the probability of variables given new information E – also known as evidence – to yield the updated probability:

[3] According to Markov condition, in a Bayesian network a node is conditionally independent of its non-descendants given its parents. For example, in Fig. 1, X3 is independent of X4 given X1 and X2, i.e., P(X3 | X1, X2, X4) = P(X3 | X1, X2).

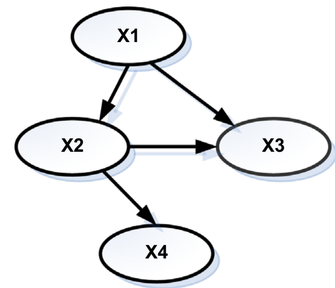

Fig. 1. A typical ordinary Bayesian network.

$$P(U|E)=\frac{P(U)\cdot P(E|U)}{\sum_{U/E} P(U)\cdot P(E|U)} \tag{2}$$

where $P(U \mid E)$ is the updated joint probability; $\sum_{U/E}(.)$ is the summation over all values of U except E.

2.2. Dynamic Bayesian network

Dynamic Bayesian network (DBN) is an extension of ordinary BN [22,23] that, compared to its ordinary ancestor, facilitates explicit modeling of temporal evolution of random variables over a discretized time line. Dividing the time line to a number of time slices, DBN allows a node at i-th time slice to be conditionally dependent not only on its parents at the same time slice but also on its parents and itself at previous time slices. However, usually only two time slices are considered in the modeling, so that the joint probability distribution of a set of random variables at time $t+\Delta t$, that is $P(U^{t+\Delta t})$, can be expanded as:

$$P(U^{t+\Delta t})=P(X_1^{t+\Delta t}, X_2^{t+\Delta t},\ldots,X_n^{t+\Delta t}) = \prod_{i=1}^{n} P(X_i^{t+\Delta t} \mid X_i^t, pa(X_i^t), pa(X_i^{t+\Delta t})) \tag{3}$$

where $X_i^{t+\Delta t}$ and X_i^t are the copies of X_i in two consecutive time slices with a time interval of Δt, and $pa(X_i^{t+\Delta t})$ and $pa(X_i^t)$ are the parent sets of X_i at the time slices $t+\Delta t$ and t, respectively.

Fig. 2 depicts a DBN as a replication of the BN of Fig. 1 over three consecutive time slices. The directed arcs connecting the nodes in the same time slices are called intra-slice arcs (black arcs in Fig. 2) while the arcs linking the nodes in consecutive time slices are called temporal or inter-slice arcs (red arcs in Fig. 2). According to the DBN in Fig. 2, the conditional probability of X_3, for example, at the time slice of $t+\Delta t$ would be $P(X_3^{t+\Delta t} \mid X_3^t, X_1^{t+\Delta t}, X_2^{t+\Delta t})$.

Conventionally, the DBN can be represented as Fig. 3, in which an arc from a node to itself (represented by red arcs in Fig. 3) denotes the temporal evolution of the node, taking place from a time slice to the next (i.e., within Δt). The higher order temporal evolutions can be denoted as numbers attached to the temporal arcs.

3. Graph theory

A mathematical graph is an ordered pair $G = (V, E)$ where $V = \{v_1, v_2, \ldots, v_n\}$ and $E = \{e_1, e_2, \ldots, e_m\}$ denote sets of n vertices (nodes) and m edges (directed or undirected), respectively. In a weighted graph, a set of numerical values can also be assigned to either the nodes or edges of the graph. In this case, the weighted graph can be presented as $G = (V, E, W_V, W_E)$ where W_V and W_E are weight vectors allocated to the vertices and edges, respectively.