Journal of the Brazilian Computer Society

RESEARCH Open Access

Stochastic modeling and analysis of vapor cloud explosions domino effects in chemical plants

Diego Sierra[1†], Leonardo Montecchi[2*†] and Ivan Mura[3†]

Abstract

Because of the substances they process and the conditions of operation, chemical plants are systems prone to the occurrence of undesirable and potentially dangerous events. Major accidents may occur when a triggering event produces a cascading accident that propagates to other units, a scenario known as *domino effect*. Assessing the probability of experiencing a domino effect and estimating the magnitude of its consequences is a complex task, as it depends on the nature of the substances being processed, the operating conditions, the failure proneness of equipment units, the execution of preventive maintenance activities, and of course the plant layout. In this work, we propose a stochastic modeling methodology to perform a probabilistic analysis of the likelihood of domino effects caused by propagating vapor cloud explosions. Our methodology combines mathematical models of the physical characteristics of the explosion, with stochastic state-based models representing the actual propagation among equipment units and the effect of maintenance activities. Altogether, the models allow predicting the likelihood of major events occurrence and the associated costs. A case study is analyzed, where various layouts of atmospheric gasoline tanks are assessed in terms of the predicted consequences of domino effects occurrence. The results of the analyses show that our approach can provide precious insights to support decision-making for safety and cost management.

Keywords: Vapor cloud explosion, Stochastic models, Domino effect, Risk analysis, Cost analysis

Introduction

Chemical process plants are an example of critical systems. In these systems, the occurrence of undesirable events such as leakage of materials, uncontrolled fires, and even explosions may result in catastrophic consequences, including harm to human life integrity.

The consequences of an undesirable event may be disastrous, and the magnitude of effects depends on several factors. Some of these factors are easier to consider, such as the characteristics of the materials being processed (e.g., reactivity, flammability) and the operational conditions (e.g., temperature, pressure). Some others, such as the consequences of a wrong plant design or the incorrect management of equipment are more difficult to understand and to account for. Catastrophic events are usually related to an initial hazardous event or scenario, which subsequently escalates to greater and more dangerous magnitudes. Escalation may trigger a chain of unwanted events whose effects progressively increase both in space and time, until producing a single, major accident. When this happens, we talk about a failure *domino effect* [3].

Failure domino effects in chemical plants can occur because of a handful of reasons. The very first occurring event in the chain of unwanted scenarios is known as the *triggering* or *initiating* event. This is usually a fire (either pool fire, jet fire, flash fire, fire ball, etc.) or an explosion, e.g., a vapor cloud explosion (VCE), or a boiling liquid expanding vapor explosion (BLEVE). Subsequent events can be of any kind, and they are not necessarily mutually exclusive, meaning that a triggering jet fire can end up causing both a BLEVE and a fireball [36].

*Correspondence: leonardo@ic.unicamp.br
†Diego Sierra, Leonardo Montecchi and Ivan Mura contributed equally to this work.
[2]Universidade Estadual de Campinas, Campinas, Brazil
Full list of author information is available at the end of the article

In this paper, we study the domino effect of VCEs, where both the main triggering event and the subsequent events are VCEs [16]. VCEs occur when a large amount of flammable material is released into partially congested atmospheres and such material does not ignite immediately [14]. Rather, it accumulates and generates a cloud of flammable vapor, i.e., gas or mist, with enough chemical energy to generate flame speeds that accelerate to sufficiently high velocities to produce significant increase of vapor pressure (*overpressure*).

VCEs are particularly dangerous because they can easily provoke explosions that lead to domino effects, due to the accumulation of flammable materials in a growing cloud [22]. The explosions generated from such events can rise to destructive levels, making them one of the worst possible cases in chemical industry. Analyzing domino effects of VCEs is thus of special importance for guaranteeing the safety of plants in this industrial domain [17].

The objective of this work is to help understanding safety hazards in chemical plants, by proposing a systematic methodology to quantify the probability of occurrence of failure domino effects after an initiating VCE event. To this end, we propose a modeling methodology that combines mathematical models of the physical characteristics of the explosion, with stochastic state-based models representing the actual propagation among equipment units and the effect of maintenance activities. In particular, we use the multi-energy method [3] for blast estimation, and discrete-time Markov chains (DTMCs) [35] and stochastic activity networks (SANs) [31] for the modeling of propagation effects.

The approach consists of three phases: (i) we first characterize the likelihood of occurrence of VCEs affecting chemical process units, then (ii) we model the consequences of a VCE in terms of the impact that the energy release may have on neighboring units, and finally, (iii) these two elements of risk are embedded into stochastic state-based models that are used to represent the spatial arrangements of equipment and to simulate the propagation of events, finally estimating the probability of domino effects affecting different equipment units.

This paper is an extended version of [33]. With respect to such work we provide the following extensions:

- We allow for a more accurate characterization of the failure process of individual equipment units. While in [33] the failure times were exponentially distributed, which means only constant failure rates were considered, we now generalize failure times so that they can be gamma distributed. The gamma family of distributions, which includes the exponential one as a special case, can model the effects of the equipment aging process, such as wearing, on the failure rate.
- We provide an analytic model based on DTMCs for analyzing the domino effect. While in [33] the analyses required discrete-event simulation for all the metrics of interest, the DTMC model can provide exact results for a subset of them.
- We extend the SAN models to consider maintenance activities. Compared to [33], more interesting scenarios can now be analyzed, in which the probabilistic losses that might occur due to domino effects can be traded with the certain costs to be paid for maintaining equipment units in the plant. Cost analyses can thus be conducted to identify the most profitable schedule of maintenance activities.
- Finally, we restructure the document and we add three new sections with a deeper discussion of background, related work, and limitations.

The rest of this paper is organized as follows. In the "Vapor cloud explosions" section, we introduce the necessary background on VCEs, while in the "Related work" section, we discuss the work related to this paper. In the "Modeling methodology" section, we provide an overview of the modeling methodology and we define the metrics of interest that we aim to estimate. The "Modeling of one-step VCE propagation" section details the mathematical modeling of the physical characteristics of a VCE and its propagation to nearby units, while the "Modeling of domino effects" section presents state-based stochastic models that will be used to estimate the propagation of failure domino effects. In the "Case study" section, a case study based on atmospheric gasoline tanks is presented and modeled using our methodology, providing an example of application. Finally, in the "Limitations to validity" section, we discuss the main limitations of the methodology, and in the "Conclusions and future work" section, we present concluding remarks and we discuss possible future enhancement of this work.

Vapor cloud explosions

Equipment in a process plant may fail, causing unwanted consequences. For a failure to happen, a root cause (also called initiating event) must firstly occur. Then, other intermediate events may happen until the occurrence of the final failure effect or failure mode. After a failure has occurred, it may produce more severe consequences (also called final events), which may also depend on other external events.

The main focus of this work are VCEs, which are final events. In the middle, the considered failure mode is the loss of containment, i.e., a leak. A VCE event is essentially the explosion of a "vapor cloud," an agglomeration of an important amount of flammable mass. Such a cloud can be formed due to the accumulation of vapors or from liquid spills that are subsequently evaporated.

Once the cloud is formed, there is a risk it may explode. However, in order for the cloud to be able to produce an explosion, the following three main conditions must hold.

1. The substance in the cloud must be within its flammability limits. These are temperature limits within which it is possible for a flammable substance to ignite, depending on the kind of substance.
2. Ignition must be delayed. In case the cloud starts burning before it is completely formed, other fire scenarios would occur instead of a VCE. Such other events are out of the scope of this paper.
3. Turbulence must be present in the cloud. The release mode of the substance (a jet, for instance) can trigger this turbulence. Interaction with close-by objects may also work as partial confinement and generate turbulence within the cloud.

Once the explosion happens, a part of the chemical energy produced by the combustion reaction will turn into mechanical energy, resulting in a blast wave. Blast waves produce a pressure increase that builds up in a first moment due to the combustion, but that subsequently diminishes thanks to the expansion of gasses [24]. This increase of pressure is called *overpressure*, and it characterizes the blast wave of any explosion. The amount of overpressure depends on the type of explosion. In this work, we focus on detonation processes (i.e., large and instantaneous explosions) [10].

Immediately after the explosion starts, an overpressure peak is produced, which moves through space, diminishing as distance increases. *Blast estimation* methods model the dependence of the produced overpressure on the distance from the detonation point and the amount of released mass. They thus permit quantifying the overpressure experienced at a certain distance from the explosion point.

There is not a single agreed way of performing blast estimation, and three main methods are most commonly used:

– *TNT equivalency*, which first calculates the equivalent mass of trinitrotoluene (TNT) that would generate such explosion, and then uses this value for further overpressure calculations.
– *Multi-energy*, which bases its calculations on the fact that the explosion behavior is in large part determined by confined parts of a vapor cloud.
– *Baker-Strehlow-Tang*, which differs slightly compared to the multi-energy method in that the strength of the blast wave is proportional to the maximum flame speed that the cloud has reached. In this model, the speed is an input parameter.

In this work, we will use the multi-energy method as the basis for overpressure calculation, given its simplicity in terms of required input parameters and its wide acceptance concerning the faithful representation of the dynamics of an explosion [26].

Related work

VCEs are regarded as one of the potentially most disruptive events in industrial plants. For this reason, several works have analyzed their behavior, their possible causes, and their consequences. However, to the best of our knowledge, a comprehensive methodology is not yet available, and VCEs modeling is still an active research field.

Different aspects of VCE modeling are being investigated in the literature. Some works focus on the initiation process, that is, the triggering of an initial VCE. For example, the authors of [28] estimate the probability of the occurrence of a VCE based on stochastic variables like frequency of material release, probability of not having an immediate ignition, and meteorological conditions.

A major challenge in studying VCEs lies in the fact that their impacts are difficult to be quantified. For this reason, many works focus on modeling the direct effects of a VCE, which consists in estimating the energy released by the explosion and the propagation of the blast. Although some well-known blast estimation methods exist (e.g., the multi-energy method, see above), they only provide an approximated result. Research work is thus devoted to improve the accuracy of these methods, or understanding VCE behavior under specific conditions.

The authors of [36] propose a method for taking into account channelling and shielding effects when estimating the blast pressure, while in [11], the authors studied the blast wave of elongated VCEs. In fact, most work assumes that the cloud of flammable material participating in the VCE is hemispherical, which is however rarely the case, due to congestion caused by other equipment. More in general, the authors of [37] examine the effect of the geometrical shape of the flammable cloud on the explosion, analyzing a constant volume of clouds with different height-width ratios and length-width ratios. Other works, as in [13], focus on the prediction of the VCE blast resulting from the leakage of a specific material.

Another research direction consists in validating the existing models. The authors of [27] studied and calibrated the multi-energy method in different scenarios, by comparing the obtained results with detailed computational fluid dynamics simulations. More recently, the authors of [2] extended a method for blast estimation from the literature and compared its predictions with the damage observed in four real historical accidents. Some studies have performed risk assessments on VCEs [1], although very few have tried modeling and assessing the impact of domino effects caused by VCEs.

Petri nets and their extensions are widely used for the assessment of safety-critical systems and critical infrastructures. For example, the authors of [12] used (untimed) Petri nets to model interdependencies between critical infrastructures and to verify that specific invariants are not violated. SANs have been used in [21] to define an approach for the evaluation of the risk associated with the execution of maintenance operations on petroleum installations. Similarly, the work in [6] defined a framework based on SANs to model and evaluate the impact of cascading effects in electric power systems.

To the best of our knowledge, few works have used stochastic models to characterize domino effects caused by VCEs. The authors of [40] use timed colored hybrid Petri nets (TCHPNs) to model response actions to flammable liquid tank fires. The focus is on comparing different emergency strategies to avoid the domino effects, and not on evaluating the consequences. The recent work in [15] gives a definition of vulnerability index of tanks in the context of a domino effect scenario and proposes a methodology to evaluate it, by combining different techniques. However, they do not consider maintenance effects.

The work in [38, 39] proposes a methodology based on Petri nets to model the cascading effect of VCE accidents, and it is perhaps the most similar to ours. However, our work takes also into account for: (i) time, (i) the effect of maintenance, and (iii) costs. Furthermore, we adopt a modular approach in the construction of the model, which simplifies its adaptation to different scenarios.

Modeling methodology

VCEs are dangerous events that besides entailing capital losses and operation disruptions also represent extreme safety hazards for personnel operating in chemical plants. An explosion occurring at an element of the process may propagate to other equipment units and produce other kinds of unwanted events. In this work, we restrict ourselves to consider only initiating events of VCE type, and we also assume that secondary or propagated ones are also of that type, ignoring other unwanted events different from VCEs.

In the following, we provide an overview of the proposed methodology ("Overview" section), together with the main assumptions on which it is based ("Assumptions" section), as well as the measures of interest that we aim to calculate ("Metrics of interest" section).

Overview

The proposed modeling methodology is described graphically in Fig. 1. The figure describes the workflow that should be followed for modeling and analyzing VCE domino effects in a generic industrial plant.

We model VCEs as probabilistic events, according to the following three steps: (i) initiation modeling, (ii) propagation modeling, and (iii) domino effects modeling. *Initiation modeling* basically consists in characterizing the failure process, that is, determining the probability distribution of initiating events. *Propagation modeling* consists in determining the individual (i.e., one-step) propagation probabilities between equipment units i and j, based on their distance and on mathematical models of VCE physical characteristics. Finally, in *domino effects modeling*, such information is aggregated into different types of probabilistic models, namely DTMCs and modular SANs models, that can represent the domino effect process. Such models are solved analytically and evaluated by discrete-event simulation to obtain the final metrics.

Initiation modeling

Models for the distribution of the time to the occurrence of different types of failures have been proposed in the literature. Commonly accepted approaches for industrial processes equipment are to use the Weibull [5] or gamma distributions [34] to represent the random nature of failure times. Both these distributions have the particularity of being characterized by the *rate* and the *shape* factor, which makes them particularly convenient for representing the aging process of equipment.

In this work, we use the gamma distribution to model the time to failure of an equipment unit, that is, the time to the occurrence of an initiating event (i.e., a VCE) caused by that unit. The gamma distribution is commonly used to model fire-related initiating events similar to those we consider in this paper. For example, in [34], the gamma distribution was used to model "fire or explosion" and "large release" events on hydrogen containment equipment.

The specification of a gamma distribution requires two parameters, a *rate* λ and a *shape* k. The rate parameter can be interpreted as the frequency of "shocks" (i.e., adverse events) to which the equipment is subject, while the shape can be interpreted as the number shocks until failure [23], thus effectively modeling degradation caused by aging. When the shape parameter is $k = 1$, the distribution coincides with the negative exponential distribution with constant failure rate λ, thus reducing to the case we previously considered in [33].

Suppose the chemical plant comprises a set $E_1, E_2, \ldots, E_n$ of n equipment units. We model the time-to-failure (TTF) of equipment unit E_i as being an independent non-negative random variable TTF_i, with known gamma probability distribution of parameters $\lambda_i > 0$ and $k_i > 0$. The cumulative distribution function

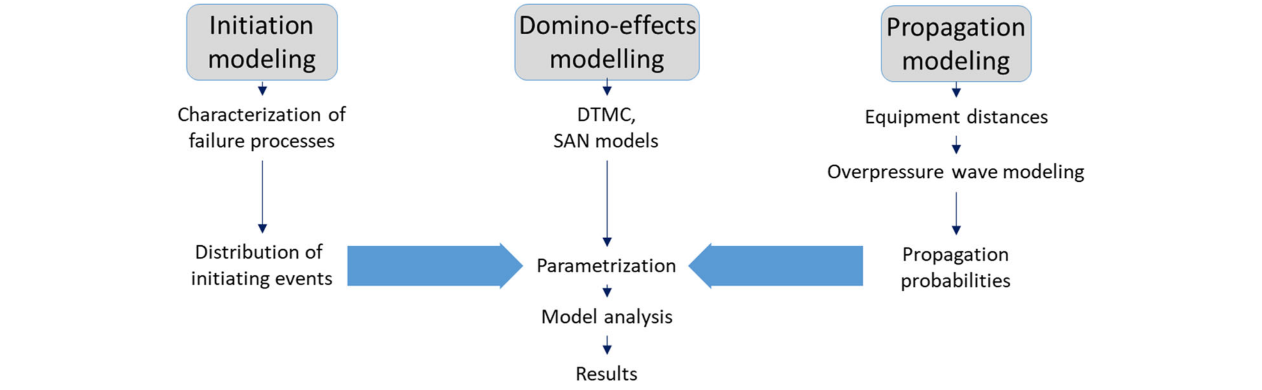


Fig. 1 Workflow of the proposed modeling methodology

of TTF_i has the following analytic form [23]:

$$\mathrm{Prob}[\,\mathrm{TTF}_i \leq t] = \frac{\gamma(k_i, \lambda_i t)}{\Gamma(k_i)}, \quad t \geq 0,\ i = 1, 2, \ldots, n, \quad (1)$$

where the parameter t represents the current time, $\Gamma(k)$ is the gamma function, and $\gamma(k, t)$ is the lower incomplete gamma function [23], i.e.:

$$\Gamma(k) = \int_0^\infty t^{k-1} e^{-t} dt, \quad (2)$$

$$\gamma(k, t) = \int_0^t t^{k-1} e^{-x} dx. \quad (3)$$

The expected value of the time to failure of equipment i is given by:

$$\mathrm{E}[\,\mathrm{TTF}_i] = \frac{k_i}{\lambda_i}. \quad (4)$$

The initiating VCE event may occur at any of the equipment units. The time of its occurrence is a random variable $\mathrm{T}_{\mathrm{init}} = min_i\{\mathrm{TTF}_i\}$. We will only consider one initiating event, and all the other VCEs that may possibly happen would be caused by direct or indirect propagation of the initial one. We made this choice because in this work *we want to analyze the domino effects of a single VCE initiating event in isolation*. While it would be perfectly possible to consider multiple initiating events with our approach, it would make it impossible to establish the relative contribution of each single initiating event on the observed final effects.

Propagation modeling

For a chain of failure events to occur, the energy released in the initiating VCE must be sufficiently high to affect the neighboring units. Obviously, the odds of event propagation depend not only on the amount of released chemical energy, but also on the closeness of other equipment and on the susceptibility of the involved substances to ignition. Moreover, the domino effect is not deterministic, but rather probabilistic (i.e., propagation may not happen).

Several studies in the literature have proposed statistical models to predict the likelihood of a piece of equipment being affected by the explosion of neighboring units (see the "Related work" section). Here, we use those mathematical models to parametrize state-based stochastic models that can represent the dynamic evolution of the state of equipment units, accounting for the occurrence of initial events and for the possible routes of VCE propagation. In particular, we base on studies in the literature to extract the probability p_{ij} of a failure of VCE type propagating from unit i to unit j, as a function of the distance between units and of the released energy. This step of the methodology is further detailed in the "Modeling of one-step VCE propagation" section.

Domino effect modeling

For the modeling of the actual domino effects, we will be considering two distinct approaches. First, we use the propagation probabilities to parametrize a DTMC model that can be used to analyze the consequences of an initial event, when the propagation times are abstracted. For these simplified scenarios, the DTMC allows obtaining the exact value of the metrics of interest when time is abstracted. Second, we build a stochastic Petri net model for representing the occurrence of the initiating and of the propagation events, this time explicitly modeling the event occurrence times. The Petri net model allows obtaining statistical approximation of all the metrics of interest via discrete-event simulation.

Petri nets are useful mathematical tools for modeling, analyzing and simulating different kinds of systems, which were initially proposed in 1962 by Petri in his Ph.D. dissertation thesis to model concurrent systems [25]. They have two basic types of modeling elements: places, depicted as hollow circles and representing state variables of the system, and transitions, depicted as empty rectangles, which represent system changes or occurrence of events. Places can contain tokens, which model entities, depicted as black dots, and the number of tokens in a place at a certain moment is called the *marking* of the place. Tokens are added or removed to/from places of a Petri net according to transitions and to the connections between places and transitions, which specify enabling for transitions as well as the changes in the marking of the places upon their occurrence.

The rules that specify the dynamic evolution of the marking are called *firing rules* [39], and they are easily understood by observing the example of a Petri net shown in Fig. 2. The example shows a possible modeling of the state of a unit which can be functioning (a state represented by place `Up`) or failed (modeled by place `Failed`). The event leading to failure requires a token in place `Cause` to be present in order to occur. Upon failure, a token will be deposited in place `Failure`, enabling the transition `Repair`, which restores the state of the unit, as well as transition `Propagation`, which as suggested by its name might be used to model a further cause of failure for another process unit.

Although the originally proposed Petri nets did not include probabilistic elements, it is quite natural to consider the time associated to transitions as being drawn from probabilistic distributions. This class of Petri nets is often called stochastic Petri nets (SPNs) [7]. The firing of tokens can be also dependent on complex functions of the markings, and it is possible to conduct Monte Carlo simulations to evaluate interesting measures about the likelihood of the occurrence of events. In this work, we use SANs [31], which can be considered an extension of SPNs. The SAN formalism is implemented in the Möbius modeling tool [8], which features useful extensions that allow for compact models and faster simulation. This step of the methodology is further detailed in the "Modeling of domino effects" section.

Assumptions

Our modeling methodology is based on a set of assumptions, which are listed in the following.

1. The time to failure of a process unit, causing leakage of flammable material, is characterized by a gamma distribution.
2. The only unwanted event resulting from leakage of flammable material is a VCE. In fact, in this work, we are specifically interested in assessing the probability of occurrence of a domino effect following a VCE event.
3. A failure occurring at a tank immediately causes a VCE. As explained in the "Modeling of one-step VCE propagation" section, this is not the case in reality, as some additional conditions must hold. However, by assuming a deterministic occurrence of VCEs upon unit failure, we are considering the worst-case scenario.
4. A process unit may be affected by a VCE only once for the duration of the analyzed scenario. We are in fact interested in analyzing a single domino effect chain in isolation.
5. Propagation of a VCE event to a nearby equipment, if it occurs, is instantaneous (i.e., the propagation delay is negligible).
6. The occurrence of a VCE event on equipment i causes a cost C_i^V for the plant owner, where the superscript V stands for VCE. This value considers both direct cost (e.g., damage to equipment) and indirect cost (e.g., plant downtime).
7. Preventive maintenance is performed periodically on equipment units. The maintenance period of equipment i is deterministic and denoted as T_i^M, where the superscript M stands for maintenance. After maintenance, the equipment is considered as good as new.
8. The execution of preventive maintenance of equipment i has a cost of C_i^M for the plant owner.

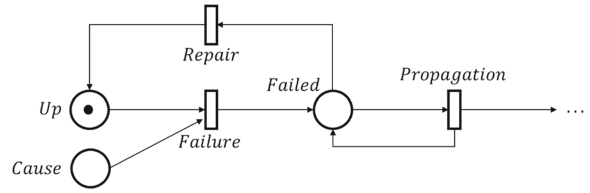


Fig. 2 Petri net example

These assumptions are reasonable considering that our objective is analyzing exactly the chain of VCE events. Relaxing these assumptions, particularly item 2 above, is part of our future work.

Metrics of interest

The objective of this work is to provide stakeholders (e.g., chemical plant owners) with a tool to compare different design choices in planning the layout of chemical infrastructures. For this reason, we focus on concise metrics that can provide a good indication of the safety (i.e., absence of catastrophic failures [29]) and the expected cost of the analyzed configuration. With this in mind, we define the following measures, where t represents time:

- $F^i(t)$, defined as the probability that unit i will be affected by a VCE not later than t.
- $N_{fail}(t)$, defined as the average number of process units that will be affected by a VCE before or on time t.
- $C(t)$, defined as the expected cost for the plant owner up to time t.

The first metric can be used as an indicator of the level of risk of unit i, for a given layout and a given time window. It can be used to identify the units that are subject to the highest hazard level. Instead, the second metric is an indicator of the safety level of the whole layout scenario, for a given time window. It can be used to comparatively evaluate different alternative layouts. Finally, the third metric is an indicator of the adequacy of the maintenance plan and can be used to identify the best trade-offs between maintenance frequency and chance of occurrence of domino effects.

To be able to calculate such metrics, we first have to characterize the occurrence of VCE events and their propagation ("Modeling of one-step VCE propagation" section), and then construct the model representing the domino effect ("Modeling of domino effects" section).

Modeling of one-step VCE propagation

As anticipated earlier, in this paper, we use the multi-energy method for overpressure calculation within the *propagation modeling* step (see Fig. 1). The multi-energy method for calculating the overpressure, for a given distance of interest, is summarized in the following steps [3].

1. *Cloud characterization.* This step aims at finding the amount of released mass in the cloud, which often requires dispersion calculations. Since these calculations are not the main focus of this work, an overall mass is approximated for cloud calculations. This mass must at least correspond to the stoichiometric quantity required for combustion to occur.
2. *Calculation of released energy.* The amount of released energy will correspond to the product of the volume of the mixture and the amount of energy released per cubic meter. The volume used in this step must take into consideration the mass calculated in the previous step. However, only the *confined part* of the cloud, i.e., the part of the cloud that is in a confined space or obstructed should be considered, as unconfined parts would burn out without significantly increasing the pressure.
3. *Distance scaling.* Scaling laws exist for modeling the physical properties of explosions, which relate the properties of blast waves from different explosions. Such laws allow extrapolating the blast wave properties of explosions from data obtained under different conditions (e.g., different amount of explosive, different distance). Based on E, the released energy calculated in the previous step, a *scaled distance* $\bar{R}$ is first calculated, as a function of the distance R and the atmospheric pressure P_a, as follows[1]:

$$\bar{R} = R\sqrt[3]{\frac{P_a}{E}}. \tag{5}$$

4. *Overpressure calculation.* From the scaled distance $\bar{R}$, a corresponding scaled overpressure can be found based on a Sachs-scaled side-on overpressure graph, as the one shown in Fig. 3. Such charts correlate dimensionless (scaled) values of overpressure and distance, based on the assumed source strength or severity of the explosion, which ranges from 1 (lowest) to 10 (highest). This value must be specified for the cloud according to level of confinement in the area. A value of 7 is used in this work (corresponding to congested areas). Once the scaled overpressure has been determined, the final overpressure value is found by a further rescaling by P_a, the atmospheric pressure value.

After the first event has happened (i.e., a vapor cloud has exploded), it can propagate to other equipment, resulting in a domino effect. That is, if other hazardous equipment is present nearby, the overpressure generated by the explosion may damage it, causing the release of additional flammable material, which in turn may generate other VCE events.

This propagation is not deterministic, but rather probabilistic, as it depends on several factors (e.g., released energy, distance). Several literature approaches have developed empirical models to relate escalation probabilities to overpressure received from a blast wave, e.g., [38]. The authors of [9] proposed a *probit* model to estimate the escalation probability from overpressure values of vapor cloud explosions in atmospheric tanks, by first determining a factor Y as follows:

$$Y = -18.96 + 2.44ln(\Delta P), \tag{6}$$

with ΔP being the overpressure, and then using $\phi(\cdot)$, the cumulative distribution function of the standard normal distribution, to calculate P_e, the escalation probability, as $P_e = \phi(Y-5)$. The obtained probability value P_e is thus the probability that a VCE event would escalate to another equipment located at a certain distance R, causing a subsequent VCE event.

Based on the specific scenario to be analyzed, such probability values need to be estimated for each value of the distance between pair of equipment that might propagate a VCE event. We shall be using these estimated probabilities to parametrize the DTMC and SAN models

[1] In the conference version of this paper [33], this formula wrongly appeared without the cube root for a mistake in the processing of the document. The number were however calculated with the correct formula, which is the one reported in Eq. 5.

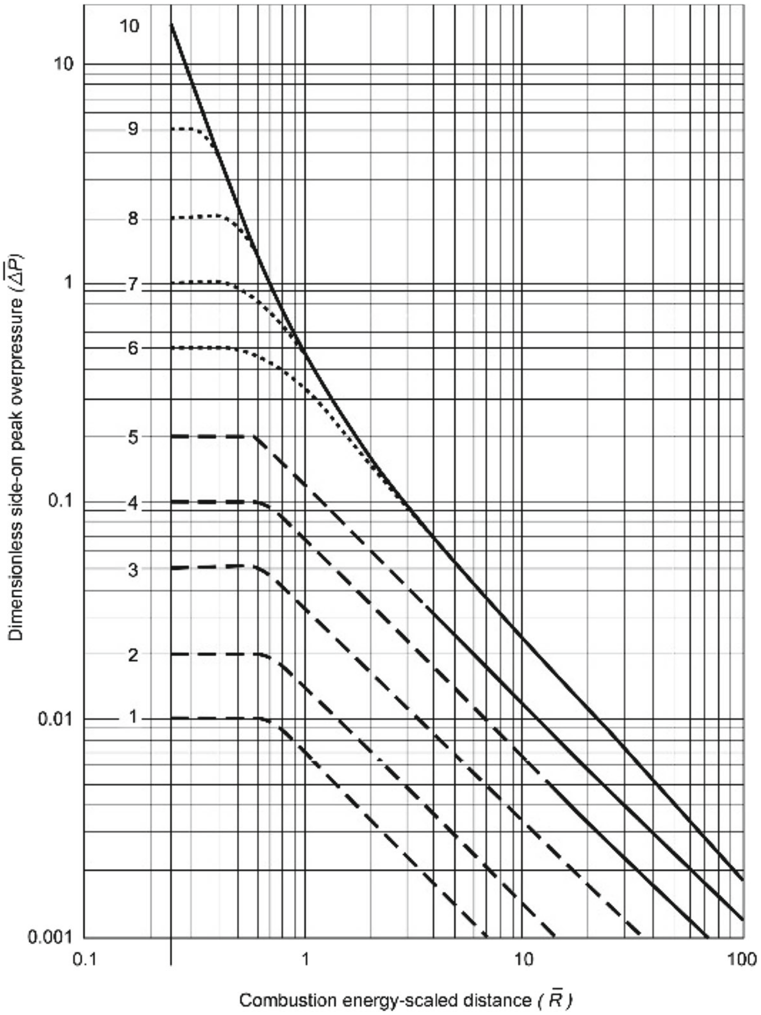


Fig. 3 Sachs-scaled side-on overpressure chart [3]

that allows predicting the likelihood of domino effects resulting from an initiating VCE.

Modeling of domino effects

In this section, we present two distinct types of models that can be used to estimate the metrics of interest defined in "Metrics of interest" section. We use a DTMC modeling to represent the propagation of VCEs once the initial event has occurred: since we are assuming propagation times are negligible, actual times can be totally abstracted and the study of domino consequences can be conducted in an exact way, without using simulation. Then, to deal with the time distribution of VCE initial events, we build SAN models of the equipment units, which can be composed to define a model of the whole plant, and analyzed by discrete-event simulation to determine time-dependent metrics of interest. In the following, we shall be describing the two modeling approaches.

DTMC model

For the sake of our modeling, we are here considering the chain of events that occur in a plant right after the occurrence of an initial VCE event, say on unit i, until no more explosion events can happen.

Let us suppose that a unit i in the plant just exploded. Then, each other equipment unit j will be subject to an overpressure wave and, depending on its distance from i, it will suffer a VCE with some known probability p_{ij}. In case j explodes, the same process will repeat and other units may be affected. If no unit explodes, the whole domino effect stops.

Since the times of propagation are negligible, we can model the system by a DTMC $\{X_m, m \geq 0\}$. The state variable of the process is the collection of the states of the n equipment units in the plant, i.e., $X_m = (U_m^1, U_m^2, \ldots, U_m^n)$ and the state of each unit can be in the discrete set $S_i = \{0, 1, 2\}$, where:

- 0 models the *initial* state, that is, the normal condition of the unit, susceptible to be affected by explosions;
- 1 stands for *active*, that is the unit is suffering the consequences of a VCE, and can propagate it to other units;
- 2 represents the final state *exploded*, when a unit has already suffered the consequences of a VCE, and cannot anymore propagate it.

A transition from the initial state 0 to state 1 will model the fact that a unit has been affected by an explosion. After reaching state 1, the next state of the unit will then become 2 with probability 1, and will not change anymore. However, before reaching this final state, the unit may propagate an explosion to all other units in state 0. The global state of the chain evolves in discrete-time according to the propagation of VCE events, i.e., the number of units in state 0 decreases over time and it becomes constant (it may reach zero) when the propagation process has stopped.

With such a state representation, the initial state of the model will be one of those in which exactly one unit is in state 1 and all other units are in the 0 state. The propagation process can continue until at least one unit is in state 1 and ends if the state does not include any unit in the 1 state. The total possible number of states is $3^n - 1$, because the state where all units are in state 0 is not included. The one-step transition probabilities between states of the chain can be expressed in terms of the explosion propagation probabilities p_{ij}. To provide a compact notation, it is convenient to introduce, for $x \in \mathbb{R}$ and $\vec{u} \in \mathbb{R}^n$, the indicator function $\mathcal{I}(x, \vec{u}) = (I(x, u_1), I(x, u_2), \ldots, I(x, u_n))$, where $I(x, u_i) = 1$ if $u_i = x$ and $I(x, u_i) = 0$ otherwise, for $i = 1, 2, \ldots, n$. For vectors in $\mathbb{R}^n$, we shall be denoting by $\|\cdot\|_1$ the norm-1 of a vector (the sum of the absolute values of the vector entries), and we will be using the comparison operator $\geq$ component-wise.

We can now describe $\theta_{\vec{u},\vec{v}}$, the probability that the DTMC $\{X_m, m \geq 0\}$ jumps from a state $\vec{u} = (u_1, u_2, \ldots, u_n)$ to a state $\vec{v} = (v_1, v_2, \ldots, v_n)$. Let us first observe that, for the transition probability to be non-zero, the following must hold of $\vec{u}$ and $\vec{v}$:

$$\|\mathcal{I}(0, \vec{u})\|_1 \geq \left\|\mathcal{I}(0, \vec{v})\right\|_1 \tag{7}$$

$$\mathcal{I}(2, \vec{v}) = \mathcal{I}(2, \vec{u}) + \mathcal{I}(1, \vec{u}) \tag{8}$$

Then, for any two states $\vec{u}$ and $\vec{v}$ that satisfy both Eqs. 7 and 8, the transition probability $\theta_{\vec{u},\vec{v}}$ has the form $\theta_{\vec{u},\vec{v}} = \prod_{i=1}^{n} \alpha_i$, where the factors α_i are as follows:

$$\alpha_i = \begin{cases} 1 & \text{if } u_i = 1 \\ 1 & \text{if } u_i = 2 \\ \sum_{j \in A} p_{j,i} & \text{if } u_i = 0 \wedge v_i = 1 \\ \prod_{j \in A} (1 - p_{j,i}) & \text{if } u_i = 0 \wedge v_i = 0 \end{cases}$$

and A is the set defined as $A = \{j | \mathcal{I}(1, \vec{u})_j = 1\}$, i.e., the set of indices of the units that in state $\vec{u}$ can propagate an explosion (state is 1). For any two states $\vec{u}$ and $\vec{v}$ that do not satisfy either Eqs. 7 or 8, it is $\theta_{\vec{u},\vec{v}} = 0$.

Such a DTMC is an absorbing stochastic process as, independently from the initial state, it will surely terminate its evolution in a state $\vec{v}$ where no unit is in state 1 (i.e., $\left\|\mathcal{I}(1, \vec{v})\right\|_1 = 0$). Out of the $3^n - 1$ states, $2^n - 1$ are absorbing states and the other $3^n - 2^n$ are transient states. Figure 4 shows an example of the state-transition diagram of the DTMC, when $n = 3$ units are considered, and the initial state of the system is $(1, 0, 0)$, i.e., unit 1 is exploding and units 2 and 3 are susceptible to explode.

To analyze the consequences of domino effects, it is sufficient to determine the absorption probabilities of the chain, which provide the likelihood of the system to end the domino propagation in the states with any given number of exploded units. This is easily accomplished by simple linear algebra, as follows. Let P be the matrix that collects the one-step transition probabilities $\theta_{\vec{u},\vec{v}}$ of the DTMC. Then, by a proper ordering of the states, P can be written in the following block form:

$$P = \begin{bmatrix} Q & R \\ 0 & I \end{bmatrix}$$

where Q and R are the sub-matrices that collect the transition probabilities between transient states and from transient to absorbing states, respectively. Then, matrix $(I - Q)^{-1} \cdot R$ provides the limit conditional absorption probabilities, i.e., the probability that the chain will end its evolution in any of the absorbing states, given the initial state [18]. From such conditional probabilities, the measures of interest can be computed. For instance, if $\vec{\alpha}$ is the vector that assigns the initial state probability distribution, and $\vec{\beta}$ the vector whose jth entry is the number of exploded units of the jth absorbing state, then the average number of exploded units can be computed as $\vec{\alpha} \cdot (I - Q)^{-1} \cdot R \cdot \vec{\beta}$.

SAN model

In this section, we describe the SAN model of the VCE domino effect. This model complements the DTMC model of the previous section with the possibility to represent (i) random occurrences of the initial events and (ii) maintenance activities. However, as opposed to the DTMC model, it cannot be evaluated in exact form, and we shall use discrete-event simulation to evaluate the metrics of interest.

Template models

One of the objectives of the methodology we are proposing is to facilitate the evaluation of the VCE risk associated to different scenarios in a chemical plants. To achieve this objective we adopt a “template-based” approach for the

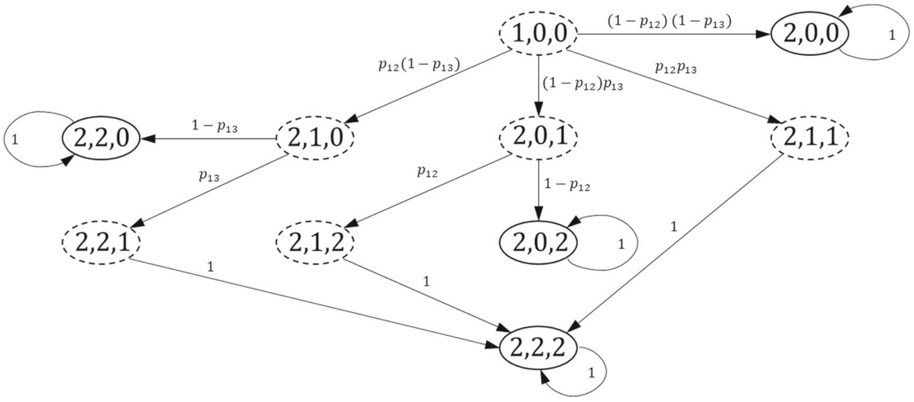


Fig. 4 Example DTMC state transition diagram. Dashed contour for transient states, solid contour for absorbing ones

construction of the SAN model, according to the approach introduced in [20], in which a library of basic parametric models are first defined. Then, such models are instantiated multiple times and connected together to obtain the global models corresponding to the intended scenarios.

The reusability and maintanability of models is therefore improved: submodels can be modified in isolation from the rest of the model, can be substituted with more refined implementations, and can be rearranged based on modifications in system configuration. Most importantly, using such approach facilitates the automated composition of SAN models for different scenarios based on their high-level specification [20].

The tank model

In this work, we exemplify the template-based modeling by using only a single template, the `Tank` model. This is justified by the specific case study we will be dealing with in the "Case study" section. Its graphical representation using the SAN notation is shown in Fig. 5, together with its parameters. Places highlighted with a dashed yellow rectangle are *interface places* of the template, that is, those that will be used for composition with other instances. Parameters of the template include the parameters of the gamma distribution that regulates the initial VCE event in the tank (k, λ), the number of nearby pieces of equipment which may be affected by propagation (n), the probability that propagation of the VCE actually occurs for each of them $(p_1, \ldots, p_n)$, the time interval at which maintenance is executed on the tank (T^M), the cost of the execution of maintenance on the tank (C^M), and the cost of the occurrence of a VCE event on the tank (C^V).

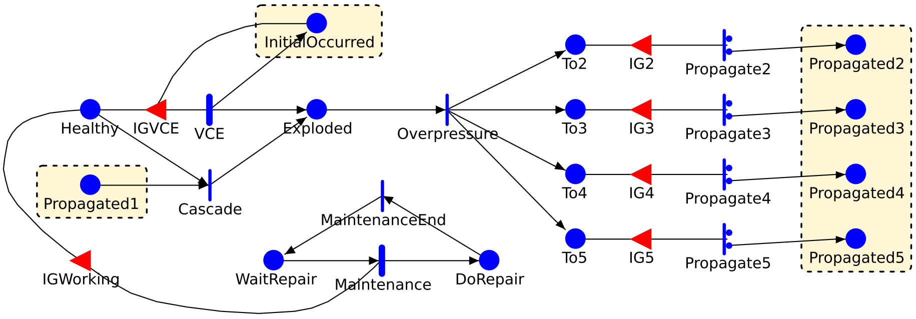
Note that the image in Fig. 5 actually shows the structure of the model for a tank with four neighboring units (i.e., $n = 5$), as the ones that will be used in the case study presented in the "Case study" section. The number of nearby units is however configurable with parameter n, and the model can be automatically altered to reflect a different value. The structure of the model is described in the following.

Initially, the `Healthy` place contains one token, representing that the tank is in good conditions (i.e., no leaking of flammable material). A tank in good conditions may be affected by a VCE for two reasons: either (i) it is the one directly causing the initiating event or (ii) it is affected by propagation from a VCE occurring in one of the nearby pieces of equipment.

The first case is represented by the `VCE` activity, which is distributed according to a gamma distribution with parameters (k, λ) and it is enabled when there is a token in the `Healthy` place. When the `VCE` transition fires, it means that a leakage of flammable material has occurred and the subsequent VCE event occurred (as per assumptions in the "Assumptions" section). The token is then removed form the `Healthy` place, and one is added to places `Exploded` and `InitialOccurred`. The place `InitialOccurred` is shared between all the instances of the template, and it is used to block subsequent initial events after one has occurred (we assumed a single initial event).

The second case, in which the tank is affected by incoming propagation, is represented by place `Propagation1` and the immediate activity `Cascade`. `Propagation1` is also an interface place, that is, it is shared with other instances of the `Tank` template, representing the other tanks in the scenario. In case one of the other tanks successfully propagates a VCE event to the tank represented by the model (assume `Tank #1`), a token gets added to place `Propagation1`. Such token triggers activity `Cascade`, which removes the token from `Propagation1` and adds one to `Exploded`.

Independently from the reason why a VCE event has been triggered, the presence of a token in `Exploded` triggers the `Overpressure` instantaneous activity,



(k, λ)	Parameters of the gamma distribution regulating the initial VCE event
n	Total number of tanks
$\{p_2, \ldots, p_n\}$	Probability of propagation to nearby tanks
$M_{enabled}$	Whether maintenance should be performed (true/false)
T^M	Interval of execution of maintenance
C^M	Cost of execution of maintenance
C^V	Cost of VCE event

Fig. 5 Template SAN model for an atmospheric tank

representing the propagation of the overpressure wave and the possible triggering of a cascading VCE event. Propagation to each individual tank occurs with a different probability, based on the distance at which it is located from the tank that suffered the initial event (see the "Modeling methodology" section). This aspect is modeled by the instantaneous activities `Propagate`$_i$, each one representing propagation to a different tank. Each of these activities may have two different outcomes (cases), probabilistically chosen: propagation occurs (p_i) or not $(1 - p_i)$. The actual probability values $\{p_2, \ldots, p_n\}$ are parameters of the template model, and are calculated in the previous step of our methodology.

In case propagation occurs, one token is added to the corresponding `Propagated`$_i$ places (e.g., `Propagated2` for Tank #2). Such places are also interface places, and they are analogous to `Propagated1` for the other instances of the `Tank` template model. This is how the modeling of the domino effect is achieved, and any VCE event in a tank can cascade multiple times, potentially causing a VCE event in all the tanks in the scenario.

Maintenance is modeled by the timed activity `Maintenance`, whose firing time is deterministic with parameter T^M. If the parameter $M_{enabled}$ is set to true, then the place `WaitRepair` contains a token, and the activity `Maintenance` is thus enabled. Upon firing, a token is removed from `WaitRepair` and one is added to `DoRepair`. When there is a token in place `DoRepair`, the *reactivation function* [31] of activity `VCE` triggers a reactivation, that is, the firing time of the activity is resampled from the associated probability distribution. This mechanism effectively models the repair of the component to one as good as new. Finally, the instantaneous activity `MaintenanceEnd` removes a token from `DoRepair` and adds one to `WaitRepair`, enabling the activtiy `Maintenance` again for the next maintenance period.

Overall model and metric specification

The overall model of a scenario is obtained by creating multiple instances of the `Tank` template model and connecting together all the `Propagated`$_i$ interface places having the same name. This is illustrated, visually, in Fig. 6b. All the instances of the template are connected using the Rep/Join state-sharing formalism [30] (Fig. 6b). In this way, cascading effects of VCE events are automatically taken into account by the SAN model (Fig. 6a).

Once the model of the complete scenario has been constructed, the measures defined in the "Metrics of interest" section need to be specified in terms of the SAN model. This is typically done by defining reward variables [41].

In our case, the target measures can be computed as follows.

– $F^i(t)$ is the expected value, at time t, of the following reward variable:

$$\mathcal{R}^i = \begin{cases} 1 & \text{if } \#(\texttt{Tank}_i\texttt{.Healthy}) = 0 \\ 0 & \text{otherwise,} \end{cases}$$

where $\#(\texttt{Tank}_i\texttt{.Healthy})$ is the marking of the `Healthy` place in the ith instance of the `Tank` template.

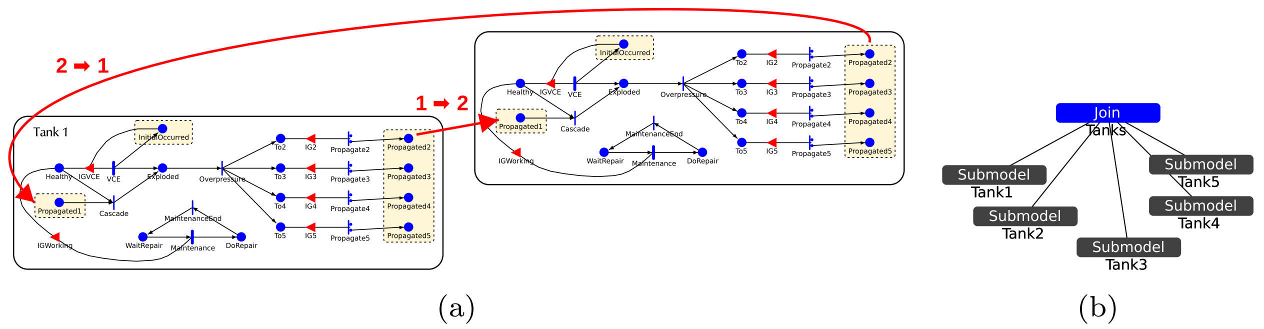


Fig. 6 Multiple instances of the `Tank` template model are connected together using the Join state-sharing formalism (**b**). In this way, cascading effects are automatically taken into account by the SAN model (**a**)

- $N_{fail}(t)$ is the expected value, at time t, of the following reward variable:

$$\mathcal{R}_{fail} = n - \sum_{i=1}^{n} \#(\mathtt{Tank}_i\mathtt{.Healthy}),$$

where $\#(\mathtt{Tank}_i\mathtt{.Healthy})$ is the marking of the `Healthy` place in the ith instance of the `Tank` template, and n is the total number of tanks in the scenario.

- $C(t)$ is the expected value, at time t, of the following reward variable:

$$\mathcal{R}_{cost} = \sum_{i=1}^{n} C_i^V \left(1 - \#(\mathtt{Tank}_i\mathtt{.Healthy})\right)$$
$$+ \sum_{i=1}^{n} C_i^M \left(\#(\mathtt{Maintenance}_i)\right),$$

where $\#(\mathtt{Tank}_i\mathtt{.Healthy})$ is the marking of the `Healthy` place in the ith instance of the `Tank` template, $\#(\mathtt{Maintenance}_i)$ is the number of firings (time it has fired) of the activity `Maintenance` of the ith instance of the `Tank` template, n is the total number of tanks in the scenario, and C_i^M and C_i^V are the cost associated to maintenance and occurrence of VCE event for the ith tank.

Case study

As it is common practice in the literature, atmospheric storage tanks containing gasoline are considered for the evaluation of the proposed methodology.

We consider five gasoline tanks and five different layout scenarios to be compared. The candidate layouts are shown in Fig. 7a–e. In the figures, we show the distances that represent the main input to the calculation of the P_e probabilities, according to the procedure described in the "Modeling of one-step VCE propagation" section. Parameters a and b, which define the size of the considered area, are set to 80 m and 120 m, respectively.

As for the failures of the tanks, (i.e., occurrence time of initiating VCE events), they all follow the same gamma distribution. The value for the rate parameter λ has been set based on the data in [4], considering the equipment "3.6.1.1 VESSELS-ATMOSPHERIC-METALLIC." Based on such data, the average failure rate for such equipment is 0.985 failures per 10^6 h, that is, $\lambda = 9.85 \cdot 10^{-7}$ h^{-1}. We set the shape parameter to $k = 1.5$; this means that the event of interest (occurrence of a VCE) occurs every 1.5 failures of the tank itself, that is, on 2/3 of the occasions. While this is a reasonable value for the purpose of this paper, a more accurate investigation of this parameter will be part of our future work.

In the following, we perform three distinct types of evaluations for the possible layout designs:

1. A *what-if* analysis, to estimate the consequences of a failure affecting Tank #1 with probability 1 at time 0;
2. A*transient* analysis, considering domino effects caused by the occurrence at random times of tank failures;
3. A *cost* analysis, which takes into account the execution of periodic maintenance on the effects of failure occurrence and propagation.

Since the first type of analysis does not require modeling the time of occurrence of the events, the DTMC model is used for the *what-if* analysis. The other two analyses will be instead based on the SAN model, evaluated with the discrete-event simulator provided with the Möbius framework [8].

Results obtained with the DTMC model are exact, while, when not specified otherwise, each value computed by simulation is estimated with a confidence level of 95% and a confidence interval of no more than 5% relative width.

What-if analysis

In this section, we report the results of the what-if analysis described above, which has the objective to assess the potential VCE domino effects caused by a failure of Tank #1. This same analysis can be repeated to consider

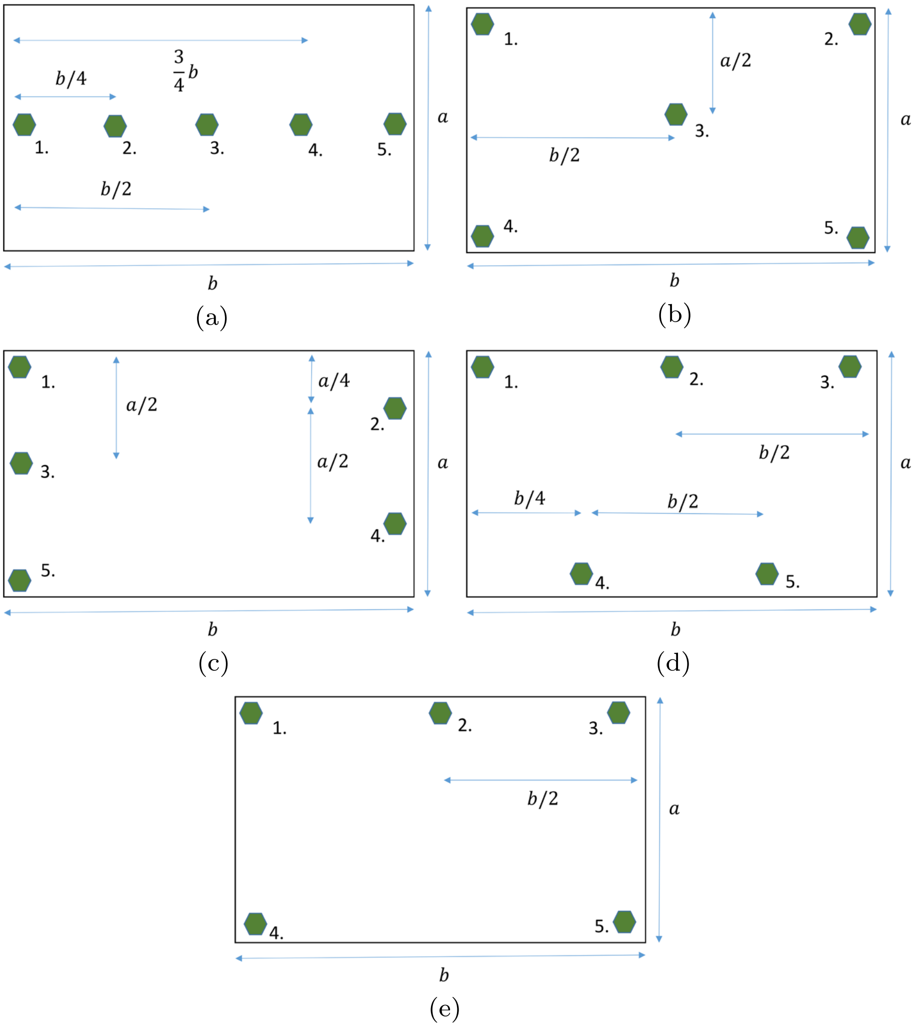


Fig. 7 Layouts scenarios for evaluation ($a = 80, b = 120$ meters). **a** Layout of scenario A. **b** Layout of scenario B. **c** Layout of scenario C. **d** Layout of scenario D. **e** Layout of scenario E

the case when the initial event happens to any other unit. The results of the evaluation of F^i and N_{fail} for the five considered scenarios are shown in Fig. 8. Since we assumed that failure propagation among tanks is instantaneous, we use the DTMC model to evaluate the metrics. Results for Tank #1 have not been included in the figures, because it is assumed that the initiating event occurs in such tank for all scenarios, and as such F^1 is constant with value 1.0.

For the considered case study, our modeling methodology provides results that are easily interpreted. In fact, the layout with a linear placement of tanks (scenario A) has the highest individual probabilities of explosion among all the scenarios. This is indeed the configuration in which tanks are closer, with a minimum distance between them of $b/4$ (i.e., 30 m). When the average spacing between equipment is increased, clearly it becomes less probable for a VCE to affect adjacent equipment. Overall, scenarios A and C present the highest probability of domino effects, while scenarios B, D, and E are less risky in comparison to the other layouts.

However, a greater distance from the first tank (which, we recall, in this evaluation always serves the purpose of generating the initiating event) does not necessarily mean a lower probability of explosion, as closeness with other equipment can trigger domino effects. Such effect can be clearly seen in scenario A, where the closeness of equipment units among each other has the results of increasing the probability of domino effects by one order of magnitude in comparison to the other scenarios. In fact, in scenario A even for equipment that is farther from the detonation point (Tank #5), the probability of being affected by the VCE domino effect is one order of magnitude higher than the maximum experienced by any tank in scenarios B, D, and E (Fig. 8a).

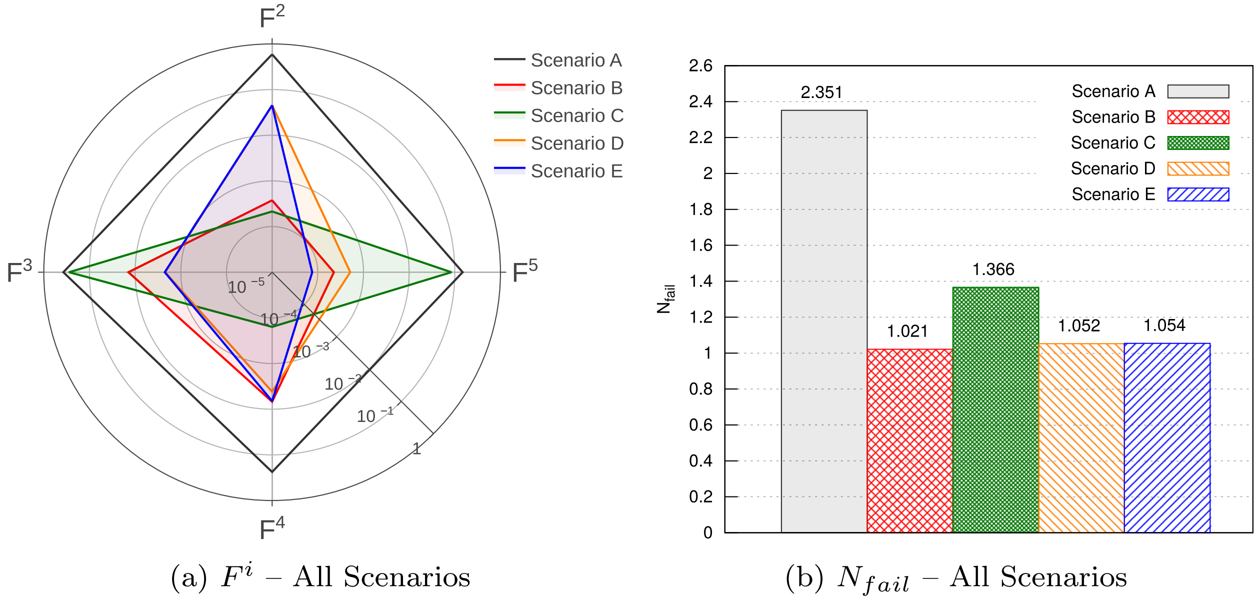


Fig. 8 Results of the what-if analysis assessing the impact of a VCE occurring on Tank #1. **a** Probability of a domino VCE event affecting the other four tanks in the different scenarios. **b** The average number of tanks affected by VCE for each scenario

Nevertheless, by analyzing the plot for F^i (Fig. 8a), it is not straightforward to understand which out of the five scenarios is the safest one on average. For example, in scenario B, the probability of explosion for Tank #2 is lower than in scenario D, but for Tank #3, it is the opposite. Similarly, the probability of explosion for Tank #5 is the lowest in scenario E, but for Tank #2, it is the lowest in scenario C.

The overall safety of the different layouts with respect to a VCE occurring on the first tank can be better understood by analyzing the N_{fail} metric (Fig. 8b). From that figure, it can be clearly understood that, under these assumptions, scenario B is the one resulting in the lowest average number of tanks being affected by the domino effect, while D and E are almost equivalent with respect to this metric. There is however a difference for Tank #5; in fact, F^5 is lower in the last scenario because it is farther from the initiating event and far enough from the other tanks as well.

This kind of evaluation can help identifying certain patterns that, although clear in those specific scenarios, can be more difficult to devise in complex layouts. Also, this evaluation has highlighted the complementary nature of the two proposed metrics in performing what-if analysis.

It is worthwhile noticing that the results reported in Fig. 8b correspond to those previously obtained in ([33], Fig. 11f). However, in this paper, they are calculated using the DTMC model, so they are exact, while in [33], they had been just statistically estimated by discrete-event simulation. With respect to the previous version of the paper, Fig. 8b uses the linear scale instead of the logarithmic one, and we have added the value of 1 to N_{fail}, corresponding to the failure of the tank on which the initiating event occurs.

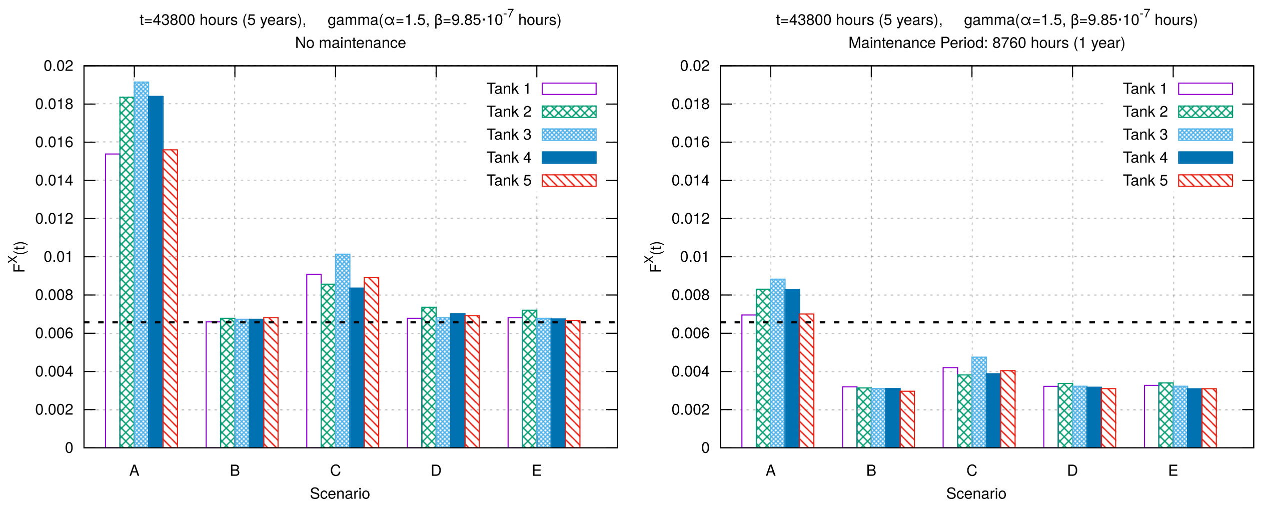
Transient analysis

In this section, we perform a transient analysis of the model, that is, we evaluate how the probability of VCE domino effect occurrence changes with time. In this evaluation, we assume that the initiating event can occur in any of the five atmospheric gas tanks.

We used such values to evaluate the metric $F^i(t)$ for all the tanks and all the scenarios at the instant of time of 43800 h, roughly corresponding to 5 years. The results of such evaluation are reported in Fig. 9. The left part of the figure (Fig. 9a) shows the average number of tanks that would suffer a VCE (either because of a tank failure or a domino effect), without performing any maintenance activities.

The results confirm the ones obtained in the previous evaluation, that is, scenarios A and C are the ones that are most affected by the domino effects of VCEs. The results in Fig. 9 also confirm that the model is able to accurately distinguish tanks based on their location. In fact, looking at results for scenario A, the highest probability of explosion is for Tank #3, then for Tank #2 and Tank #4, and finally for Tank #1 and Tank #5. This is consistent with the layout of Fig. 7a, in which Tank #3 has the minimum average distance from the other tanks.

The most interesting result are however the values obtained for scenarios B, D, and E. While they confirm



(a) Without maintenance

(b) With maintenance every year

Fig. 9 Probability of a VCE affecting different tanks on the different scenarios, assuming a random initial event. Values of $F^i(t)$ with $t = 43800$ h $=$ 5 years, without any maintenance activity (**a**) and with preventive maintenance of tanks performed every year (**b**)

that these three layouts are almost equivalent, the figure also shows another interesting result. For each tank in these scenarios, the probability of being affected by a VCE is almost the same. Furthermore, this value is very close to the value of the cumulative distribution function of the gamma distribution regulating the failure process of individual tanks. In fact:

$$\text{Prob}[\,\text{TTF} \le t] = \frac{\gamma(k, \lambda t)}{\Gamma(k)} = \frac{\gamma(1.5, 9.85 \cdot 10^{-7} \cdot 43800)}{\Gamma(1.5)} \approx 0.00657. \qquad (9)$$

The resulting value is highlighted in the figure by a dashed black line. As visible in Fig. 9a, this value is very close to the value of $F^i(t)$ obtained for all the tanks in scenarios B, D, and E. This means that, in such layouts, *the domino effect does not add significant contribution to the probability of a tank being affected by a VCE*. The same is not true for scenarios A and C, which instead are significantly affected. This is consistent with the results we obtained in [33]. Hence, we may formulate the hypothesis that changing the probability distribution of the occurrence time of initiating events does not affect the relative hazard proneness of layout scenarios.

Figure 9b shows the same results when preventive maintenance is performed at scheduled intervals of 8760 h (∼1 year). Following the same considerations as before, we note that scenario A is particularly unsafe even with such a reasonable maintenance policy. In fact, even in this case, the probability of a tank suffering a VCE is still higher than the threshold given by the value of the cumulative distribution function regulating the occurrence of VCE on individual tanks. We can then conclude that scenario A must be avoided, while we can consider scenario C under the condition that yearly maintenance activities are scheduled.

We note that the results in Fig. 9b could not be obtained with the previous version of the model, as it did not consider maintenance. This demonstrates the usefulness of the extension offered in this paper and how it could be used in practice to evaluate the appropriateness of a certain layout.

Cost analysis

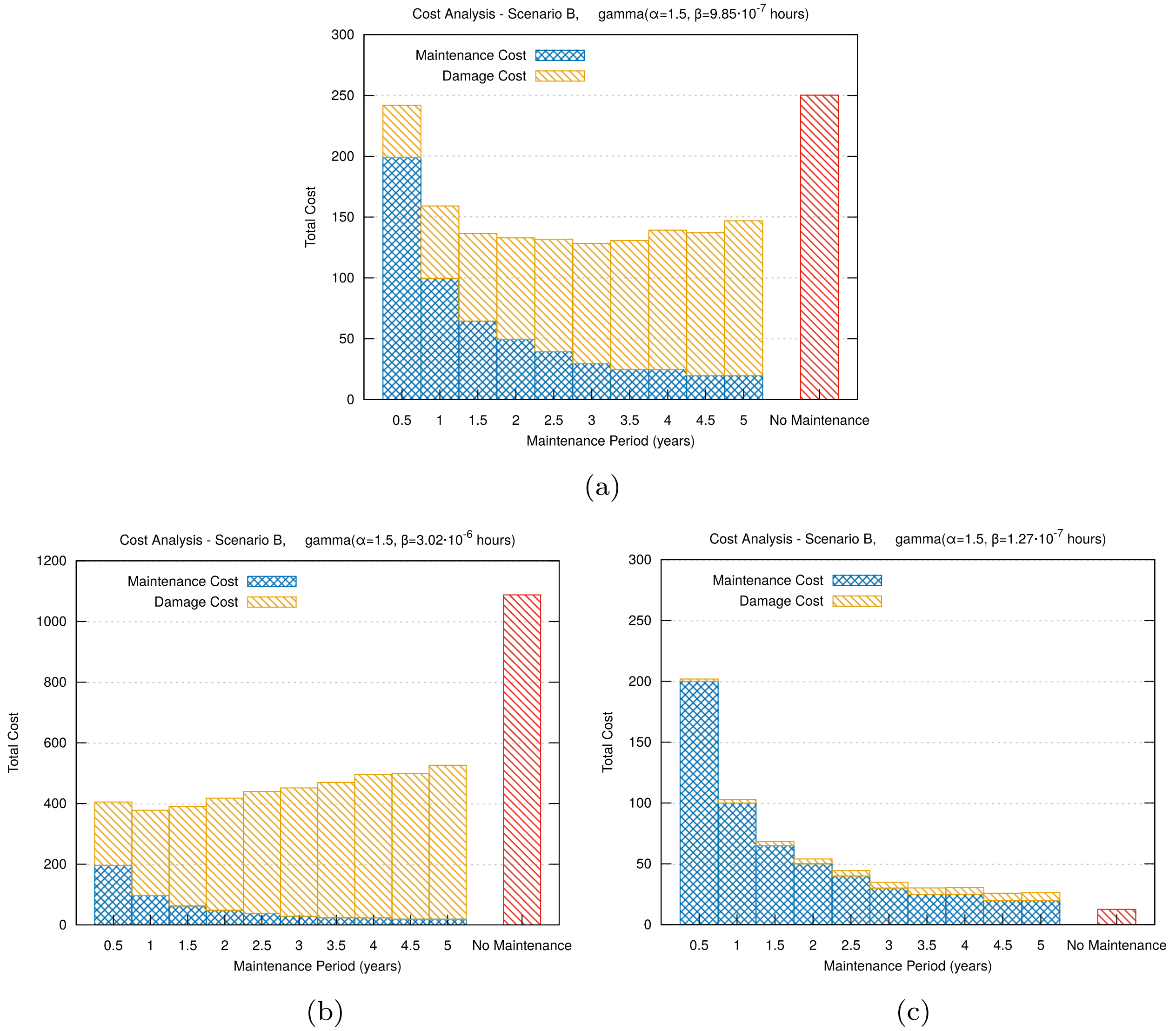
A complementary perspective for deciding whether maintenance activities should be planned, and how often, is to analyze the expected costs to be undertaken by the plant owner. The occurrence of an unsafe event, and its propagation due to domino effects, has a cost in terms of damage to equipment, loss of material, harm to personnel, etc. At the same time, however, periodic maintenance has also a cost, in terms of labor, subsitution of equipment, and downtime of the production process.

Once appropriate safety levels are respected, the most convenient maintenance policy is thus the one that minimizes the total expected cost, that is, the maintenance cost plus the expected costs due to VCE events. This metric corresponds exactly to $C(t)$ defined in the "Met- rics of interest" section and can be evaluated using the methodology defined in this paper. We note that this kind of analysis could not be performed with the model in [33], as it did not take into account maintenance activities nor costs.

We perform a cost analysis considering three different values of λ for tanks, and different maintenance periods ranging from 6 months to 5 years, at increments of 6 months. The failure rates used in this analysis are taken from the same source [4], which contains "lower," "average," and "upper" values for the failure rate of atmospheric vessels. For the purpose of this evaluation, we assume that an unsafe event produces a cost two order of magnitude greater than the execution of maintenance, that is, we set $C_i^M = 10$ and $C_i^V = 1000$ for all the tanks. We accumulate the costs until time $t = 175200$ h (20 years), that is, we assume a lifespan of the system of 20 years.

Results of this analysis for scenario B are reported in Fig. 10. We focus on scenario B because it has been identified as the least prone to domino effects, and thus, it is the most recommended in terms of safety. Figure 10a shows the result for the "average" value of λ in [4], which is also the value used in previous evaluations. In this case, adopting the most frequent maintenance (6 months) has almost the same cost as not performing maintenance at all, while the most convenient maintenance period is 3 years.

Figure 10b shows the results when using the "high" value of λ, that is, tanks fail more frequently. In this case, any of the considered frequency options for the execution of maintenance reduces the costs with respect to not performing maintenance at all. The best policy in



(a)

(b)

(c)

Fig. 10 Analysis of expected costs of scenario B after 20 years, considering different frequencies of execution of preventive maintenance and different values for the λ parameter of tanks. **a** $\lambda = 9.85 \cdot 10^{-7}$ h^{-1} ("average"). **b** $\lambda = 3.02 \cdot 10^{-6}$ h^{-1} ("high"). **c** $\lambda = 1.27 \cdot 10^{-7}$ h^{-1} ("low")

this case is to perform maintenance every year. Finally, the result when using the “low” value for λ are depicted in Fig. 10c. In this case, maintenance only increases the overall costs, without actually producing any benefit. The best policy in this case is to not perform maintenance, at least during the considered timespan of the system of 20 years.

Limitations to validity

The work presented in this paper is based on a set of assumptions, which are described in the “Assumptions” section. The main limitations therefore concern the extent to which such assumptions are realistic and the generalizability of the methodology.

Most of the assumptions that have been introduced were justified in the “Assumptions” section, and they have been devised following common practice from the literature. Nevertheless, two strong assumptions were introduced that may limit the validity of results. The first one is that the only possible failure mode is a VCE. The second is that the domino effect among different pieces of equipment, if it occurs, is immediate. This is not always the case in reality. However, from the perspective of evaluating the domino effects of VCEs, we note that both assumptions are considering the worst case. The results are thus conservative with respect to the actual safety of the system configuration against VCE domino effects.

Approximations are also introduced by blast estimation, which adopts a simplified model of the explosion effects. We mitigated this aspect by using a well-established blast estimation method from the literature, the multi-energy method. To further mitigate this aspect, the method can be calibrated following an approach similar to the one in [27].

Finally, in this paper, we have analyzed a limited set of scenarios. Namely, we limited our analysis to the layouts reproduced in Fig. 7, and to the failure of Tank #1 for what concerns the *what-if* analysis. Deeper validation of the methodology would require its application to different scenarios and with different set of parameters and possibly its validation against historical data from real accidents as done by the authors of [2].

Conclusions and future work

In this paper, we tackled the problem of assessing the safety of chemical plants, taking into consideration the types of equipment and of materials being processed, as well as its physical layout. The problem of trading-off area and piping costs (which results in dense layouts) with the expected costs incurred in case of accidents (which are higher in dense layouts) is a complex one, as it requires integrating diverse types of information.

We focused on the safety issues posed by VCEs, and we proposed a methodology based on probabilistic modeling to assess the consequences of domino effects. Our modeling methodology considered a standard characterization of the initiation events, and it used probit models to estimate the likelihood of explosion propagation, taking into account the distances between equipment units. These elements were integrated into probabilistic models that allow analyzing general cases of plant layouts.

We exercised the models on a case study composed by several atmospheric gasoline tanks. We compared safety-related metrics for various possible layouts of the tanks in the same physical space, showing that our approach allows determining interesting options for spacing elements and for trading the expected cost of VCEs and of preventive maintenance. Future work aims at validating the methodology by further applying it on different plant layouts and with different parameter settings.

The research results presented in this work represent a first concrete step for quantitatively assessing the safety of plant layouts. Further research could be conducted to better characterize in a quantitative way domino effect exposure, specifically on more robust models accounting for unwanted events other than VCEs. A more accurate calculation of domino effect probabilities would be possible by improving dispersion calculations for partial confinement and turbulence calculations within the vapor cloud.

Another direction for future work consists in improving the modularity of the SAN model and automating model construction, directly taking as input a layout of the chemical plant. In this perspective, we plan to investigate the application of model-driven engineering (MDE) techniques [19, 32], with the objective to automatically derive our probabilistic model from a high-level description of the physical layout of the infrastructure under analysis.

Abbreviations

BLEVE: Boiling liquid expanding vapor explosion; DTMC: Discrete-time Markov chain; MDE: Model-driven engineering; SAN: Stochastic activity network; SPN: Stochastic Petri net; TCHPN: Timed colored hybrid Petri net; TNT: Trinitrotoluene; TTF: Time-to-failure; VCE: Vapor cloud explosion

Acknowledgements

The authors would like to acknowledge the contributions of Prof. Felipe Muñoz Giraldo from the Department of Chemical Engineering of Universidad de los Andes to the conceptual formulation of the failure propagation model.

Authors’ contributions

All the authors have contributed equally to the methodological and technical aspects of this research. All the authors have read and approved the final manuscript.

Funding

This work has received funding from the European Union’s Horizon 2020 research and innovation program under the Marie Sklodowska-Curie grant agreement No 823788 “ADVANCE” and by the São Paulo Research Foundation (FAPESP) under grant #2019/02144-6.

Availability of data and materials

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Universidad de los Andes, Bogotá, Colombia. [2]Universidade Estadual de Campinas, Campinas, Brazil. [3]Duke Kunshan University, Kunshan, China.

Received: 30 April 2019 Accepted: 9 September 2019
Published online: 31 October 2019

References

1. Atkinson G, Cowpe E, Halliday J, Painter D (2017) A review of very large vapour cloud explosions: cloud formation and explosion severity. J Loss Prev Process Ind 48:367–375. https://doi.org/10.1016/j.jlp.2017.03.021
2. Bauwens C, Dorofeev S (2015) Effects of the primary explosion site and bulk cloud in VCE prediction: a comparison with historical accidents. Process Saf Prog 34(2):147–153. https://doi.org/10.1002/prs.11703
3. Casal J (2008) Evaluation of the effects and consequences of major accidents in industrial plants. Industrial Safety Series, vol. 8. Elsevier Science. https://doi.org/10.1016/S0921-9110(08)80011-0
4. Center for Chemical Process Safety (1989) Guidelines for Process Equipment Reliability Data with Data Tables. https://doi.org/10.1002/9780470938355
5. Center for Chemical Process Safety (2010) Guidelines for Improving Plant Reliability through Data Collection and Analysis. https://doi.org/10.1002/9780470935262.pubnote
6. Chiaradonna S, Di Giandomenico F, Lollini P (2011) Definition, implementation and application of a model-based framework for analyzing interdependencies in electric power systems. Int J Crit Infrastruct Prot 4(1):24–40. https://doi.org/10.1016/j.ijcip.2011.03.001
7. Ciardo G, German R, Lindemann C (1994) A characterization of the stochastic process underlying a stochastic petri net. Softw Eng IEEE Trans 20(7):506–515
8. Clark G, Courtney T, Daly D, Deavours D, Derisavi S, Doyle JM, Sanders WH, Webster P (2001) The Mö. In: Proceedings 9th International Workshop on Petri Nets and Performance Models (PNPM'01). pp 241–250. http://dl.acm.org/citation.cfm?id=882474.883479
9. Cozzani V, Salzano E (2004) The quantitative assessment of domino effects caused by overpressure: Part I. Probit models. J Hazard Mater 107(3):67–80. https://doi.org/10.1016/j.jhazmat.2003.09.013
10. Eckhoff RK (2016) Gas and Vapor Cloud Explosions, 2 edn., chap. 2,. Gulf Professional Publishing - Elsevier. https://doi.org/10.1016/B978-0-12-803273-2.00002-5. http://www.sciencedirect.com/science/article/pii/B9780128032732000025
11. Geng J, Thomas K, Baker Q (2016) A study of the blast wave shape from elongated VCEs. J Loss Prev Process Ind 44:614–625. https://doi.org/10.1016/j.jlp.2016.05.026
12. Gursesli O, Desrochers AA (2003) Modeling infrastructure interdependencies using Petri nets. In: SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme - System Security and Assurance (Cat. No.03CH37483), vol. 2. pp 1506–1512. https://doi.org/10.1109/ICSMC.2003.1244625
13. Jallais S, Vyazmina E, Miller D, Thomas J (2018) Hydrogen jet vapor cloud explosion: a model for predicting blast size and application to risk assessment. Process Saf Prog 37(3):397–410. https://doi.org/10.1002/prs.11965
14. Javidi M, Abdolhamidzadeh B, Reniers G, Rashtchian D (2015) A multivariable model for estimation of vapor cloud explosion occurrence possibility based on a Fuzzy logic approach for flammable materials. J Loss Prev Process Ind 33:140–150. https://doi.org/10.1016/j.jlp.2014.11.003
15. Jiang D, Pan XH, Hua M, Mébarki A, Jiang JC (2019) Assessment of tanks vulnerability and domino effect analysis in chemical storage plants. J Loss Prev Process Ind 60:174–182
16. Johnson DM, Tomlin GB, Walker DG (2015) Detonations and vapor cloud explosions: Why it matters. J Loss Prev Process Ind 36:358–364. https://doi.org/10.1016/j.jlp.2015.03.017
17. Khakzad N, Reniers G, Abbassi R, Khan F (2016) Vulnerability analysis of process plants subject to domino effects. Reliab Eng Syst Saf 154:127–136. https://doi.org/10.1016/j.ress.2016.06.004
18. Kulkarni VG (2011) Introduction to Modeling and Analysis of Stochastic Systems. Springer-Verlag, New York. https://doi.org/10.1007/978-1-4419-1772-0. https://www.springer.com/gp/book/9781441917713
19. Montecchi L, Lollini P, Bondavalli A (2011) Towards a MDE Transformation Workflow for Dependability Analysis. In: 16th IEEE International Conference on Engineering of Complex Computer Systems, Las Vegas. pp 157–166. https://doi.org/10.1109/ICECCS.2011.23. https://ieeexplore.ieee.org/document/5773390
20. Montecchi L, Lollini P, Bondavalli A (2019) A template-based methodology for the specification and automated composition of performability models. IEEE Trans Reliab. In press
21. Montecchi L, Refsdal A, Lollini P, Bondavalli A (2016) A model-based approach to support safety-related decisions in the petroleum domain. In: 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). pp 275–286. https://doi.org/10.1109/DSN.2016.33
22. Mukhim ED, Abbasi T, Tauseef SM, Abbasi SA (2017) Domino effect in chemical process industries triggered by overpressure—Formulation of equipment-specific probits. Process Saf Environ Protect 106:263–273. https://doi.org/10.1016/j.psep.2017.01.004
23. O'Connor AN (2011) Probability Distributions Used in Reliability Engineering, Reliability Information Analysis Center (RIAC)
24. Park S, Jeong B, Lee BS, Oterkus S, Zhou P (2017) Potential risk of vapour cloud explosion in FLNG liquefaction modules. Ocean Eng 149:1–15. https://doi.org/10.1016/j.oceaneng.2017.08.032. http://linkinghub.elsevier.com/retrieve/pii/S0029801817304845
25. Petri CA (1962) Communication with automata. PhD thesis, University of Hamburg
26. Raman R, Grillo P (2005) Minimizing uncertainty in vapour cloud explosion modelling. Process Saf Environ Protect 83(4B):298–306. https://doi.org/10.1205/psep.05028
27. Raman R, Grillo P (2005) Minimizing uncertainty in vapour cloud explosion modelling. Process Saf Environ Protect 83(4):298–306. https://doi.org/10.1205/psep.05028. 7th World Congress of Chemical Engineering
28. Ramírez-Marengo C, Diaz-Ovalle C, Vázquez-Román R, Mannan MS (2015) A stochastic approach for risk analysis in vapor cloud explosion. J Loss Prev Process Ind 35:249–256. https://doi.org/10.1016/j.jlp.2014.09.006
29. Rushby J (1994) Critical system properties: survey and taxonomy. Reliab Eng Syst Saf 43(2):189–219. http://dx.doi.org/10.1016/0951-8320(94)90065-5. http://www.sciencedirect.com/science/article/pii/0951832094900655. Special Issue on Software Safety
30. Sanders WH, Meyer JF (1991) Reduced base model construction methods for stochastic activity networks. IEEE J Sel Areas Commun 9(1):25–36
31. Sanders WH, Meyer JF (2002) Stochastic activity networks: formal definitions and concepts. In: Lectures on Formal Methods and PerformanceAnalysis. Springer-Verlag New York, Inc., New York. pp 315–343. http://dl.acm.org/citation.cfm?id=567305.567314
32. Schmidt DC (2006) Guest editor's introduction: Model-driven engineering. Computer 39(2):25–31
33. Serra D, Briceño J, Buitrago H, Rozo B, Montecchi L, Mura I (2018) Probabilistic modeling of failure domino effects in chemical plants. In: 8th Latin-American Symposium on Dependable Computing (LADC), Foz do Iguaçu. p 2018. https://doi.org/10.1109/ladc.2018.00016
34. Simion GP, VanHorn RL, Smith CL, Bulmahn KD, Bickel JH, Sattison MB (1993) Risk analysis of highly combustible gas storage, supply, and distribution systems in PWR Plants. Tech. Rep. NUREG/CR-5759. In: Idaho National Engineering Laboratory. https://doi.org/10.2172/10162133
35. Trivedi KS (1982) Probability and Statistics with Reliability, Queuing, and Computer Science Applications. Wiley
36. Wesevich J, Hassig P, Nikodym L, Nasri V, Mould J (2017) Accounting for channeling and shielding effects for vapor cloud explosions. J Loss Prev Process Ind 50:205–220. https://doi.org/10.1016/j.jlp.2017.09.015
37. Zhang S, Zhang Q (2018) Influence of geometrical shapes on unconfined vapor cloud explosion. J Loss Prev Process Ind 52:29–39. https://doi.org/10.1016/j.jlp.2018.01.004
38. Zhou J, Reniers G (2017) Petri-net based cascading effect analysis of vapor cloud explosions. J Loss Prev Process Ind 48:118–125. https://doi.org/10.1016/j.jlp.2017.04.017

39. Zhou J, Reniers G (2018) Modeling and analysis of vapour cloud explosions knock-on events by using a Petri-net approach. Saf Sci 108(January):188–195. https://doi.org/10.1016/j.ssci.2018.04.019
40. Zhou J, Reniers G (2018) Petri-net based evaluation of emergency response actions for preventing domino effects triggered by fire. J Loss Prev Process Ind 51:94–101. https://doi.org/10.1016/j.jlp.2017.12.001
41. Zimmermann A (2008) Stochastic Discrete Event Systems: Modeling, Evaluation, Applications. Springer-Verlag, Berlin. https://doi.org/10.1007/978-3-540-74173-2

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.