Journal of Loss Prevention in the Process Industries 22 (2009) 513–519

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

Modelling the risk of failure in explosion protection installations

P. Date [a,*], R.J. Lade [b,1], G. Mitra [a], P.E. Moore [c,2]

[a] Center for the Analysis of Risk and Optimisation Modelling Applications (CARISMA), School of Information Systems, Computing and Mathematics, Brunel University, Middlesex UB8 3PH, UK
[b] Kidde UK, Thame Park Road, Thame, Oxfordshire OX93RT, UK
[c] UTC Fire & Security, Colnbrook, Berkshire SL3 0HB, UK

ARTICLE INFO

Article history:
Received 7 January 2009
Accepted 25 March 2009

Keywords:
Risk modelling
Graph theory
Explosion protection

ABSTRACT

This paper proposes a new algorithm to compute the residual risk of failure of an explosion protection system on an industrial process plant. A graph theoretic framework is used to model the process. Both the main reasons of failure are accounted for, *viz.* hardware failure and inadequate protection even when the protection hardware functions according to specifications. The algorithm is shown to be both intuitive and simple to implement in practice. Its application is demonstrated with a realistic example of a protection system installation on a spray drier.

1. Introduction

Explosion protection systems designed and installed on industrial processing plants offer protection against the prevailing and the envisioned explosion hazards. For any explosion protection system installation, there is a non-zero probability that the system will fail to mitigate an explosion. We will refer to this probability as the *residual risk*. The purpose of this paper is to quantify this risk of explosion protection system failure in a tractable manner. While the underlying science behind flame propagation and explosion mitigation means is well understood, and extensively studied (Bartknecht, 1993; Eckhoff, 2003; Moore & Spring, 2004; Siwek & Cesana, 2001), the computation of risk of explosion protection failure for the process plant as a whole is a non-trivial problem and has received far less attention. Owners/operators, who carry the ultimate responsibility, are making a key decision on the acceptability of a specific safety system configuration – often without a clear methodology to quantify or ascribe residual risk which it entails. We set out a systematic methodology for quantifying the residual risk for installed explosion mitigation provisions in process systems, and demonstrate how this can help in making decisions about balancing safety requirements and cost-effectiveness.

A directed graph representation (see, e.g. West, 2001, chap. 1) is used to represent the process plant and the intended or installed explosion safety system as a whole, comprising a set of vertices linked by directed edges. Each vertex represents a process vessel (e.g. a drier or a cyclone) and is characterised by a set of connectivity and probability parameters. This conceptual architecture allows the cumulative probability of failure to be computed by a simple algebraic model. The computational model and the processing algorithm explicitly accounts for both the principal mechanisms of failure; *viz.* a complete failure of the safety system (e.g. due to a critical hardware failure) and a failure due to inadequate protection (e.g. due to the reduced explosion pressure of a suppressed or vented explosion occurrence still being greater than the pressure shock resistance of the vessel). This paper demonstrates the computation of residual risk using this methodology for a typical example of a process plant where explosible dust represents the principal explosion hazard (see Barton, 2002 for a detailed analysis of this hazard). The selected example illustrates some of the prevalent protection issues in a simple spray drying process. The explosion protection options of explosion venting, explosion suppression and explosion isolation (using either triggered chemical barriers or triggered mechanical barriers) are considered. We demonstrate how a change in the protection system design affects the residual risk of an unmitigated explosion, thereby providing a clear and quantifiable trade-off between the achieved level of protection and cost. This methodology will also assist operators in meeting their obligations under the European Regulations (ATEX, 2005) to assess and ascribe the residual risk of unmitigated explosions. In the authors' view, the proposed model is also a convincing example of collaboration between process industry practitioners and academic researchers working in operations research to solve a challenging industrial problem.

* Corresponding author. Tel.: +44 1895 274000; fax: +44 1895 269732.
E-mail addresses: paresh.date@brunel.ac.uk (P. Date), rob.lade@kiddeuk.co.uk (R.J. Lade), gautam.mitra@brunel.ac.uk (G. Mitra), peter.moore@fs.utc.com (P.E. Moore).
[1] Tel.: +44 1844 265117; fax: +44 1844 265157.
[2] Tel.: +44 1753 689848; fax: +44 1753 683810.

0950-4230/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jlp.2009.03.007

Recently, development of a very useful calculation tool for quantitative risk assessment was reported in Van der Voort et al. (2007). The focus of this reference is on computing risk contours using knowledge of the flame propagation and the consequence of a dust explosion. In contrast to this work, the focus of our methodology is to provide a simple and effective means for cost/benefit analysis in choosing an explosion safety system for a given plant.

The rest of the paper is organised as follows. The next section provides a short, non-technical tutorial on explosion protection systems. In Section 3, a directed graph based representation of such installations is presented. Section 4 provides the main contribution of this paper where a new, systematic method to compute residual risk in an explosion protection system is presented. This method is illustrated through a comprehensive example in Section 5. Finally, Section 6 summarises the contribution and outlines the direction of present research.

2. Explosion protection installations: a primer

We first outline the basic issues involved in explosion protection installations. For the sake of completeness, the generic components and their functions are reviewed briefly. This section also establishes some of the notation which will be used in the subsequent sections.

- A process plant typically comprises a series of interconnected vessels in which different operations such as drying, grinding, filtering or mixing are carried out. Each vessel has its own pressure shock resistance, which we denote by P_s. This is a pressure that the vessel can withstand without physical deformation. Many processes involve potential sources of ignition (e.g. mechanical friction in a grinder) as well as potential fuels to cause an explosion (e.g. any dispersed and combustible dust). In the event of an ignition, the flame propagates from the ignition kernel causing the pressure inside a vessel to rise beyond P_s, leading to a considerable damage to the plant and a possible risk to human life. To avoid this scenario, explosion protection systems are installed in process plants.
- Depending on the requirements, either explosion suppression or explosion venting means (or both) is installed on each vessel deemed to be at risk. Explosion suppression rapidly deploys appropriate flame suppressant to quench the propagating flame front while explosion vent panels installed onto vessel walls rupture to mitigate the rising pressure within the plant item. Explosion venting is a passive mitigation means since the vent panels yield at a prescribed pressure. Both the protection methodologies aim at reducing the explosive pressure increase to a value below P_s. In either case, it is possible to calculate the expected reduced pressure after mitigation for a given protection system. We denote this reduced pressure by P_{red}. Note that a different number of suppressors or different types of suppressors will yield different P_{red} for the same vessel. The same comment applies for the number and the types of vent panels. For a successful explosion mitigation in any vessel, the inequality $P_{red} < P_s$ must hold. The parameters P_{red} and P_s are discussed in more detail in Section 4.2.
- For explosion suppression, an explosion event is typically detected by pressure detectors, which detect a rise (or the rate of rise) in pressure. The detector sends this signal to a control panel which then deploys the suppressors. A control panel may be common to several vessels which together form a protection zone. In case of explosion isolation between connected vessels, optical flame detection is also used on the mouth of the connecting duct.
- Following a mitigated explosion event in one vessel, flame often propagates along adjoining duct-work causing further explosions in connected vessels. An explosion due to a propagated flame may be more intense than the explosion due to a direct ignition, due to increased turbulence and a jet flame ignition; see Holbrow, Lunn, and Tyldesley (1999) for guidance on containment and venting of explosions due to flame propagation. The installed protection system on each vessel should account for the possibility of explosion by flame propagation. The ducts where there is a risk of flame propagation may have an explosion isolation barrier installed which may either be a transient chemical barrier (i.e. a suppressor) or a fast acting valve both of which reduce the likelihood of flame passage. This barrier is deployed in the case of an explosion in the upstream or downstream vessels by the corresponding control panel.
- In case of a chemical or a mechanical barrier as above, the time for the barrier to be established and the time for the flame to reach the barrier can be computed (subject to suitable assumptions). We denote these two times by t_b and t_f respectively. For a successful explosion isolation, the inequality $t_b < t_f$ must hold, i.e. the barrier is established before the arrival of the flame front. The parameters t_b and t_f are discussed in more detail in Section 4.2.

3. Directed graph representation

In our formulation, the industrial process plants under study are represented by a fully connected, directed graph and each vessel in the system is represented as a vertex. The edges between the vertices represent paths of possible flame propagation (e.g. duct-work between different vessels) in case of an ignition. Between any pair of adjacent vertices, there are two directed edges in opposite directions. Each edge is associated with a weight which represents the probability of flame propagating down the duct in question. The upstream and downstream flame propagation probabilities are typically different due to the bulk movement of the material. To represent this, we impose a restriction that any pair of adjacent vertices (u, v) have two edges between them, one where u is a tail and another where u is a head.

This simple representation is best explained through an example. Fig. 1 shows a spray drying process. A wet dairy product is spray dried, and then passes through two fluid bed driers that further reduce the moisture content of the final product. Dust content in the drying air is separated by a ganged pair of cyclones, and returned through a fines return line to the spray drier. Spray drier designs that use a fines return loop are known to be more susceptible to dust explosion incidents because of the higher level of connectivity between the fluid bed driers and the spray drier. In this example, explosion protection is achieved by appropriate explosion relief vent panels installed on the cyclones, and by a three-zone explosion suppression system. Protection zones will be explained in more detail in Section 5.

Fig. 2 shows the corresponding directed graph representation for this process. We can use *vertices* and *vessels* interchangeably; keeping in mind that one is an abstract representation of the other. Table 1 lists all the vertices for reference.

It is worth mentioning that this is *not* a simple graph (see West, 2001 for a definition) since it will always have multiple edges. This restricts the applicability of standard tools of representing graphs and performing operations such as enumeration. However, the graphs of real process plants rarely have more than 8 vertices, so that the computation of joint probabilities is not too taxing.

Please cite this article in press as: Date, P., et al., Modelling the risk of failure in explosion protection installations, Journal of Loss Prevention in the Process Industries (2009), doi:10.1016/j.jlp.2009.03.007

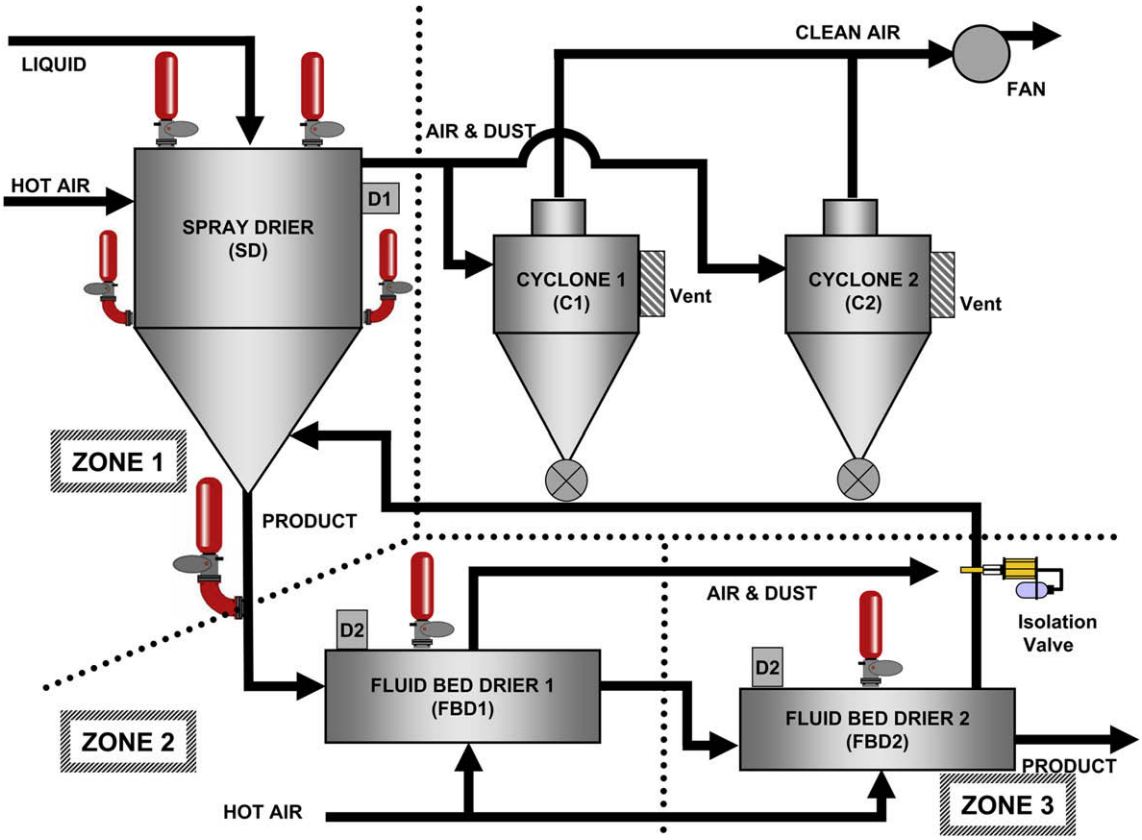

Fig. 1. Spray drier explosion protection installation.

4. A model for computation of residual risk

4.1. Assumptions

We first introduce the assumptions and the notation, which are used to specify the residual risk model. The assumptions are based on experience of professionals in the explosion protection industry regarding what needs to be taken into account in modelling the residual risk.

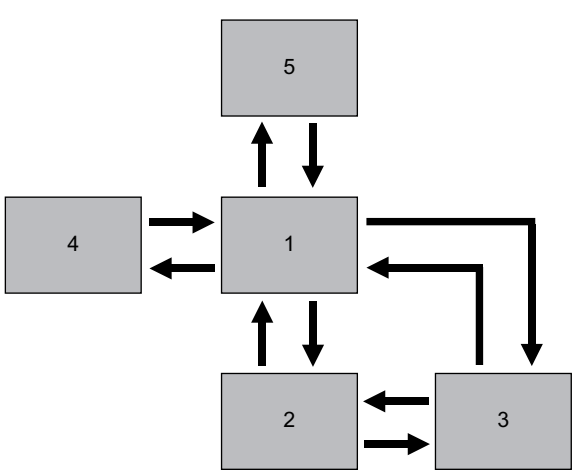

Fig. 2. Directed graph representation for spray drier system.

- We use the probability of an unmitigated explosion in any one of the vessels in the process in a given unit of time as a proxy for residual risk. The unit of time may be consistent with the maintenance schedule, although any other time duration may be postulated for comparing different safety configurations.
- In any vessel, an ignition may occur at any location with equal probability.
- An unmitigated explosion in any vessel or at any vertex is considered as a failure. We do not account for differing severity of failure in different vessels. In reality, failure of some vessels may merely lead to inconvenience rather than a catastrophe. However, treating all failures as equally catastrophic still yields valuable information in comparing different choices of safety system configurations.
- Given an ignition event at a vertex, only the probabilities of an unmitigated explosion at the same vertex or adjacent vertices are considered in the computation of risk. This assumption is made mainly for simplicity of exposition and can easily be relaxed in practice.
- We assume that there is only one type of detector and at most two different types of suppressors on any vessel. This is

Table 1
List of vertices for spray drier example.

Vertex	Component
1	Spray drier
2	Fluid bed drier 1
3	Fluid bed drier 2
4	Cyclone 1
5	Cyclone 2

Please cite this article in press as: Date, P., et al., Modelling the risk of failure in explosion protection installations, Journal of Loss Prevention in the Process Industries (2009), doi:10.1016/j.jlp.2009.03.007

a fairly realistic assumption from a practical point of view. Note that the number of suppressors or detectors is not restricted. A given vessel can have any number of suppressors (resp. detectors) but they can be of at most two different types (resp. of the same type). Given an ignition, an unmitigated explosion is assumed to occur when any one detector or any one suppressor fails.

- We also assume that there are at most two different types of vent panels on any vessel.
- In practice, there may be multiple flame paths between two vessels. We will consider these paths to be independent and compute the total probability of flame propagation over all paths in such cases. In the example of Section 5, we have shown the individual probabilities along each path for completeness; please see Table 5.
- P_{red}, P_s, t_b, t_f and the fundamental flame propagation probabilities Q_j^s (defined in the next section) are assumed to be known and are assumed to be stationary through time.

4.2. Definition of model parameters

In the model for computation of risk based on a graph representation, each vertex i of the system is characterised by a set of parameters described in this section.

(1) $Q_E(i)$ is the probability of an occurrence of an ignition event in any vessel i, which, if not effectively suppressed or vented, will result in an unmitigated explosion. For a given process plant and over a given period of time, we assume that $\sum_i Q_E(i) = 1$, *i.e.* we compute the probability of an unmitigated explosion *given* an ignition in one of the vessels.

(2) $k_1(i)$ and $k_2(i)$ are the number of vent panels of type 1 and type 2 respectively, mounted on vessel i. Default values of $k_1(i)$ and $k_2(i)$ are 0. If there is only one type of vent panel, then $k_1(i)$ denotes the number of vent panels and $k_2(i) = 0$. Vent panels of different types will have different mean time between failures (MTBFs) and different properties with regards to achieved P_{red}.

(3) $k_3(i)$ is the number of detectors on a vessel i. There are two main ways of detecting an ignition. *Pressure detectors* detect the change in pressure after sufficient combustion has occurred, while *flame detectors* respond to incidents when the ignition location is close to the detector. The speed of response of a pressure detector is almost independent of ignition location, and a single detector can suffice for even large vessels. Note however that a single flame detector placed far from the point of ignition may end up detecting the ignition too late and fail to deploy explosion isolation measures in time to prevent explosion propagation upstream/downstream. Multiple flame detectors can be placed to cover the entire volume of larger vessels – often resulting in faster detection than with pressure detection.

(4) $k_4(i)$ and $k_5(i)$ and are the number of suppressors of type 1 and type 2 respectively, mounted on vessel i. Default values of $k_4(i)$ and $k_5(i)$ are 0. If there is only one type of suppressor, then $k_4(i)$ denotes the number of suppressors and $k_5(i) = 0$. As mentioned in the previous section, there are many types of suppressors. It is realistic to assume that there are at most two types of suppressors on any particular vessel.

(5) Assuming the time between failures to be a Poisson distributed random variable (see, e.g. Grimmett & Stirzaker, 2001, Section 6.8), the probability of failure of a particular component j on vessel i in one random year is given by

$$\pi_j(i) = 1 - e^{-\lambda_j(i)}. \tag{1}$$

For each vessel, parameters λ_j (which are reciprocals of the corresponding MTBFs) are defined for vents of at most two different types ($j = 1, 2$), detectors of a single type ($j = 3$) and suppressors of at most two different types ($j = 4, 5$). These parameters and the values used in our spray drier example are tabulated in Table 2. The MTBFs shown in the table are not meant to be accurate or even pertinent for the specific hardware, but are deemed to be representative for our purpose. For simplicity, we assume that $\pi_j(i)$ for a given j is the same for all the vertices i in the graph, although different vessels may have protection components of different makes (and hence different MTBFs) in reality.

(6) In addition, different vessels are grouped together into zones (or equivalently, different vertices are grouped together into sub-graphs). Each zone has a single control panel with a specified MTBF ($\lambda_6(j)$ for a zone j). All the suppressors in a zone are deployed simultaneously with any detection in the zone. Grouping protection systems into zones reduces the consequence of flame transfer between vessels in the same zone.

(7) A fast acting valve may be installed between two vessels i, k to reduce the possibility of flame passage. Its MTBF is represented by $\lambda_7(i, k)$, with $\pi_7(i, k)$ computed as in (1).

(8) If there is a suppressor installed on a pipe connecting two vessels i and j, its MTBF is denoted by $\lambda_4(i, j)$ and the probability of its failure is denoted by $\pi_4(i, j)$.

(9) $P_{red}(i, j)$ is the reduced pressure at vertex i due to ignition at vertex j and $P_s(i)$ is the pressure shock resistance of vertex i. Both $P_{red}(i, j)$ and $P_s(i)$ are assumed to be independent normal variables with specified means and variances which are assumed to be stationary through time. The specified values of these parameters are intentionally very conservative both representing the worst case, to err on the side of caution. A judgement needs to be made about the choice of mean values of these variables to ensure that the computation of risk is realistic and is not affected excessively by the built-in safety factors in the design of any protection system. We have elected a standard deviation of 10% of the nominal value for both $P_{red}(i, j)$ and $P_s(i)$, and the values quoted for $P_{red}(i, j)$ and $P_s(i)$ are two standard deviation limit values.

(10) $Q_{vessel}(i, j)$ represents the probability that the explosion protection hardware system does not fail but the reduced pressure is still higher than the pressure shock resistance of the vessel:

$$Q_{vessel}(i,j) = \mathbf{P}(P_{red}(i,j) - P_s(i) > 0). \tag{2}$$

This allows us to represent the proximity of $P_{red}(i, j)$ to $P_s(i)$ in the system design and account for any intentional design safety factors in our computation of residual risk.

(11) In a similar manner we can define a set of parameters relating to the connectivity between plant items and any isolation barriers installed. $t_b(i, j)$ is the time from ignition, for the flame propagation barrier (either a chemical barrier or a valve) to be

Table 2
Notation for $\pi_j(i)$ and values for the spray drier example (only one type of vent panel assumed).

Component	j	$1/\lambda_j(i)$	$\pi_j(i)$ (or $\pi_j(i, k)$ for valve)
Vent panel type 1	1	50 000	0.000020
Detector	3	4000	0.000250
Suppressor type 1	4	30 000	0.000033
Suppressor type 2	5	50 000	0.000020
Control panel	6	25 000	0.000040
Valve	7	2000	0.000500

Please cite this article in press as: Date, P., et al., Modelling the risk of failure in explosion protection installations, Journal of Loss Prevention in the Process Industries (2009), doi:10.1016/j.jlp.2009.03.007

established when the flame is propagating from an ignition in vessel i to vessel j and $t_f(i,j)$ is the time that the flame front will arrive at the barrier location. $t_b(i,j)$ and $t_f(i,j)$ are assumed to be independent normal variables with specified means and variances which are stationary through time. Once again, the specified values of these parameters are invariably very conservative, both representing the worst case to err on the side of caution. For reasons similar to those employed for $P_{red}(i,j)$ and $P_s(i)$, we have chosen to assume a standard deviation of 10% of the nominal value for both $t_b(i,j)$ and $t_f(i,j)$, and that the values quoted for $t_b(i,j)$ and $t_f(i,j)$ are the two standard deviation limit values. $Q_{barrier}(i,j)$ in (3) represents the probability that the isolation barrier hardware is actuated and the barrier is established, but the barrier is deployed too late to stop the flame from reaching the next vertex.

$$Q_{barrier}(i,j) = \mathbf{P}\Big(t_b(i,j) - t_f(i,j) > 0\Big). \tag{3}$$

(12) Let $Q_f^s(i,j)$ be the fundamental flame propagation probability between vertices i and j. This will depend on duct diameter and length, the relative volumes of connected vessels, the material explosibility, etc. Relative magnitudes of these probabilities may be determined from qualitative knowledge. As an example, $Q_f^s(2,3)$ is likely to be significantly higher than $Q_f^s(1,3)$ in the spray drier installation mentioned in the previous section, for any realistic protection installation. The total flame propagation probability from vertex i to vertex j, $Q^s(i,j)$, is the summation of the probability of complete hardware failure of barrier and the probability due to late activation of barrier:

$$Q^s(i,j) = Q_f^s(i,j) \times \Big(Q^h(i,j) + \Big(1 - Q^h(i,j)\Big) \times Q_{barrier}(i,j)\Big), \tag{4}$$

where $Q^h(i,j)$ is the probability of hardware failure and $(1 - Q^h(i,j)) \times Q_{barrier}(i,j)$ is the failure due to late activation of barrier. $Q^h(i,j)$ may itself be computed as $\pi_3(i) + (1 - \pi_3(i))\pi_4(i,j)$ if the preceding vessel i is protected passively by explosion venting and a single detector or as $\pi_4(i,j)$ if the preceding vessel is protected by explosion suppression. The reason for this difference is that the failure of detector in the latter case will cause the vessel i to fail, and its role in the flame propagation to vessel j is then insignificant. The case when the preceding vessel has multiple detectors can be dealt by using $\beta(i)$ defined in the next section in place of $\pi_3(i)$, in the computation of $Q^h(i,j)$ above.

When all the above parameters are specified for each vertex and each edge in the graph, we have all the information necessary to compute residual risk in the system. There are a variety of ways in which this information can be represented in software. The purpose of this paper, however, is to outline a methodology rather than to discuss its precise implementation.

It is also worth mentioning that the residual risk computed using this method is valuable mainly as a tool for comparison of different configurations of explosion protection systems, *e.g.* using different types of suppressors on a vessel yielding different P_{red} or using a mechanical barrier (i.e. a valve) instead of a chemical barrier (i.e. a suppressor). Some of the parameters above (such as $Q_f^s(i,j)$) have to be based on qualitative knowledge and some of the assumptions are not realistic in all situations (such as the exact ignition location is ignored). However, provided the *same* assumptions and the *same* parameters are used in computing the residual risk for two or more safety system configurations, the model provides very valuable information enabling the user to make an informed decision about the choice of the safety system.

Table 3
Computation of $\alpha_1(i)$ and $\alpha_2(i)$ based on the number of vent panels ($k_1(i)$, $k_2(i)$) and $\pi_j(i)$ as defined in equation (5).

	$k_1 = k_2 = 0$	$k_1 > 0, k_2 = 0$	$k_1 > 0, k_2 > 0$
α_1	0	$\sum_{j=0}^{k_1-1}(1-\pi_1(i))^j \times \pi_1(i)$	$\sum_{j=0}^{k_1-1}(1-\pi_1(i))^j \times \pi_1(i)$
α_2	0	0	$\sum_{j=0}^{k_2-1}(1-\pi_2(i))^j \times \pi_2(i)$

We support this assertion by way of a detailed illustration in Section 5.

4.3. Algebraic formula for computation of risk

The risk of failure of any vertex i due to ignition in vertex j is denoted by $R_{i,j}$ and it can be computed as the sum of risk of hardware failure and the risk of inadequate protection:

$$R_i' = \alpha(i) + (1-\alpha(i))\beta(i) + (1-\alpha(i))(1-\beta(i)) \times \gamma(i), \tag{5}$$

$$R_{i,j} = R_i' + \left(1 - R_i'\right) \times Q_{vessel}(i,j) \tag{6}$$

where $\alpha(i) = \alpha_1(i) + (1-\alpha_1(i)) \times \alpha_2(i)$ is the probability of failure of any one vent panel. The computation of $\alpha_1(i)$ and $\alpha_2(i)$ based on the number of vent panels is summarised in Table 3.

$$\begin{aligned}\beta(i) &= \textstyle\sum_{j=0}^{k_3-1}(\pi_3(i))(1-\pi_3(i))^j \quad \text{if } k_3 > 0,\\ &= 0 \quad \text{otherwise}\end{aligned}$$

is the probability of failure of any one detector and $\gamma(i) = \gamma_1(i) + (1-\gamma_1(i))\gamma_2(i)$ is the failure probability of failure of any one suppressor. The computation of $\gamma_1(i)$, $\gamma_2(i)$ based on the number of suppressors is summarised in Table 4.

The terms in the expression (6) for $R_{i,j}$ may be explained as follows. The first term in the expression (5) for R_i' represents an explosion due to an ignition event not being vented. The second term represents an explosion due to an ignition event not being detected. The last term represents an explosion due to failure of suppressor of either types. R_i' as a whole represents the probability that an unmitigated explosion occurs in vessel i due to hardware failure, given an ignition event. Finally, the second term in the expression for $R_{i,j}$ represents the failure of vessel i due to partial or inadequate protection.

The risk of failure of any vertex due to an ignition in vertex i may be denoted by δ_i and can be computed as:

$$\delta_i = Q_E(i)\left(R_{i,i} + \left(1 - R_{i,i}\right)\sum_{j\in\Phi_i} Q^s(i,j) \times R_{j,i}\right) \tag{7}$$

where Φ_i denotes the set of vertices adjacent to vertex i. Each $R_{j,i}$ is computed as in (6). Note that the first term represents an event where an ignition in vertex i causes an unmitigated explosion in the vertex i. The second term with a summation over j represents an event where there is no unmitigated explosion in vertex i given an ignition in the same vertex, however, the flame propagates to a neighboring vertex j causing an unmitigated explosion in vertex j.

Instead of computing "per-ignition" risk (due to ignition in each vertex i) δ_i as above, one may choose to compute "per-vertex" risk,

Table 4
Computation of $\gamma_1(i)$ and $\gamma_2(i)$ based on the number of suppressors ($k_4(i)$, $k_5(i)$) and $\pi_j(i)$ as defined in equation (5).

	$k_4 = k_5 = 0$	$k_4 > 0, k_5 = 0$	$k_4 > 0, k_5 > 0$
γ_1	0	$\sum_{j=0}^{k_1-1}(1-\pi_4(i))^j \times \pi_4(i)$	$\sum_{j=0}^{k_1-1}(1-\pi_4(i))^j \times \pi_4(i)$
γ_2	0	0	$\sum_{j=0}^{k_2-1}(1-\pi_5(i))^j \times \pi_5(i)$

Please cite this article in press as: Date, P., et al., Modelling the risk of failure in explosion protection installations, Journal of Loss Prevention in the Process Industries (2009), doi:10.1016/j.jlp.2009.03.007

i.e. the total risk of failure in each vertex due to ignition in the same vertex or any of the connecting vertices. Denoting this risk by ζ_i, it can be seen that

$$\zeta_i = Q_E(i) \times R_{i,i} + \sum_{i \in \Phi_j} Q_E(j) \times (1 - R_{j,j}) \times Q^s(j,i) \times R_{i,j} \tag{8}$$

The overall residual risk R is computed as

$$R = \sum_j \left\{ \pi_6(j) + (1 - \pi_6(j)) \times \sum_{i \in \Psi_j} \zeta_i \right\} \tag{9}$$

where the summation is over all zones and Ψ_1, Ψ_2, … are zones with corresponding control panel MTBFs $\lambda_6(1)$, $\lambda_6(2)$, etc.

Note that the sum of probabilities can theoretically exceed unity in the computation of ζ_i, δ_i, etc. However, the risk of failure in any vessel approaching unity would be an unrealistic (and certainly unacceptable) scenario in any practical safety installation and we have chosen to ignore such unrealistic cases from our model. If necessary, these cases can be dealt with using $\min(\cdot, 1)$ operator throughout the computation of probability parameters. In case where $\min(\cdot, 1)$ is used to limit probability to 1, R can no longer be interpreted as a probability. However, it will still serve as a (somewhat heuristic) measure of residual risk.

Here, it is worth re-emphasizing that the risk R is computed for one unit of time and a different value will be obtained if we consider a different length of time (and hence a different set of parameters). In any case, the proposed computational model cannot be expected to yield an *exact* value of residual risk for a particular length of time, since some of the underlying assumptions are based on qualitative knowledge and cannot be easily verified. However, as mentioned in Section 4.2, the main purpose of this model is to compare two or more safety configurations under the same set of parameters, time horizon and assumptions.

From a representational point of view, it is possible to model R'_i in (5) as a fault tree (see, e.g. Bedford & Cooke, 2001; O'Connor, 2002). However, this does not seem to benefit the actual computation of residual risk and hence is not explored further.

Lastly, it is worth mentioning that knowledge of graph theory is *not* required for the implementation of the model. The representation of the system is in terms of a set of vertices, which may be represented by a variety of data structures, while the computational model is in terms of simple algebraic formulae.

5. Example of the computation of residual risk

5.1. Description of the process

Fig. 1 shows our example of a simple spray drying process, with its vertices enumerated in Table 1. Using suitable fuel explosibility rate constant, maximum explosion pressure, vessel volumes, vessel strengths, detection pressures and vent activation pressures for the protection system it is possible to derive predicted reduced explosion pressures for each plant item, either using proprietary software (e.g. Siwek & Cesana, 2001) or in-house software packages (the numerical values used for computation of model parameters are available from the authors). Of course, other means for calculating or deriving these pressures are equally valid. Those pertinent to our example are shown in Table 5. Table 6 lists the t_b, t_f and $Q_{barrier}(i,j)$ values for those plant interconnections where explosion isolation is employed. t_b and t_f have been calculated using our in-house calculation tools with representative hardware and input parameters, such as material explosibility, vessel size, duct diameter and process air flow. Once again other means for calculating these times are equally valid.

Table 5
Probabilities of flame propagation through interconnections.

(i,j)	$Q^s_j(i,j)$	$Q^h(i,j)$	$Q_{vessel}(i,j)$
(1,2)	5.20×10^{-3}	1.00	1.00
(1,2)	8.98×10^{-3}	3.33×10^{-5}	1.00
(1,3)	5.13×10^{-3}	1.00	1.00
(1,4)	2.86×10^{-2}	1.00	1.82×10^{-2}
(1,5)	2.86×10^{-2}	1.00	1.82×10^{-2}
(2,1)	5.75×10^{-3}	5.00×10^{-4}	5.95×10^{-11}
(2,1)	8.12×10^{-3}	1.00	5.95×10^{-11}
(2,3)	5.40×10^{-3}	1.00	1.00
(2,3)	8.98×10^{-3}	1.00	1.00
(2,3)	5.48×10^{-3}	1.00	1.00
(3,1)	5.75×10^{-3}	5.00×10^{-4}	1.00
(3,2)	5.48×10^{-3}	1.00	1.00
(3,2)	8.12×10^{-3}	1.00	1.00
(3,2)	5.48×10^{-3}	1.00	1.00
(4,1)	1.05×10^{-1}	1.00	5.95×10^{-11}
(4,5)	2.60×10^{-1}	1.00	1.82×10^{-2}
(5,1)	1.05×10^{-1}	1.00	5.95×10^{-11}
(5,4)	2.60×10^{-1}	1.00	1.82×10^{-2}

Table 6
$Q_{barrier}(i,j)$ for two isolation barriers.

	$Q_{barrier}(i,j)$
Isolation barrier 1 (1,2)	2.09×10^{-5}
Isolation barrier 2 (2,1)	2.34×10^{-3}
Isolation barrier 2 (3,1)	6.66×10^{-11}

Finally we need to determine the probability of flame propagation between vertices. As described in Section 4.2, this comprises terms for the hardware $Q^h(i,j)$ and the fundamental flame propagation probability $Q^s_j(i,j)$. We must ascribe a value for the latter, and this is subject to a degree of uncertainty. However, with the large corpus of experimental data available both in the literature and in-house, it is possible to determine 'representative' values depending on the particular geometric configuration (source vessel, duct diameter and length, etc.) and material explosibility.

The connectivity parameters relevant of our example are shown in Table 5 and are deemed representative for the example process plant and elected isolation hardware. It should be noted that in the case where there are multiple flame paths between vertices (e.g. there are three between the two fluid bed driers), then the arithmetic sum of the probabilities is taken to err on the side of safety. We can now calculate the residual risk of safety system failure due to either an ignition in vertex i (per-ignition risk, δ_i) or the total risk of failure of each vertex due to ignition in any vertex (per-vertex risk, ζ_i). These residual risks are shown in Tables 7 and 8 respectively. We have assumed in this instance that the probability of ignition for each vertex is equal, which is not unreasonable considering the nature of the spray drying process. However, this would not be the case in a process plant where one vessel was much more likely to have an explosion due to the propensity of ignition sources (e.g. sparks from a grinder).

Table 7
Risk computation per ignition (with three zones).

δ_1	3.41×10^{-3}
δ_2	6.49×10^{-3}
δ_3	6.26×10^{-3}
δ_4	3.14×10^{-3}
δ_5	3.14×10^{-3}

Please cite this article in press as: Date, P., et al., Modelling the risk of failure in explosion protection installations, Journal of Loss Prevention in the Process Industries (2009), doi:10.1016/j.jlp.2009.03.007

Table 8
Risk computation per vessel (with three zones).

ζ_1	1.11×10^{-4}
ζ_2	7.95×10^{-3}
ζ_3	7.77×10^{-3}
ζ_4	4.64×10^{-4}
ζ_5	4.64×10^{-4}

Table 9
Risk Computation per vessel (with two zones).

ζ_1	1.11×10^{-4}
ζ_2	2.23×10^{-3}
ζ_3	2.25×10^{-3}
ζ_4	4.64×10^{-4}
ζ_5	4.64×10^{-4}

Table 10
Risk computation per vessel (with one zone).

ζ_1	1.10×10^{-4}
ζ_2	7.37×10^{-4}
ζ_3	7.37×10^{-4}
ζ_4	4.64×10^{-4}
ζ_5	4.64×10^{-4}

For the same process and the same protection hardware, the safety configuration can be changed by changing the zones in the protection system. From Fig. 1 we can see that the protection system is divided into three discrete 'zones', whereby detection in any one zone leads to the actuation of all the suppressors in that zone only. From Table 5 we can see there is a high level of connectivity between the two fluid bed driers, and the consequence of flame transfer would lead to an enhanced explosion in the connected vessel. This enhanced secondary explosion is likely to be more severe than the point ignition assumption that was used in designing the explosion protection on this plant item. This of course affects the calculated risk for this vertex as can be seen by the magnitude of $Q_{\text{vessel}}(2, 3)$. In order to reduce this risk, it would be common practice to merge zone 2 and zone 3 such that actuation of either detector on the fluid bed driers would deploy both suppression systems. This will significantly reduce the explosion severity in the connected vessel since any flame that does transfer will be trying to ignite an atmosphere that will be engulfed in suppressant. This is represented in our calculation as can be seen from Table 9 where the residual risk in both the fluid bed driers (ζ_2 and ζ_3) is now much reduced.

It is interesting to continue this line of action and combine the whole protection system into a single zone and recalculate ζ_i, see Table 10. With all three vessels under the same control zone, $Q_j^s(i, j)$ for the connections between these vessels is set to zero. While this yields further reduction in ζ_2 and ζ_3, the isolation barriers no longer add benefit in terms of residual risk and may be considered an inefficient use of financial resources directed towards plant safety. Further, a single zone system is more prone to nuisance actuations.

The interested reader is referred to Ganguly, Date, Mitra, Lade, and Moore (2007), Lade and Moore (2008) and Moore and Lade (2009) for further and more extensive use of this model of computing the residual risk of safety system failure.

6. Conclusion

This paper addresses the problem of ascribing residual risk for an industrial explosion protection system. Drawing on the domain knowledge of explosion protection professionals, we have designed a simple but effective algebraic model based on bi-directed graphs to compute the residual risk. This also demonstrates the adaptation of existing analytical tools in operational research to challenging, real life problems. The proposed model captures the residual risk of a protection installation in a meaningful way and allows us to analyze quantitatively the cost/benefit trade-offs in different protection system configurations. Even though some of the mathematical tools used will be unfamiliar to the process engineers, the actual methodology is quite simple to implement and does not require knowledge of graph theory. The authors feel that this model is an extremely useful aid for better and more informed design decisions, leading to enhanced overall process safety and greater overall cost-effectiveness in protection system design.

The methodology presented here is suited for explosion protection systems in industrial process plants. Modification and adaptation of this model to address specific issues in the computation of risk for other explosion protection applications, such as protection on offshore platforms, is a topic of current research.

At present, this methodology has been implemented on trial examples in a prototype software at Kidde Research, UK. A full-scale implementation along with drafting of the required design rules and carrying out the necessary physical experiments is currently in progress.

Acknowledgements

The authors are grateful to Prof. Roger Cooke at Resources for the Future (RFF) for helpful discussions, and to Mr Robert Pallant from Kidde Research for his help in data analysis and interpretation. The authors would also like to thank doctoral students Ms T. Ganguly and Mr T. Ji at Department of Mathematical Sciences, Brunel University for their assistance in the software implementation.

References

ATEX (2005). *Guidelines on the application of council directive 94/9/EC of 23 March 1994 on the approximation of the laws of the member states concerning equipment and protective systems intended for use in potentially explosive atmospheres*. European Commission.
Bartknecht, W. (1993). *Explosionsschutz – Grundlagen und Anwendung*. Berlin, Heidelberg, New York: Springer Verlag.
Barton, J. (2002). *Dust explosion prevention and protection: a practical guide*, Institution of Chemical Engineers.
Bedford, T., & Cooke, R. (2001). *Probabilistic risk analysis: Foundation and methods*. Cambridge University Press.
Eckhoff, R. (2003). *Dust explosions in the process industries*. Elsevier.
Ganguly, T., Date, P., Mitra, G., Lade, R. J., & Moore, P. E. (2007). A method for computing the residual risk of safety system failure. In *Proceedings of the 12th international symposium on loss prevention and safety promotion in the process industries*. Edinburgh, UK.
Grimmett, G., & Stirzaker, D. (2001). *Probability and random processes*. Oxford University Press.
Holbrow, P., Lunn, G. A., & Tyldesley, A. (1999). Dust explosion protection in linked vessels: guidance for containment and venting. *Journal of Loss Prevention in the Process Industries, 12*, 227–234.
Lade, R., & Moore, P. (2008). A methodology to guide industrial explosion safety system design. In *Proceedings of hazard XX: process safety and environment protection*. Manchester, UK.
Moore, P., & Lade, R. (2009). Quantifying the effectiveness of explosion protection measures. In *Proceedings of the 11th process plant safety symposium*. Tampa, USA.
Moore, P., & Spring, D. (2004). Design of explosion isolation barriers. In *Proceedings of hazards XVIII: process safety*. Manchester, UK.
O'Connor, P. (2002). *Practical reliability engineering*. John Wiley and Sons.
Siwek, R., & Cesana, C. (2001). Software for explosion protection, WinVent and ExTools. *Safe handling of combustible dusts*. 1601, Nuremberg: VDI Bewrichte.
Van der Voort, M. M., Klein, A. J. J., de Maaijer, M., van den Berg, A. C., van Deursen, J. R., & Versloot, N. H. A. (2007). A quantitative risk assessment tool for the external safety of industrial plants with a dust explosion hazard. *Journal of Loss Prevention in the Process Industries, 20*, 375–386.
West, D. (2001). *Introduction to graph theory*. Prentice Hall.

Please cite this article in press as: Date, P., et al., Modelling the risk of failure in explosion protection installations, Journal of Loss Prevention in the Process Industries (2009), doi:10.1016/j.jlp.2009.03.007