

A METHODOLOGY TO GUIDE INDUSTRIAL EXPLOSION SAFETY SYSTEM DESIGN

R J Lade[1] and P E Moore[2]
[1]Kidde Research, Mathisen Way, Poyle Road, Colnbrook, Berkshire, SL3 0HB, UK, Phone: +44 1753 689848. Fax: +44 1753 683810.
[2]UTC Fire & Security, Mathisen Way, Poyle Road, Colnbrook, Berkshire, SL3 0HB, UK, Phone: +44 1753 689848. Fax: +44 1753 683810.

Process plant owners/operators have an obligation to assess and ascribe the residual risk of an unmitigated explosion occurrence under the ATEX Directives, and in doing so are making a key decision on the acceptability of that residual risk. All safety systems have a residual risk that they fail to achieve their mission, whether it be via hardware failures, personnel errors, errors in the theoretical and design assumptions, or inadequacies in the quantification of the prevailing hazard.

It is essential that suppliers and users of explosion protection products and systems fully understand the efficacy and reliability upon demand of such products and systems. A systematic methodology for quantifying residual risk in the context of installed explosion mitigation has been described by the authors. This methodology explicitly accounts for the two principal mechanisms of failure:

a) failure of the hardware;
b) ineffective explosion protection (e.g. the reduced explosion pressure of a suppressed or vented explosion occurrence is greater than the pressure shock resistance of the vessel).

This paper considers the challenges faced in determining a meaningful residual risk datum for a processing plant. In particular it sets out the importance of the implicit assumptions and shows, by reference to process industry examples, the benefits of electing a systematic means of ascribing explosion protection security.

In order to quantify the residual risk of safety system failure in the practice, an overarching understanding of the efficacy of explosion mitigation means, system design, safety factors (both implicit and explicit) and the consequence of flame propagation between connected vessels, is of paramount importance. Existing explosion protection design guidance is invariably constructed around test data that have taken the premise that central ignition of a homogeneous and turbulent optimum fuel concentration in a closed vessel represents the worst case scenario. However this is not necessarily the most appropriate baseline for ascribing the risk of an unmitigated explosion occurrence.

This work demonstrates that explosion protection "trade off" decisions, design safety factors, and the design premise itself all contribute to the "relied upon" safety integrity of an industrial process. With this understanding and the adoption of a systematic methodology to determine a residual risk datum, practitioners can make more informed and cost effective design decisions, leading to enhanced overall process safety.

DESCRIPTION OF THE CALCULATION METHODOLOGY

A method for calculating residual risk of safety system failure has been set out previously by the authors [Ganguly, 2007], and the pertinent mathematical derivations are fully explained elsewhere [Date, 2008]. In this paper we present a brief description of the model and its implicit assumptions, using the same nomenclature as previously, for ease of reference.

Our intention is to demonstrate the value of such an approach to improve overall process safety. The process plant and its protection system are represented by a connected, bi-directional graph (West, 2001). In this architecture each plant item in the process is represented as a vertex, whereby edges between vertices represent possible flame paths (i.e. the connecting duct-work).

ASSUMPTIONS

- We use the probability of an unmitigated explosion in a given unit of time as a proxy for residual risk.
- All ignition locations within each plant item are equally probable.
- An unmitigated explosion (failure) is defined as any occurrence where the reduced explosion pressure of a suppressed or vented explosion is greater than the pressure shock resistance of a plant component.
- Given an ignition event, an unmitigated explosion is assumed to occur when any one component of the protection system fails, be it a vent panel, detector, suppressor or control panel. Consideration of component redundancy and the impact on residual risk is fully tractable, but is not addressed further here.
- We consider the consequence of all failures equally. In reality, not all failures will lead to a catastrophe, however by comparing all failures equally we are still able to compare different safety system designs.
- We only consider the probability of failure of the plant item that has the ignition event and those directly connected to it. The model is not bound by this assumption – extension to second order connectivity is tractable, but of negligible significance.

DEFINITION OF MODEL PARAMETERS

Each vessel or plant item i (vertex i) within the process plant, together with its associated explosion protection system is characterised by a set of parameters which are described in this section.

- $Q_E(i)$ is the ignition probability in vessel i. For a given process plant and over a given unit of time we assume that $\sum_i Q_E(i) = 1$, i.e. that there will be one ignition occurrence somewhere in the process plant.
- $P_{red}(i, j)$ is the reduced explosion pressure in vertex i following an ignition in vertex j. $P_s(i)$ is the pressure shock resistance of the vertex i. The values quoted for $P_{red}(i, j)$ and

$P_s(i)$ are intentionally very conservative to represent the worst case and to err on the side of safety. However, excessive safety factors will result in unrealistic values for the computed residual risk. We have elected to use a standard deviation of 10% of the mean value for both $P_{red}(i, j)$ and $P_s(i)$, and that the values specified are the two standard deviation limit values.

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

$$Q_{vessel}(i, j) = P[P_{red}(i, j) - P_s(i) > 0] \tag{1}$$

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.

- In a similar manner, we can define a set of parameters which relate to the efficacy of explosion isolation barriers. We define $t_b(i, j)$ as the time taken from ignition for the isolation barrier to be established between vessels i and j. Implicit in $t_b(i, j)$ is the time taken to detect the explosion (whether via optical or pressure detection) and the actuation time of the isolation hardware such that flame cannot pass. $t_f(i, j)$ is the time taken for the flame front to arrive at the barrier location, and will be the summation of the time taken for the flame to enter the duct from the ignition location, and the time for the flame to transit the duct to the barrier position. Thus for efficacious explosion isolation $t_f(i, j) > t_b(i, j)$. Once again the specified values for these parameters are very conservative and we apply the same assumptions as with the pressure parameters, taking a standard deviation of 10% of the mean and that the specified values are the two standard deviation limit values.
- $Q_{barrier}(i, j)$ represents the probability that the isolation hardware is actuated and the barrier established, but the barrier is deployed too late and flame passes into the adjoining vessel:

$$Q_{barrier}(i, j) = p[t_b(i, j) - t_f(i) > 0] \tag{2}$$

- $Q_f^s(i, j)$ is the probability of flame propagation between connected vessels i and j which then leads to an enhanced explosion in j. This of course will be sensitively dependent on the geometric configuration (relative vessel sizes, duct length and diameter, process flow direction and velocity) together with the fuel properties and the explosion mitigation means employed on both the source and connected vessels.
- The total flame propagation probability from vessel i to j, $Q^s(i, j)$, can be computed by summing the probability due to hardware failure ($Q_h(i, j)$) and the probability due to late activation of the barrier $1 - (Q_h(i, j)) \times Q_{barrier}(i, j))$ to give:

$$Q^s(i, j) = Q_f^s(i, j) \times [Q_h(i, j) + (1 - Q_h(i, j)) \times Q_{barrier}(i, j)] \tag{3}$$

- $Q_h(i, j)$ can be calculated with knowledge of the mean-time-between-failure of the hardware components combined in an appropriate manner to represent the configuration of the protection system [Date, 2008, Ganguly, 2007].

When all of the above parameters have been specified for each vessel and connection, we have all the necessary information to compute the residual risk of safety system failure.

COMPUTATION OF RESIDUAL RISK

The risk of failure of any vessel i due to ignition in vessel j, is denoted $R_{i,j}$ and can be computed as the sum of the risk of hardware failure, $Q_h(i)$, and the risk of inadequate protection, $(1 - Q_h(i)) \times Q_{vessel}(i, j)$:

$$R_{i,j} = Q_h(i) + (1 - Q_h(i)) \times Q_{vessel}(i, j) \tag{4}$$

Once again, $Q_h(i)$ can be calculated with knowledge of the mean-time-between-failure of the pertinent hardware. We can now calculate the risk of failure in any vessel i due to an ignition in the same vessel or any vessel directly connected, ζ_i, as:

$$\zeta_i = Q_E(i) \times R_{i,i} + \sum_{i \in \Phi j} Q_E(j) \times (1 - R_{j,j}) \times Q^s(j,i) \times R_{i,j} \tag{5}$$

where Φ_i, denotes the set of vertices adjacent to vertex j.

EXAMPLE COMPUTATION OF RESIDUAL RISK

To illustrate this calculation methodology and demonstrate its use in guiding explosion safety system design, we consider the example of a simple milling and collection process (see Figure 1), where explosible dust represents the principal hazard [Eckhoff, 2003]. In this process a granulated chemical product is fed into a Grinder, and the product fines are pneumatically transported to a Storage Hopper. Residual dust from the Cyclone is extracted by a Bag-Filter before the process air is returned to the atmosphere. The Bag Filter and the Storage Hopper are protected by explosion suppression systems, whilst the Grinder and Cyclone are protected by appropriately sized explosion vent panels. In this example, a fast-acting explosion isolation valve has been installed to minimise the risk of flame propagation from the Grinder to the Cyclone.

First we must ascribe ignition probabilities ($Q_E(i)$) for the four vessels in our example process. This will of course be dependent on the material being processed (e.g. explosibility, concentration, minimum ignition energy etc.) and the nature of the process. In order to attain representative values we have taken literature data [Jeske, 1997] and organised it so as to be able to quote typical ignition probabilities for generic plant processes. Part of the organisation of this data involved excluding ignition sources that were external to the process, such as fire, and then grouping ignition sources that were pertinent to generic plant processes and then normalising these probabilities. Although this methodology is a simplification of the practice, it is based on real data and serves the purpose of providing representative ignition probabilities. The $Q_E(i)$ values determined for each vessel in our example are shown in Table 1. Also shown in Table 1 are the vessel strengths, $P_s(i)$, and the reduced

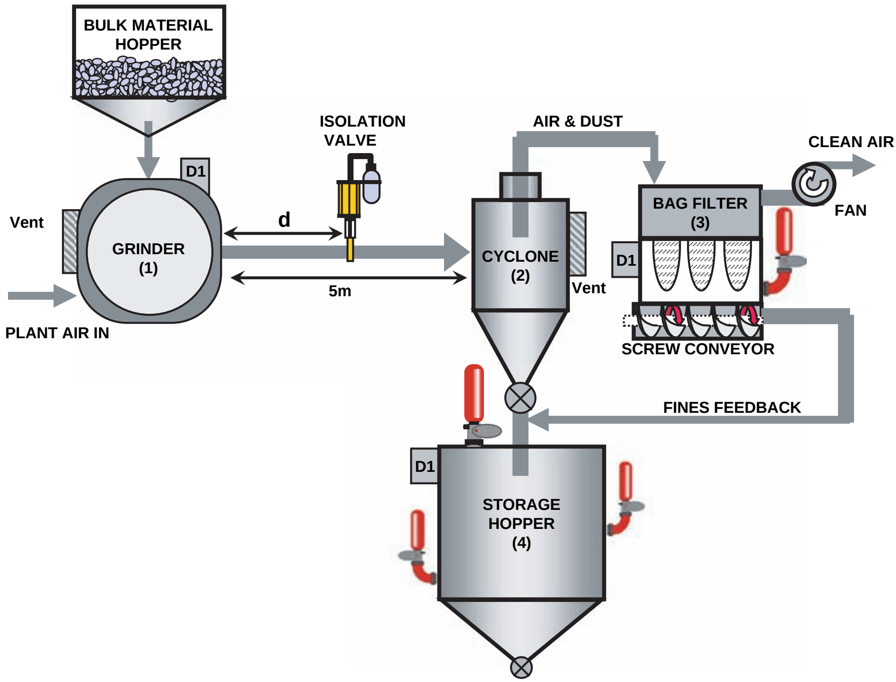

Figure 1. Schematic representation of an example milling and collection process. The grey arrows represent material flow through the plant. d represents the installed distance of the isolation barrier from the Grinder

Table 1. Ignition probabilities, $Q_E(i)$, pressure shock resistance, $P_s(i)$, reduced explosion pressure, $P_{red}(i, i)$, and the probability that the explosion protection hardware does not fail, but the reduced explosion pressure is still higher that pressure shock resistance of the vessel, $Q_{vessel}(i, i)$, (calculated using Equation 2) for each vertex in the example milling and collection process

Plant item	Vertex	$Q_E(i)$	$P_s(i)$/bar(g)	$P_{red}(i,i)$/bar(g)	$Q_{vessel}(i, i)$
Grinder	1	67%	0.55	0.50	2.34×10^{-4}
Cyclone	2	11%	0.45	0.42	1.29×10^{-4}
Bag filter	3	17%	0.40	0.40	6.52×10^{-3}
Storage hopper	4	5%	0.30	0.28	4.60×10^{-4}

explosion pressures from an ignition in i, $P_{red}(i, i)$, the latter being determined by using either proprietary software [Siwek, 2001] or in-house software packages [Moore, 2001]. Other means of calculating these pressures are equally valid.

We also need to determine $P_{red}(i, j)$ when $i \neq j$. This is the reduced explosion pressure following flame transfer from a connected vessel resulting in a flame jet ignition event. The resulting explosion incident is often more severe than the point ignition assumption that was used in designing the explosion protection on the connected plant item. The extent of the explosion enhancement due to flame jet ignition for our example has been estimated by referring to the literature data regarding this phenomenon, [Lunn,1996; Holbrow, 1996]. From these data the explosion enhancement was interpolated using the dust variant of an industry standard computational fluid dynamic (CFD) explosion modelling tool (FLACS,2005). Table 2 lists the $P_{red}(i, j)$ values for each connected vessel.

Next we need to represent the fast-acting explosion isolation valve fitted between the Grinder and the Cyclone at a distance, d = 3 m from the Grinder, see Figure 1. In this example the isolation valve relies upon a pressure detector fitted to the Grinder. The closing time of such a valve is typically 40 ms and we calculate $t_b(1,2) = 79$ ms, and $t_f(1,2) = 49$ ms using our in-house software package [Moore, 2005] with representative input parameters such as duct diameter, air flow, material explosibility etc. Other means of calculating these times are equally valid. This is **not** an explosion isolation solution since $t_b(1,2) > t_f(1,2)$ as a consequence of the valve being located too close to the Grinder, and therefore not prEN150089:2006 compliant.

Table 2 also lists $Q_f^s\ (i, j)$ for each flame path, together with the resulting $Q^s(i, j)$. $Q_f^s\ (i, j)$ has been determined from the large corpus of experimental data generated by Holbrow et al. [Holbrow, 1996] together with our own test data. A large proportion of these data sets are for explosions in connected vented vessels, therefore $Q_f^s\ (i, j)$ needs to be adjusted to represent configurations where either the source, connected or both vessels

Table 2. Reduced explosion pressure in vertex i following an ignition in vertex J, $P_{red}(i, j)$, the probability of flame propagation leading to an enhanced explosion in j, $Q_f^s(i, j)$ and total flame propagation probability, $Q^s(i, j)$, for each connection in the example milling and collection process

(i, j)	$P_{red}(i, j)$/bar(g)	$Q_f^s, (i, j)$	$Q^s(i, j)$
(1,2)	1.00	0.320	0.218
(2,1)	0.70	0.261	0.261
(2,3)	0.72	0.080	0.080
(3,2)	0.86	0.013	0.013
(3,4)	0.83	0	0
(4,3)	0.50	0	0
(4,2)	0.49	0.047	0.001
(2,4)	0.66	0.009	0.001

have explosion suppression systems fitted. The extent and form of this adjustment is work in-progress and so we have elected the following considered assumptions. Here V_1 refers to the source vessel where the ignition occurs and V_2 is the connected vessel.

- **V_1 Suppressed : V_2 Vented:** With the source vessel suppressed, only ignition locations close to the duct mouth will allow flame to enter the duct before the vessel is engulfed with suppressant. These ignition locations represent only a small fraction (~5%) of the vessel volume† and we have adjusted $Q_f^s\,(i, j)$ according to this criteria.
- **V_1 Vented : V_2 Suppressed:** If the source vessel is vented then flame transfer to V_2 is as probable as in the vented:vented case. However, in most configurations the pressure in the connected vessel will have risen sufficiently such that the suppression system will have actuated before the flame arrives at the vessel. The experimental data, supported by our CFD investigations show that on average only 25% of occurrences result in flame entry in V_2 before the suppressant has essentially engulfed the vessel volume. Once again we have elected this criteria to adjust $Q_f^s\,(i, j)$.
- **V_1 Suppressed : V_2 Suppressed:** With both vessels suppressed, it is difficult to envision a situation whereby an enhanced explosion in the connected vessel can occur, and we have therefore elected to set $Q_f^s\,(i, j)$ at zero for this scenario.

In our example, $Q^s\,(1,2)$ will of course include terms for the isolation hardware, $Q_h\,(1,2)$, and the probability due to late activation, $Q_{barrier}\,(1,2)$ according to Equation 3.

Finally we can now calculate the risk of failure in any vessel due to an ignition in the same vessel or any vessel directly connected, see Table 3.

IMPACT OF CHANGES IN EXPLOSION PROTECTION SYSTEM DESIGN

As we can see from Table 3, the Bag Filter is at greatest risk. This can be attributed to the proximity of $P_{red}\,(3,3)$ to $P_s\,(3)$ and the connection with the Cyclone and Storage Hopper

Table 3. Residual risk of safety system failure for each vertex in the grinding and milling example process

Plant item	Vertex	Risk of failure due to an ignition in the same vessel or any vessel directly connected
Grinder	1	$\zeta_1 = 2.79 \times 10^{-3}$
Cyclone	2	$\zeta_2 = 4.95 \times 10^{-3}$
Bag filter	3	$\zeta_3 = 7.10 \times 10^{-3}$
Storage hopper	4	$\zeta_4 = 5.43 \times 10^{-5}$

†This argument is similar to that presented later, and in more detail, regarding ignition location and isolation barrier placement when using pressure detection, see Figure 3(A)

which are both large vessels‡. Unless we have evidence to suggest that $P_{red}(3,2)$ or $P_{red}(4,2)$ has been overstated, and thus can be reduced, the best option is to change the suppression system design such that $P_{red}(3,3)$ is reduced somewhat. In this case, a simple reduction in the suppression actuation pressure from 100 mbar to 50 mbar is sufficient to reduce $P_{red}(3,3)$ to 0.33 bar and thus reduce ζ_1 to 1.16×10^{-3}. Of course, we must be thoughtful of the impact of any unnecessary or false actuations which may be greater with a reduced actuation pressure on the suppression system fitted to the Bag Filter.

With the risk in the Bag Filter reduced, the Cyclone now becomes greatest at risk with the largest contribution coming from $Q^s(1,2)$. This stems from the fact that the barrier is positioned too close to the Grinder and therefore does not allow enough time to establish the barrier before flame passes the barrier location. For efficacious explosion isolation using this hardware, the barrier must be placed at 8.0 m from the Grinder such that $t_b(1,2) = t_f(1,2)$. However, as shown in Figure 1, the duct-work between the Grinder and the Cyclone is only 5 m long. This represents a very real issue for explosion isolation systems in the practice.

One way to better understand this problem is to calculate the minimum barrier distance, d_{min}, such that $t_b(1,2) = t_f(1,2)$ as a function of ignition location in the source vessel. Figure 2 shows this for pressure, optical and dual (pressure AND optical) detection means to actuate the isolation barrier. With pressure detection, the worst case ignition location is close to the duct mouth, since the flame will have started propagating along the duct before the pressure in the source vessel has increased sufficiently to secure detection. Consequently the largest d_{min} is for ignition close to the duct mouth. For ignition locations far from the duct mouth, the pressure detector will have actuated long before the flame reaches the duct, and as Figure 2 shows, at ignition locations greater than 0.55 m from the duct mouth, the barrier can be place adjacent to the vessel ($d_{min} = 0$).

In our Grinder example with pressure detection, we can use Figure 2 to understand the consequences of barrier placement at 3 m. We see that with ignition locations further than 0.42 m from the duct mouth the calculated barrier distance, d_{min}, is less than our installed location of 3 m and we therefore predict efficacious isolation. However, for ignition locations less than 0.42 m from the duct mouth, d_{min} is greater than 3 m and we would expect flame passage. This ignition distance, $L_{press} = 0.42$ m, allows us to draw a locus and thus define a volume element in which if ignition were to occur the isolation barrier is likely to fail its mission, see Figure 3 (A). The volume of this hemispherical region close to the duct is $0.144\,m^3$ and so constitutes 7.22% of the total vessel volume. Since we assume that all ignition locations are equally probable, this volume element represents the percentage of ignition locations that will allow flame passage and is represented in our residual risk calculation by $Q_{barrier}(1,2)$.

Let us investigate changing the detection means for the isolation barrier to an optical detector located within a few duct diameters of the duct mouth. In this case ignition far from the duct is the most challenging case. Here the flame will be travelling very fast as it

‡The explosion enhancement from flame jet ignition is proportional to the connected vessel volume ratios (V_1/V_2) [Lunn,1996; Holbrow, 1996].

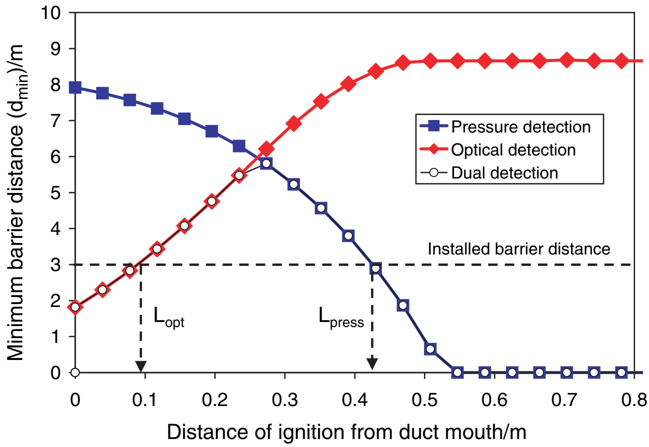

Figure 2. Minimum barrier distance (i.e. $t_b(1,2) = t_f(1,2)$) as a function of distance of ignition location from the duct mouth for pressure, optical and dual (pressure AND optical) detection means to actuate the fast-acting isolation valve. The Grinder has a volume of 2 m^3, with a air velocity through the DN300 duct of 10 m/s. The material has a fuel explosibility rate constant of 150 bar.m/s and the isolation system uses a 50 mbar detection pressure. L_{opt} and L_{press} are indicated for the installed barrier location of 3 m from the Grinder

enters the duct (when it is detected), and therefore requires a large barrier distance in order to establish the barrier. For optical detection, ignition close to the duct is the trivial case since the flame is moving very slowly as it propagates from the ignition kernel and will be detected immediately.

We see from Figure 2 that $L_{opt} = 0.09$ m and this represents a small volume element (1.52×10^{-3} m^3) whereby an ignition occurrence would result in efficacious explosion isolation. As shown schematically in Figure 3 (B), optical detection (in this example) is actually much worse than pressure detection, with 99.92% of ignition locations resulting in the isolation barrier failing its mission.

Employing dual detection takes the strengths of pressure and optical detectors, but avoids their respective weaknesses. This is shown in Figure 2 where at distances close to the duct, optical detection will actuate first, while at distances far from the duct pressure detection will actuate first. Using dual detection and locating the barrier at 5.8 m from the Grinder we would cover all possible ignition locations. However, in our example, we are still outside this design guidance and the resulting volume element in which an ignition would result in flame passage is shown schematically in Figure 3 (C) and is simply the difference in volume elements defined by L_{press} and L_{opt}. In this example, we only reduce the volume element to 7.14%, which is only marginally better than pressure detection alone (7.22%) because of the insignificant volume protected by the optical detector.

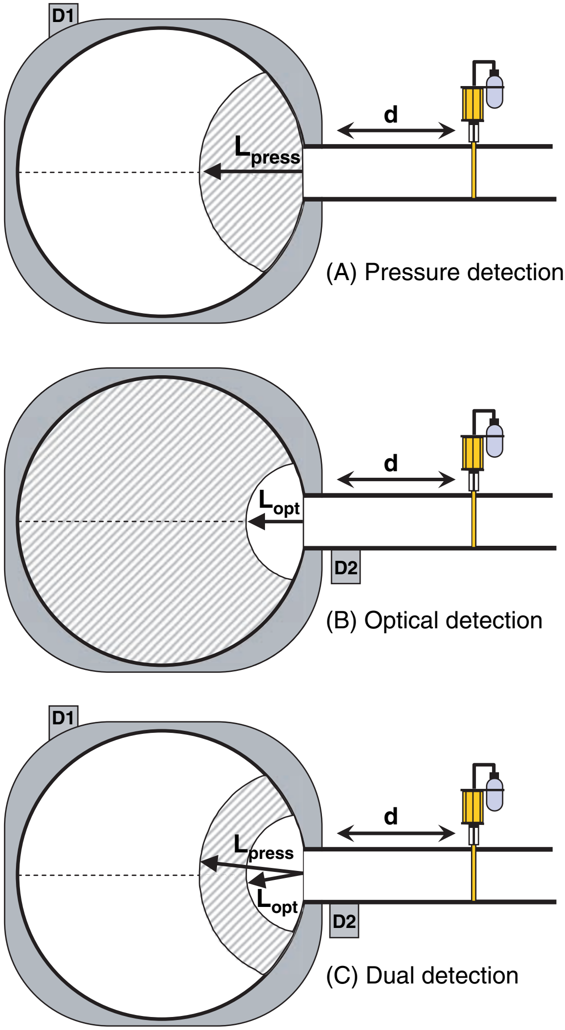

Figure 3. Schematic representation of the volume element (shaded region) in which if ignition occurred the isolation barrier would not prevent flame passage for (A) pressure, (B) optical and (C) dual detection means. L_{press} and L_{opt} represent the radius of the locus at which $t_f(i, j) = t_b(i, j)$ when using pressure or optical detection respectively

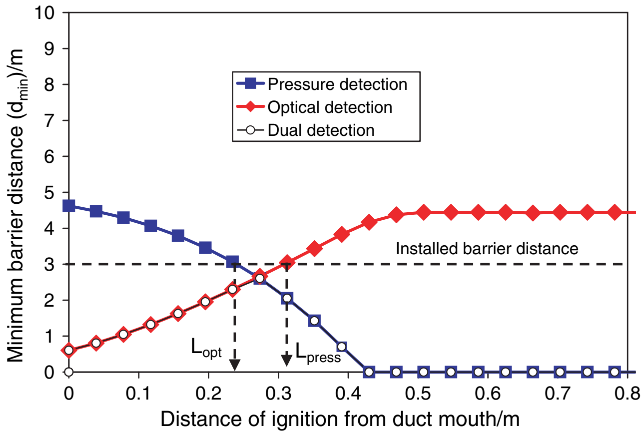

Figure 4. Minimum barrier distance as a function of distance of ignition location from the duct mouth for pressure, optical and dual (pressure AND optical) detection for the Grinder example using a chemically acting isolation barrier

If we were to replace the fast-acting valve with a chemically acting isolation barrier, the latter having a much faster deployment time, we see a marked change in the minimum barrier distances, see Figure 4. When pressure detection is employed, only 1.8% of ignition occurrences will allow flame to pass the barrier, whilst once again optical detection is a poor choice with 96.9% unprotected. However, d_{min} for dual detection is now less than our installed barrier distance meaning that all ignition locations are now protected. Table 4 shows the residual risk for the Cyclone when using a chemical isolation barrier actuated using either pressure or dual detection means.

Supposing that optical detection for the isolation barrier was not acceptable to the plant operator, maybe due to the frequency of the maintenance schedule of such a device in a dirty environment. Instead the probability of flame propagation and its consequence could be addressed to reduce the risk of safety systems failure.

Table 4. Residual risk of safety system failure in the Cyclone using either pressure or dual detection to actuate the chemical isolation barrier between the Grinder and the Cyclone. $t_f(1,2)$ varies for different detection means since the worst case ignition location is used [Moore, 2005]

Detection means	$t_b(1,2)$	$t_f(1,2)$	Risk of failure due to an ignition in the cyclone or any vessel directly connected
Pressure	61	49	$\zeta_2 = 8.25 \times 10^{-4}$
Dual	61	65	$\zeta_2 = 1.14 \times 10^{-4}$

Table 5. Residual risk of safety system failure for each vertex in the grinding and milling example process with explosion suppression fitted to the Grinder and the Cyclone. The tabulated risks are calculated using the changes in safety system design previously discussed, such as the reduced P_{red} (3,3) and a chemical isolation barrier fitted between the Grinder and the Cyclone actuated via pressure detection

Plant item	Vertex	Risk of failure due to an ignition in the same vessel or any vessel directly connected
Grinder	1	$\zeta_1 = 1.95 \times 10^{-4}$
Cyclone	2	$\zeta_2 = 3.93 \times 10^{-5}$
Bag Filter	3	$\zeta_3 = 5.19 \times 10^{-5}$
Storage Hopper	4	$\zeta_4 = 3.91 \times 10^{-5}$

Connected vented vessels (without efficacious explosion isolation) are much more likely to result in a flame transfer which can lead to an enhanced explosion occurrence in V_2. This stems from the fact that explosion venting simply mitigates against the rapid pressure rise and does not tackle the presence of flame which can lead to further ignition events. This is not the case for explosion suppression whereby the flame front itself is extinguished by the rapidly deployed suppressant agent.

In our example, fitting explosion suppression to the Grinder and the Cyclone, in place of explosion venting would significantly reduce the probability of flame transfer between the plant components. Table 5 lists the residual risk for each plant item with both the Grinder and the Cyclone fitted with explosion suppression as described above. In this case the residual risks have now been reduced by an order of magnitude for the Grinder and the Bag Filter, and by two orders of magnitude for the Cyclone.

CONCLUSIONS

- The benefit of using a systematic calculation tool to ascribe the residual risk of explosion safety system failure has been shown by reference to a practical process-industry example.
- By electing appropriate input assumptions and representative data to set out ignition probabilities and consequence of flame transfer, a meaningful measure of residual risk that an installed explosion protection measure will fail to mitigate an explosion incident can be determined.
- A software design support tool is clearly possible from the described calculation means.
- Residual risk determination is critically dependent on the detail of the elected explosion protection system. In this paper we have shown by reference to a practical example that the installation of an explosion isolation means, in this case a fast-acting valve

located at 3 m from the duct mouth rather than the prescribed 5.5 m, has important implications on overall process safety.

- Options to improve the design of explosion isolation include the incorporation of optical detection and electing a faster isolation means, and are shown to represent safety system enhancements for this example. However, the most profound change in the residual risk of failure was demonstrated by electing explosion suppression rather than explosion venting on connected vessels, and thereby significantly reducing the probability of flame transfer.
- We have shown that by determining the residual risk of failure, it is possible to select and quantify the safety integrity of explosion protection options. Through this process design, engineers and operators can make better and informed decisions, leading to enhanced safety integrity and cost effectiveness in delivering overall process safety.

ACKNOWLEDGEMENTS

The authors would like to thank Professor Gautam Mitra and Dr Paresh Date from the *Center for the Analysis of Risk and Optimisation Modelling Applications*, Brunel University for their work in devising the mathematical methodology employed for the computation of residual risk. We also would like to thank Robert Pallant from Kidde Research for his help in data analysis and its interpretation, together with his interest in this work.

NOMENCLATURE

$Q_E(i)$	Ignition probability in vessel i.
$P_{red}(i, j)$	Reduced explosion pressure in vertex i following an ignition in vertex j.
$P_s(i)$	Pressure shock resistance of vertex i.
$Q_{vessel}(i, j)$	Probability that the explosion protection hardware does not fail, but the reduced explosion pressure is still higher than the pressure shock resistance of the vessel
$t_b(i, j)$	Time from ignition for the isolation barrier to be established between vessels i and j
$t_f(i, j)$	Time taken for the flame front to arrive at the barrier location between vessels i and j
$Q_{barrier}(i, j)$	Probability that the isolation hardware is actuated and the barrier established, but the barrier is deployed too late and flame passes from vessel i to j
$Q_f^s(i, j)$	Probability of flame propagation between connected vessels i and j which then leads to an enhanced explosion in j.
$Q^s(i, j)$	Total flame propagation probability from vessel i to j which then leads to an enhanced explosion in j, taking into account any explosion isolation provision

$Q_h(i, j)$	Probability of explosion isolation hardware failure between vessels i and j
$Q_h(i)$	Probability of explosion protection hardware failure on vessel i
ζ_1	Residual risk of failure of vessel i due to an ignition in the same vessel or any vessel directly connected
Φj	The set of vertices adjacent to vertex i.
V_1	Source vessel where ignition occurs
V_2	Vessel connected to V_1
d	Distance of explosion isolation barrier from the source vessel
d_{min}	Minimum barrier distance from the source vessel such that $t_b(i,j) = t_f(i,j)$
L_{press}	radius of the ignition locus at which $t_f(i, j) = t_b(i, j)$ when using pressure detection
L_{opt}	radius of the ignition locus at which $t_f(i, j) = t_b(i, j)$ when using optical detection

REFERENCES

Date, P., Lade, R. J., Moore, P. E., Mitra, G., 2008, Modelling the Residual Risk of Safety System Failure, submitted to Operations Research, INFORMS.

Moore, P. E., Dunster, R. G., 2001, Improved Effectiveness in Explosion Suppression, VDI Berichte

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 12th International Symposium on Loss Prevention and Safety Promotion in the Process Industries'

Gexcon, 2005, FLACS: (FLame ACceleration Simulator), Gexcon AS, Bergen, Norway.

Holbrow, P., Andrews, S., Lunn, G. A., 1996, Dust Explosions in Interconnected Vented Vessels, J Loss Prevention Process Industries, 9(1): 91-103.

Jeske, A., Beck, H., 1997, Dokumentation Staubexplosionen, Analyse und Einzelfalldarstellung, BIA –Report NR. 4/82

Lunn, G. A., Holbrow, P., Andrews, S., Gummer, J., 1996, Dust Explosions in Totally Enclosed Interconnected Vessel Systems, J Loss Prevention Process Industries, 9(1): 45-58.

Moore, P., E., Spring, D., J., 2005, Design of Explosion Isolation Barriers, Trans IChemE, Part B, Process Safety and Environmental Protection, 83(B2): 161-170

Siwek, R., Cesana, C., 2001. Software for Explosion Protection, WinVent and ExTools, Safe Handling of Combustible Dusts, VDI Bewrichte 1601, Nuremberg

West, D., 2001, Introduction to Graph Theory, Prentice Hall.