Incitec Pivot Limited
INNOVATION ON THE GROUND

Risk Evaluation & Risk Treatment for Explosives Manufacturing

September 29, 2022

Incitec Pivot Limited
ABN 42 004 080 264
Level 8, 28 Freshwater Place
Southbank Victoria 3006
Australia

Introduction

Two foundational principles of explosives risk management are the minimization of explosive quantities and the minimization of human exposure to overpressure, fragments and thermal effects. Whether by means of detailed consequence modelling or using standard quantity-distance tables, it is straightforward to utilize these principles for the siting of explosives storage and manufacturing facilities and for determining the location of buildings occupied by personnel. However, when the focus is shifted to the manufacture of explosives at a given Potential Explosion Site (PES), one is confronted with the reality that Operators and Maintainers are often required to handle and work in close proximity to explosive materials and devices as well as manufacturing equipment. Although the principles of quantity and exposure minimization also hold true at this micro level, additional risk analysis and mindfulness are required to ensure that the potential fatality risk is managed to an acceptable level.

Risk Acceptance Criteria

The question "*What is an acceptable level of fatality risk?*" is somewhat subjective, depending on company and external expectations. However, knowing the target is critical to our ability to effectively manage explosives risk. When I started my career in the explosives manufacturing industry, a popular school of thought was to advocate a fatality risk target of $1x10^{-6}$ per shift. This target corresponds loosely to the probability of a fatal accident while commuting to and from work, the objective being to make sure that the risk to personnel while at work is not greater than their risk exposure while traveling to and from work. It has since become more and more common for fatality risk criteria to be specified within the corporate risk framework, underpinned by relevant societal and jurisdictional expectations.

A 2016 study of risk tolerability criteria[1] provides insights into individual fatality risk targets across various jurisdictions. One example cited is taken from the United States Department of Defense where $1x10^{-4}$ fatalities per year is defined as the upper tolerability limit for fatality risk to workers involved in the handling of explosives. In general, the authors found fatality risk targets for individual workers to range between $1x10^{-4}$ and $1x10^{-6}$ per year. Whatever the individual worker target may be, a fit-for-purpose risk management process is required to document and demonstrate proof of safety to workers, business leaders and regulators.

---

[1] An Overview of Worldwide Risk Tolerability Criteria for Chemical Process Industries, 19th Annual International Symposium, Mary Kay O'Connor Process Safety Center

Process Safety Information

Effective risk management is predicated upon a foundation of accurate, relevant and documented explosives safety information. Before one can conduct a robust analysis of explosive manufacturing hazards and risks, there must be a fundamental understanding of the following:

1) Information on explosive materials
2) Information on process technology
3) Information on process equipment

Accurate, relevant and documented explosives safety information informs the Basis of Safety and underpins all risk management and risk treatment activities. This information also plays an important role in the investigation of incidents and in the management of change over time. Without this information, it is impossible to demonstrate diligence in understanding hazards and implementing the controls that keep people safe.

Information on explosive materials

Relying solely on the information typically presented in a Safety Data Sheet is not sufficient. The ability to effectively analyze the potential for an explosives event (including the necessary controls) requires documented and detailed understanding of the explosive material characterization. Material characterization includes explosive classification, TNT equivalency, incompatibilities and minimum initiation energies from friction, impact, ESD and heat stimuli. It is also important to understand the importance of desensitization for handling (e.g., humidity controls, water content, etc.). Probit data providing experimental initiation probabilities can also be very useful for quantitative or semi-quantitative analysis, facilitating a data-based assessment of the likelihood of initiation for a range of energy inputs.

Information on process technology

In a recent guideline on process safety management for explosives manufacturing[2], the U.S. OSHA identified the following process technology information as essential:

- Bock flow or process flow diagrams
- Process chemistry
- Maximum intended inventory for each operation

---

[2] Process Safety Management for Explosives and Pyrotechnics Manufacturing, OSHA 3912-03 2017

- Safe upper and lower process limits (e.g., temperature, pressure, flow or composition)
- An evaluation of the consequences of deviations, including those affecting the safety and health of employees that could occur if operating beyond the established process limits

Information on process equipment

Current as-built engineering drawings, equipment specifications, control system descriptions, materials of construction, dimensional tolerances, and potential for confinement should be thoroughly documented. Similarly, blast protection and fragment protection structure designs should be documented with supporting calculations. Potential sources of energy within the process should also be identified and documented.

For explosive materials that demonstrate a propensity to transition from deflagration to detonation, full scale testing of mocked-up process equipment may help to assess detonation likelihood based on in-process configuration and confinement.

Managing Risks

The management of risks can be broken into two key activities: 1) Process Hazard Analysis and 2) Risk Treatment. Process Hazard Analysis involves application of a systematic methodology to identify explosion hazards and analyze the potential causes, consequences and safeguards associated with explosion events. Risk Treatment, on the other hand, considers the current risk rating and control effectiveness to select and implement options for addressing risk (i.e., lowering the current risk to a tolerable level).

Process Hazard Analysis

The primary purpose of process hazard analysis is to understand all relevant causes for a given explosion event and identify the preventative and mitigative controls in place to arrest its progression to a fatal outcome. This analysis is used to characterize the risk of the event in terms of its maximum credible consequence and corresponding likelihood. Accordingly, the primary output of the process hazard analysis is the identification of those controls that have the largest impact on reducing the consequence or likelihood. These controls are referred to as critical controls and ideally possess the attributes of effectiveness, independence and auditability.

Too often process hazard analysis is thought of in terms of a single risk analysis method, when in fact, the analysis of explosion hazards requires a combination of several complementary methodologies which are summarized below. With the benefit of accurate process safety information, these methodologies should be combined to provide a collective view of risk to personnel. The aim is to eliminate or establish positive control of ignition sources and ignition stimuli and provide protection to personnel from blast, fragments, and thermal effects, including respiratory and circulatory hazards[3].

Consequence Modelling

Fit-for-purpose consequence models are used to understand potential blast pressure, fragment and thermal impacts and the corresponding vulnerabilities to affected personnel and structures.

Qualitative Risk Analysis

Common qualitative risk assessment methodologies include: Failure Modes and Effects Analysis (FMEA), HAZARD and Operability Study (HAZOP), Bow Tie Analysis and What-If Analysis. The appropriateness of each method depends on the nature of the explosive manufacturing process or operation. Irrespective of the methodology, the desired output is the same – to qualitatively analyse and demonstrate the causal and control relationships for explosive manufacturing risks. The key output of the qualitative risk assessment is the identification of all potential causes and the corresponding critical controls. There is a significant danger of missing key causal pathways and the associated controls if the qualitative analysis is conducted as a mere paper or desktop exercise without first performing in-field observations and demanding the needed focus on the Basis of Safety.

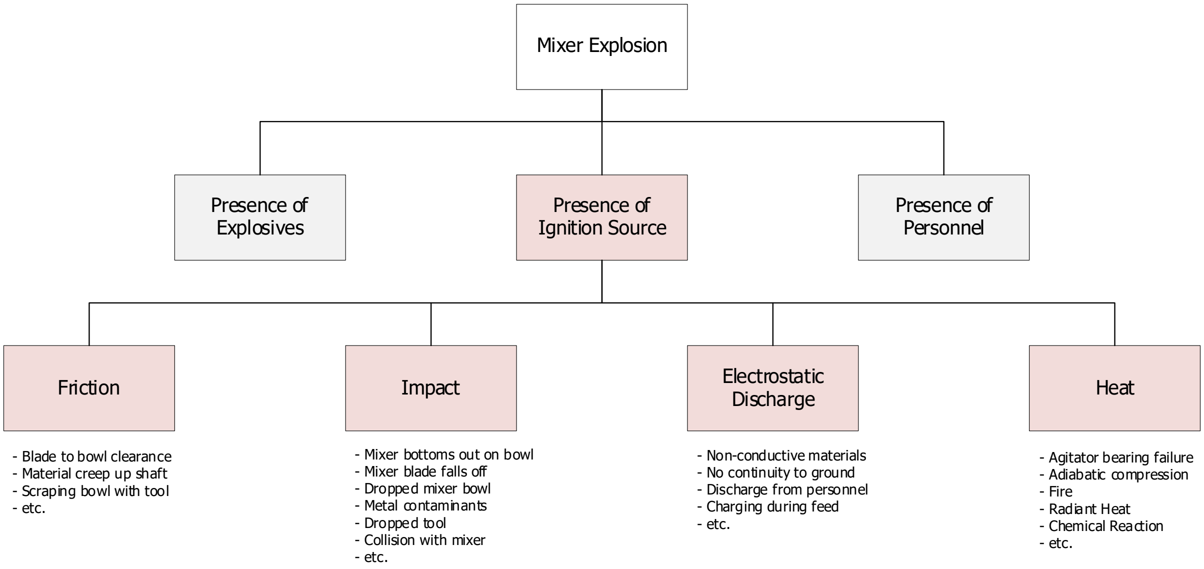
Logic Diagram

The creation of a logic diagram in advance of the qualitative risk analysis can help to ensure all aspects of the Basis of Safety are considered in the analysis. The logic diagram is constructed as a simple fault tree (without the logic gates) to identify beforehand all potential sources of initiation. As with the qualitative risk analysis, the logic diagram must not be created as a desktop exercise without having a skilled hazards analyst go and see the manufacturing operation and make critical observations and assessments in the field. The logic diagram becomes an essential checklist for the qualitative risk analysis facilitator to ensure that no causal pathways are missed, irrespective of the qualitative analysis methodology employed. An example logic diagram is presented in Figure 1.

---

[3] Department of Defense Manual, NUMBER 6055.09-M, Volume 1

Figure 1 – Example Logic Diagram



Illustrative Example prepared by A.G. Walker for SAFEX XX

Quantitative Risk Assessment

The use of quantitative or semi-quantitative tools for explosives manufacturing scenarios can provide a more detailed understanding of the risk scenario, highlighting specific gaps in the preventative and mitigative controls and informing the appropriate risk treatment options. Layer of Protection Analysis (LOPA) is the preferred semi-quantitative method for much of the processing industry; however, LOPA may not be appropriate for many explosives manufacturing operations. Specifically, LOPA is not considered suitable for scenarios that have a high reliance on administrative controls and human intervention. In these cases, Fault Tree Analysis or Event Tree Analysis should be considered.

Within the context of a Fault Tree or Event Tree analysis, human error probability and probit data can be combined to provide an informed estimate of the likelihood of an explosive event. For example, a risk scenario is identified during normal handling where a worker accidentally drops a container of impact-sensitive explosive material. To estimate the probability of an explosion, two important pieces of information are required: 1) what is the probability of the worker dropping the container? and 2) what is the likelihood that the explosive contents of the container will detonate due to a drop from normal working height? Human error rate data can provide a reasonable likelihood of dropping the container, whereas probit data can provide the probability of initiation.

Risk Treatment

The first step of Risk Treatment is an evaluation of the current risk which involves comparing the results of the Process Hazard Analysis with the established risk criteria to determine whether additional action is required. In practical terms, the first source of reference for fatality risk acceptance criteria should be the enterprise risk appetite statement and/or qualitative risk matrix. The qualitative risk matrix depicted in Figure 2 is an important risk decision making tool that articulates the upper and lower limits of tolerability based on qualitative descriptors of consequence and likelihood. The risk matrix consequence scale is typically straightforward to navigate, with the likelihood scale defining the upper and lower limits of tolerability for a given consequence.

Figure 2 - Generic Risk Matrix

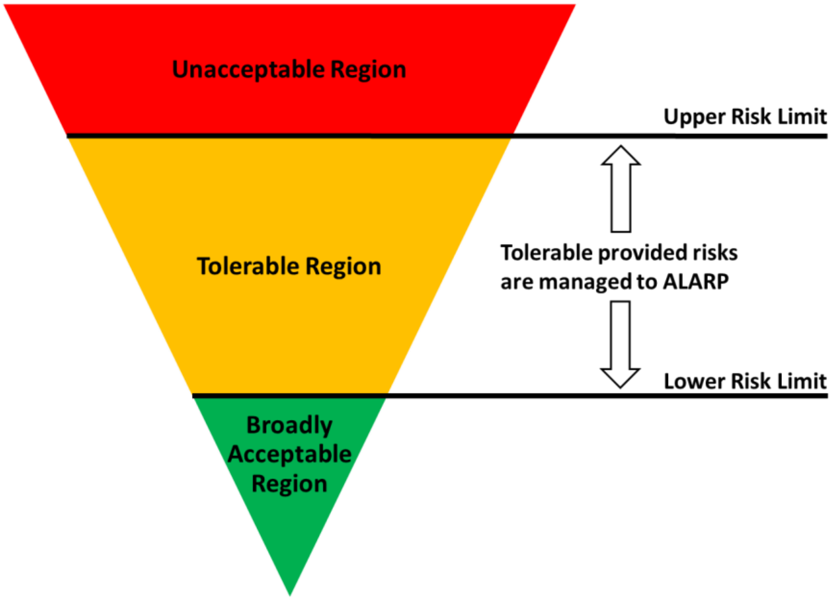
	Consequence				
Likelihood	Minor	Medium	Serious	Major	Catastrophic
Almost Certain	Moderate	High	Critical	Critical	Critical
Likely	Moderate	High	High	Critical	Critical
Possible	Low	Moderate	High	Critical	Critical
Unlikely	Low	Low	Moderate	High	Critical
Rare	Low	Low	Moderate	High	High

Illustrative Example prepared by A.G. Walker for SAFEX XX

Some risk matrices do not delineate between unacceptable and acceptable risks for potentially fatal consequences (i.e., the likelihood descriptors do not go low enough to adequately represent the low probabilities associated with explosives safety events). Where this is the case, specific quantitative fatality risk criteria are helpful for risk decision making and should be stated elsewhere within the risk management framework (e.g., as part of a risk appetite statement). The corporate risk documents should clearly define the upper and lower limits of tolerability for fatality risk in alignment with expectations from the authorities having jurisdiction.

The risk reduction spectrum is depicted in Figure 3. Based on the evaluation of risk, potential risk reduction measures are identified and prioritized to move the risk towards the risk target which is typically defined by the lower limit of tolerability. Individual fatality risk that exceeds the upper limit of tolerability is considered unacceptable. Conversely, individual fatality risk that is below the lower limit of tolerability is considered broadly acceptable. The area between the upper and lower limits is referred to as the ALARP (As Low As Reasonably Practicable) region where a risk is considered tolerable provided compliance with good practice as well as relevant condes and standards is demonstrated; and it can be demonstrated that the cost of any further risk reduction actions is grossly disproportionate to the risk benefit gained.

Figure 3 – Risk Reduction Spectrum



Adapted from Safe Work Australia Guide for Major Hazard Facilities[4]

To the extent possible, risk treatment and the associated risk reduction measures should be focused on developing critical controls that are: 1) effective under the full range of conditions, 2) independent of the cause and initiating event, and auditable.

Critical Control Management

Critical control management is a formal process of managing explosives safety risk that involves a systematic approach to ensure critical controls are in place and effective.

Many incidents occur not because of failure to recognize the hazards and risks, rather because critical controls have been allowed to deteriorate and degrade over time. Trevor Kletz[5] was well known for his statement that "*organizations have no memory*". He continues this thought

---

[4] Safety Case: Demonstrating the Adequacy of Safety Management and Control Measures

[5] Trevor Kletz, Lessons From Disaster: How Organizations Have No Memory and Accidents Recur

by saying that "*only people have memories, and they move on*". My experience over many years supports Mr. Kletz's statement - the memory of a critical control and its purpose can be erased from an organization's memory over time. This should be particularly troubling when we consider that many explosives manufacturing processes are legacy processes that have existed for generations. How much knowledge has been potentially lost or distorted over time with respect to critical controls?

To counter this tendency, critical controls must be thoroughly documented in management systems. A critical control management plan should be developed for each critical control identified as part of the hazard analysis and risk treatment processes. The critical control management plan documents the key function of the control, and specifies the performance, inspection, testing and preventive maintenance requirements necessary to ensure the control provides the desired protection.

To properly manage critical controls, they must be visible through monitoring and reporting and confirmed through ongoing verification as being present and effective. This holds true for engineering as well as administrative critical controls.

The following three examples from my previous experience across the industry highlight the importance of critical control management plans, reporting and verification:

1) The first case deals with a manufacturing process designed to compress a pyrotechnic powder into a disk form by means of a rotary press. The finished product exits the press on a small, narrow conveyor designed to deliver the disks (one by one) through a substantial concrete blast wall into an occupied packaging bay.

   The risk of ignition at the press and subsequent propagation into the packaging bay was identified through the design and hazard analysis processes. A critical control was implemented that would stop the conveyor and close a gate at the blast wall - automatically upon sensing flame in the press bay or manually by activation of an emergency shutdown from the control room. Based on the conveyor speed and spacing between disks, this critical control was deemed effective at preventing propagation into the packaging bay.

   A deflagration event occurred on the rotary press. Alert Operators immediately activated the emergency shutdown but were surprised as camera footage showed burning disks passing through the blast wall into the packaging bay. Fortunately, a major event in the packaging bay was averted, but subsequent investigation revealed that the critical control had been bridged or bypassed in the field defeating the designed protections. In this case the critical control (as designed) was effective but had not been verified as being in place at the time of the event.

2) In the second case, a conveyance mechanism was designed to transfer an explosive material with high sensitivity to electro-static initiation. Because of the ESD ignition sensitivity, great care was taken to ensure that all components of the conveyance mechanism, including an elastomeric belt, were constructed of conductive materials.

The newly installed equipment was confirmed to have acceptable resistance to earth readings. However, the effectiveness of this design was challenged when, after a brief period of operation, the conductive surfaces of the elastomeric belt were found to have accumulated a non-conductive film due to wear. In other words, normal process wear rendered the critical control ineffective with respect to its intended use.

3) The third case is somewhat unique as compared to the examples above from the explosives manufacturing industry, but illustrative of a critical control that is neither effective nor in-place. Some former colleagues in the industry had been assigned to review a demilitarization process in a remote corner of the world. They returned from their assignment commenting on a "critical control" they had observed as part of a process designed to remove TNT from old munitions. The critical control in question was a deluge system that consisted of a large water-filled bucket suspended by a fiber rope above the process area. The intent was noble – an event in the process would consume the rope allowing the contents of the bucket to fall over the process equipment. Intrigued, my colleagues were compelled to examine the bucket only to find that the bucket was empty.

Risk treatment requires the specification of critical controls that are effective in providing the desired protection. However, the effectiveness of a critical control on paper is not enough. Even the best designed critical controls are susceptible to degradation over time. A robust critical control management process is vital in ensuring the proper installation and in verifying the ongoing effectiveness of critical controls.

The Role of Mindfulness

From my experience across multiple industries, it is common during the facilitation of hazard analysis workshops to hear the following type of statement raised emphatically by at least one of the attendees:

> *"I have worked here for more than thirty years, and I have never seen that happen."*

Thirty years is but a brief moment in the probability lifetime of a given risk event, but because an individual has not experienced it within the history framed by their work experience, they have effectively dismissed in their minds the possibility of it ever occurring. Hence, we find some that will say "It cannot happen here". This belief may be a manifestation of potential weakness in a risk management culture requiring focused intervention. Professor Andrew Hopkins[6] outlines the principles of mindful leadership to help counterbalance the belief that "*It cannot happen here*."

---

[6] Andrew Hopkins, Failure to Learn

According to Hopkins, mindful leaders exhibit the following characteristics:

- ✓ **Pre-occupied** with the possibility of something going wrong
- ✓ **Hunt** for latent problems utilizing audit processes
- ✓ **Go** and find out for themselves because they know bad news does not travel upwards
- ✓ **Welcome** bad news

Being a mindful leader is a purposeful action-oriented proposition. The transformative benefit of mindful leadership lies not only in detecting early warning signs before a major accident, but also in promoting a healthy respect among the workforce for the risks associated with the explosives manufactured and handled. In other words, the focus and priorities of a mindful leader will trickle down to the workforce as a matter of importance.

An effective method for cultivating a culture of mindfulness is to tell our stories of past incidents. When I first joined the explosives industry as a new University graduate, I vividly recall our new hire orientation when we were escorted to a site where at one time a nitroglycerine manufacturing operation had existed. As a handful of new hires huddled around, a seasoned employee proceeded to tell the story of a terrible explosion that had leveled the facility right where we were standing. He then described the investigation process in which he and others walked arm-to-arm across the brush-covered hillside looking for any remnants of those who had perished in the explosion. This story captured my attention forty years ago and it has stayed with me throughout my entire career. If we fail to tell our own stories, we are missing a tremendous opportunity to keep alive, in a very personal way, those lessons from the past that have been learned at such great cost.

Conclusion

A fatal explosion is the worst failure an organization can experience. Conversely, the effective management of this risk is one of the most rewarding accomplishments. Achievement of this objective requires effort…effort to understand and formally document the energetic properties and characteristics of explosive materials and devices, effort to understand the equipment used in the manufacturing and handling of explosives, and effort to systematically analyse the hazards and identify the critical controls relied upon to achieve a tolerable likelihood. However, all this underpinning knowledge will be for naught if the collective sensitivity to the risk or the critical controls are allowed to deteriorate over time through an absence of mindfulness.