Process Safety and Environmental Protection 90 (2012) 389–403

Contents lists available at SciVerse ScienceDirect

Process Safety and Environmental Protection

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

Developments in inherent safety: A review of the progress during 2001–2011 and opportunities ahead

Rajagopalan Srinivasan[a,b,*], *Sathish Natarajan*[a]

[a] *Department of Chemical and Biomolecular Engg, National University of Singapore, 10 Kent Ridge Crescent, Singapore, 119260, Singapore*

[b] *Process Sciences and Modeling, Institute of Chemical and Engineering Science, 1 Pesek Road, Jurong Island, Singapore, 62783, Singapore*

ABSTRACT

This paper reviews the progress in inherent safety. A summary of the historical developments up to the year 2000 is first presented which sets the stage for a review of the key developments during the first 11 years of the 21st century. A landscape of inherent safety is developed by mapping publications on two coordinates. The first coordinate, the risk coordinate, indicates if the focus of a paper relates to inherent hazard or to the likelihood of events. The second coordinate, the management coordinate, focuses on the ways and means to understand and assess inherent safety. Out of the 187 papers that have appeared over this 11-year period, 131 pertained to developments in inherently safer design; these have been organized on the proposed landscape. The rest introduce the basic concepts of inherent safety and address its incorporation into regulation, education and accident investigation. These along with the application of inherent safety in industry are also discussed. We conclude with a discussion on recent trends in industry and suggest directions for future research.

Keywords: Principles; Metrics; Risk management; Human factors; Education; Sustainability

1. Introduction

"What you don't have can't leak", said Trevor Kletz (Kletz, 1978) and laid the foundation of a new approach for risk management in chemical processes. Since then, the concept called inherent safety has been the subject of much attention, with an explosion of ideas, methods, and examples as described in several books and publications (Bollinger and Crowl, 1996; CCPS, 2009; Kletz, 1998). It is now also incorporated into safety regulations (McKeon-Slattery, 2010; Sawyer, 2010). The key principles of inherent safety are now well described. This paper seeks to review the major developments over the last 11 years and suggest some topics requiring further attention. This review of inherent safety is organized around process risk management. The risks involved in chemical processes are discussed next. The evolution of inherent safety in the 20th century is summarized in Section 2. Next, in Section 3 we describe a risk management based framework for analyzing inherent safety. We use this framework for reviewing the inherent safety literature over the first 11 years of the 21st century. We conclude with a discussion of recent trends and suggest directions for future research.

1.1. *Risks in chemical processes*

Any accident in a chemical process is a product of three factors – an inherent *hazard* in the technology for converting raw materials to products, one or more *events* that instantiate a failure mode which leads to the *undesired outcome*. A *hazard* is a condition or practice that has the potential to cause harm, including human injury, damage to property, damage to the environment, or some combination of these (Sutton, 2010). The keyword in the definition is 'potential'. Hazards exist in all human activities but rarely result in an incident. An *event* defined as any occurrence in the process, such as an error, caused by equipment performance or human action or an occurrence external to the process (e.g. tsunami, earthquake, etc.) is necessary to translate a hazard into an

* *Corresponding author at*: Department of Chemical and Biomolecular Engg, National University of Singapore, 10 Kent Ridge Crescent, Singapore, 119260, Singapore. Tel.: +65 65168041.

E-mail address: chergs@nus.edu.sg (R. Srinivasan).

Received 12 March 2012; Received in revised form 15 May 2012; Accepted 14 June 2012

0957-5820/$ – see front matter

http://dx.doi.org/10.1016/j.psep.2012.06.001

accident. The first event in an accident sequence is called the initiating event. Examples include equipment or software failures, human errors, etc. A series of events link an initiating event to the outcome. These *intermediate events* could be responses from engineered safety features and administrative controls to an initiating event or knock on effects such as secondary explosions. It is important to view an accident as a discrete sequence of events because each individual event represents an opportunity to terminate the accident sequence. The *likelihood* of each event is a measure of the probability or frequency of its occurrence. The *undesired outcome* is an uncontrolled release of material or energy that results in damage to humans, the plant and the environment. Fire, explosion, and release of toxic chemicals are common examples of outcomes in the refining and petrochemical industries (Marsh, 2001).

Consider the accident in the BP Texas City refinery (CSB, 2007). The outcome of the accident were two explosions that resulted in 15 deaths, injury to 180 others, and losses of about $1.5 billion. The *hazard* in this case was the presence of a large amount of flammable material in the isomerization tower. During startup, operations personnel pumped flammable liquid hydrocarbon into the isomerization tower for over 3 h without removing any liquid out. This is the *initiating event* in this accident. Critical alarms and control instrumentation failed to alert the operator of the high level in the tower. Consequently, unknown to the operators liquid overflowed from the top of tower and formed a flammable vapor cloud. The failure of the instruments and mistakes from operators were the *intermediate events* in this accident. The flammable vapor cloud was ignited by backfire from an idling truck that resulted in two explosions.

Risk management is the term given to the collective efforts to manage risks in order to prevent accidents. Risk is defined formally as the probability that an exposure to a hazard would lead to an undesired outcome. Risk management involves a variety of techniques to (a) minimize the hazards, (b) decrease the likelihood of events, and (c) minimize the severity of the undesired outcome. Hazards can be eliminated or minimized by choosing less hazardous materials, benign reaction chemistry and forgiving process design. The likelihood of an event can be decreased by providing layers of protection using safety devices or work processes. The severity of the outcome can be minimized using operating procedures, training, emergency response, etc.

Different risk management strategies are suitable in different stages of the plant lifecycle. The lifecycle of a chemical plant can be divided into the following stages (CCPS, 2009): research, process development, detailed design, operations, maintenance and modifications and finally decommissioning. During the research stage, process chemists choose the raw materials, intermediates, synthesis routes and specify the basic operating parameters for producing the product. In the process development stage, process engineers use the information provided by chemists to design unit operations in which necessary chemical transformations are realized. The process flowsheet is also developed at this stage. During the detailed design stage, process engineers develop P&IDs, layout of the plant and specify the operating procedures to be followed for startup, shutdown, etc. Meanwhile, control engineers design the control system along with suitable safety instrumented systems (SIS). In the operations stage, the operating procedures are created or updated based on experience and retrofits to the plant.

Until the mid-20th century, risk management in chemical plants was performed only after the detailed design of the plant had been established, by which time it is too late to make changes to the process technology (materials, reactions, unit operations, etc.), the key determinants of overall risk. Moreover, risk management primarily focused on reducing the likelihood of events by providing layers of protection.

2. The early years of inherent safety: principles and metrics

On December 14, 1977, inspired by the Flixborough disaster, Dr. Trevor Kletz, presented the Annual Jubilee Lecture to the Society of Chemical Industry in Widnes, England. His lecture titled "What You Don't Have, Can't Leak" was the first clear and concise discussion of the concept of inherently safer design in chemical processes. Kletz proposed to change or alter the process to either eliminate the hazard completely or sufficiently reduce its magnitude or likelihood of occurrence, rather than controlling them. He argued that the greatest potential opportunities for impacting the risk profile occur early during process design as there is a great deal of freedom in the selection of chemistry, solvents, raw materials, intermediates, unit operations, plant location and process parameters.

For instance, during the research stage significant reduction in risk can be achieved using benign raw materials and reaction chemistry, thereby eliminating hazards inherent in the process. Risk reduction during the process development stage can be achieved by using forgiving or robust unit operations. In the detailed design stage, opportunities to eliminate the hazards are minimal. But likelihood of events can be minimized using layers of protection. Risk reduction during the operation stage can be achieved using administrative controls, emergency planning, evacuation procedures, etc. to reduce the severity of an undesired outcome. The effectiveness of the various risk reduction strategies in the different stages of the process is shown in Fig. 1. Kletz enumerated certain principles that can be followed to design inherently safer processes, key among which are *minimize*, *substitute*, *moderate* and *simplify* (Kletz, 1985).

Minimize, also called intensification, means to reduce the quantity of material or energy contained in a manufacturing process or plant. *Substitute*, as the name implies, means to replace a hazardous material or process with an alternative that eliminate or reduces the hazard. Examples include solvents, materials of construction and heat transfer media. *Moderate*, also called attenuate, means using materials under less hazardous conditions. Moderation of conditions can be accomplished by strategies that are either physical (i.e., lower temperatures) or chemical (i.e., development of a reaction chemistry which operates at less severe conditions). *Simplify*, as the word suggests, is to design the process to eliminate unnecessary complexity making it robust and forgiving, thereby reducing the opportunities for error and wrong operation. While the above four strategies are the major ones, others such as *Limitation of effects*, *Avoiding incorrect assembly* and *Making status clear* were also proposed (Kletz, 1998). It is often argued that these are sub-categories of the main principles described above.

Application of inherent safety principles helps generate modified process designs. However, design modifications rarely result in a monotonic reduction of risk. Design options with alternate chemistries, materials and unit operations will