Journal of Loss Prevention in the Process Industries 26 (2013) 821–829

Contents lists available at SciVerse ScienceDirect

Journal of Loss Prevention in the Process Industries

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

The safety barometer
How safe is my plant today? Is instantaneously measuring safety level utopia or realizable?

Bert Knegtering [a], Hans Pasman [b,*]

[a] Honeywell Safety Solutions, Rietveldenweg 32a, 's Hertogenbosch, The Netherlands
[b] Mary Kay O'Connor Process Safety Center, Texas A&M University, College Station, TX 88843-3122, USA

ARTICLE INFO

Article history:
Received 5 May 2012
Received in revised form
15 February 2013
Accepted 22 February 2013

Keywords:
Process safety
Risk factors
Safety metrics
Bow-tie model
Alarm management

ABSTRACT

During the last decade, serious accidents have continued to occur in the process industry. Apparently the scenarios of various undesired events leading to those accidents are still not sufficiently controlled. The key question is how potentially hazardous situations develop, what processes form the basis for this development, and how to control them? Safety level is not static but depends on many risk factors that change in presence and intensity over location and time. Safety level is dependent not only on technical process parameters that have immediate effects on the 'frequency' or probability of catastrophic consequences, but also depends on equipment integrity degradation, operational and management quality, attitudes, and cultural processes which may change over a prolonged time. The time and human interaction aspects make dynamic risk assessment complex. This paper will outline a conceptual approach using in addition to the regular process parameter signals received, also weak and slowly changing signals from various safety indicators, enabling to keep track of the risk factors. In theory this could lead to obtaining an instantaneous safety level 'measure' making possible forecast alarming for an imminent event to occur. Such concept could be regarded as a 'writing' safety barometer, or barograph. However, there are quite a number of problems to be solved which in the paper will be discussed.

1. Introduction

1.1. Major accident trend in the process industry

Serious large accidents continue to occur in the process industry. Table 1 gives an overview of known major accidents from 2005 through 2010. The situation is still of concern as expressed, e.g., by Jordan Barab, the Deputy Assistant Secretary of Labor for OSHA, in his speech to the National Petrochemical & Refiners Association (NPRA), May 2010, in which he mentioned the deaths of 58 workers in the American petrochemical industry in 3 months' time (Barab, 2010). As such, somehow the process industry is still not able to control safety sufficiently. Why is safety still not under control? The presupposition is that somehow certain aspects, indicators, factors, etc. are not well observed, measured, analyzed, and controlled. This was one of the findings during the BP Texas City blast investigation (CSB, 2007).

Over the last decades, much has been learned with respect to process safety incidents. As a result, working knowledge about the behavior and characteristics of hazardous substances has accumulated. Consequently, a suite of methods and tools have been developed to structurally and systematically identify potential hazardous situations involving dangerous substances, such as Hazard Identification (HAZID), Hazard and Operability studies (HazOp), Failure Mode and Effect Analysis (FMEA), and Structured What-If Technique (SWIFT) (Kletz, 1994; Lees, 1996). These methods assist much in developing credible failure scenarios. Accordingly, various prevention and protection measures have been developed to reduce the likelihood that something will go wrong with all related unwanted consequences.

In the late 80's, Reason (1990) developed what became known, after several further developments, as the Swiss Cheese Model. For an accident to happen, direct causes can be identified but also underlying ones, amongst which are unsafe acts of the frontline operator, while even more hidden are so called latent or indirect causes such as management and designer decisions, which contribute to the course of events. Accident investigators search for the root causes that are related to these latent causes.

* Corresponding author.
E-mail address: hjpasman@gmail.com (H. Pasman).

0950-4230/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jlp.2013.02.012

Table 1
Overview of some major accidents in the process industry since 2005.

Major accidents 2005–2010
• BP Texas City refinery, Texas, USA, March 2005
• Buncefield, Hemel-Hempstead UK, December 2005
• Puerto Rico, October 2009
◦ Cataño oil refinery explosion and fire, three injured, no deaths
• Sitapura, Jaipur, India, October 2009
◦ Indian Oil, refinery terminal fire five deaths, 150 injured
• Deepwater Horizon offshore platform, Gulf of Mexico, April 2010
• San Bruno, California, USA, September 2010
◦ 30 inch diameter steel natural gas pipeline exploded, eight deaths

Recently, Leveson (2011) in various publications summarized in her book, approached safety from a system control point of view. Safety can be seen as an emergent system property. Emergent properties are controlled by imposing constraints on the behavior and interactions of the system's components. Safety control structures are hierarchical. Accidents result from inadequate controls, technical or social. Causation is therefore asking why controls fail. Time lags play an important role in this failure. In view of systemic failures observed in the process industry and the complex way accidents develop, Venkatasubramanian (2011) emphasized the importance of a system approach and advises to develop a prognostic way of anticipating problems by monitoring weak signals and a real time intelligent decision support system. In this paper we shall discuss a possible direction for realizing this and difficulties involved.

1.2. Consequences of two major accidents compared

The explosions and fires at the BP refinery in Texas City U.S. (CSB, 2007) as well as those at the Buncefield oil depot in Hemel-Hempstead near London, U.K. (Buncefield Major Incident Investigation Board, 2008) have been abundantly investigated and described in many reports, journal papers, and articles in magazines. As such, no extensive description of what exactly happened will be given in this paper. Only one striking aspect will be highlighted. This aspect concerns a comparison of the safety situation on both sites and a comparison of the actual risk levels.

A similarity at both sites was an overfilling resulted in a flammable vapor cloud that was subsequently ignited, transitioning to an explosion, blast wave, and fire. The conclusion is that at both sites the safety level was unacceptably low, because on both sites the hazardous event did occur (it was *a posteriori* not safe at that moment). However, from a human consequence point of view, the difference was enormous. At the refinery in Texas City, 15 people were killed and more than 170 injured, while at Buncefield there were only two injuries despite the much stronger blast of the vapor cloud explosion. This less severe consequence with respect to human loss was because it happened on a Sunday morning. Had the Buncefield accident occurred during regular office hours, many people probably would have been injured or killed. Regarding BP Texas City, an opposite situation was applicable, as the trailers in which the contract workers were located were only temporarily in the hazardous area, such that on a different moment the blast probably would not have caused so many fatalities. These examples show clearly the necessity to take account of time and location when determining instantaneous risk.

1.3. The dynamic character of risk levels

Safety can only be measured by identifying and quantifying the risks. Risk is usually expressed as the product of consequence of an event and its probability. Consequence in turn depends on effects generated in the event and the possible presence and vulnerability of exposed 'targets'. The example of the two accidents in the previous section illustrates with regard to exposed people, how dynamically risk levels behave and how they can vary from one moment to another. There are many other parameters, such as changes in activities from normal operation to shutdown, turnaround and startup, repairs, weather conditions, procedural changes, equipment degradation, which have influence on actual risk level. An acceptable safety level is thus not 'guaranteed', because the safety level fluctuates with changing plant activities, conditions, and circumstances. The design of a plant is such that in case of foreseen possible deviations and disturbances from normal safe operation, instrument sensors or human observation should detect something is going in the 'wrong' direction. In most cases, alarms become triggered upon which attempts are made to correct the process or there may follow a trip or a shutdown to transition to a safe state. However, there are unforeseen deviations, possibly not instrumented ones, unnoticed ones because of operator/supervisor distraction, signs not perceived as an alarm because they are indirectly related to safety, changes observed but not acted upon because of other priorities, and errors or violations, such that the level of safety can deteriorate unnoticed.

The foregoing shows that accident causation can consist of a scenario of a complex causal chain of cause–effect pairs in which each effect acts as a cause of a further consequence until the outcome event is reached. Due to the numerous possibilities leading to an event in a plant of average size, a myriad of scenarios is conceivable.

If plant management could envision a risk monitor that would warn when a critical level at some point of time somewhere in the plant is becoming close, what information would be needed to realize that? Hence what method should be developed to provide plant management with more control? In the following conception, a possible route will be indicated to capture the actual safety level by considering the process as a system and applying risk assessment methods to include time dependent effects.

2. How safe is it at this moment? Risk factors

Companies in the process industry often announce near the entrance to their sites the number of accident free working days. Electronic boards at the gates of plants (Fig. 1) indicate the Lost Time Injuries (LTI), which gives information regarding the recent historical absences due to accidents on the site. This kind of information typically falls under the category 'lagging metrics' as described by the Center for Chemical Process Safety, a technical society of the American Institute of Chemical Engineering (AICHE) (CCPS, 2010). However, this information does not imply that safety is 'guaranteed'. Following the Texas City disaster in 2005, much has already been written about the difference between 'personal' safety and 'process' safety. In other words, the potential risk to a person entering a site is not reflected well by this type of indicator.

Consequently, if one does want to know what risk level prevails at the plant site that day, what additional information should be obtained? Below is an analysis of various aspects and intricacies associated with this question.

A relatively unsafe situation at a certain moment in time by a change in risk level leading to an emerging threat to people and assets could arise, for example, if maintenance is behind schedule, when there are over-rides on various safety-related actuators, welding activities on site, leakage problems, the onset of vibrations somewhere, or an adverse wind direction. Roughly, various *risk factors* such as (minor) defects, changing conditions, and changed operational routine can be distinguished into classes with