Process Safety and Environmental Protection 116 (2018) 92–105

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

A Resilience-based Integrated Process Systems Hazard Analysis (RIPSHA) approach: Part I plant system layer

Prerna Jain [a], William J. Rogers [a], Hans J. Pasman [a], Kelly K. Keim [b], M. Sam Mannan [a,*]

[a] Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX 77843-3122, USA

[b] Process Safety Consultant, Spring, TX, USA

ARTICLE INFO

Article history:
Received 2 July 2017
Received in revised form 23 August 2017
Accepted 19 January 2018
Available online 31 January 2018

Keywords:
Resilience
Process safety
Risk management
LNG
Organization
Human
System

ABSTRACT

In recent years, the chemical process industry has witnessed increased process safety management challenges. One of the initial steps in process safety and risk management of any facility is hazard identification and analysis. Two types of factors: 1) technical (*e.g.,* equipment malfunction), and 2) social (*e.g.*, human and organizational factors) are important in analyzing hazards of a socio-technical process system as a whole. With the conventional process hazard analysis (PHA) methods, there is a tendency to overlook the potential impact of socio-technical systems on the health and sustainment of safeguards. This disregard leads to ignoring social factors, such as shift handover communication, downtime, operating and maintenance procedures, and more. This need calls for the development of a holistic and integrated systems framework for hazard analysis. This paper presents a novel hazards analysis approach that incorporates both technical and social factors within a single analysis method called Resilience-based Integrated Process Systems Hazard Analysis (RIPSHA). This approach is based on the following resilience aspects – 'early detection', 'error tolerant design', 'plasticity', and 'recoverability'. This work establishes and presents a worksheet for analysis of hazards within process systems. The paper concludes with an example of a liquefied natural gas (LNG) process system to illustrate the key concepts of this integrated approach.

1. Introduction

In recent years, it has been observed that the increasing development in technology and rising awareness amongst members of the public have led to process safety and risk management challenges. Incidents have continued to occur in the process industry with various underlying causes in spite of the advanced risk management methodologies that have been implemented (Jain et al., 2016). Some of these causes are increased competition and cost pressure, complex technology, energy saving in view of climate change, better process efficiency, and a series of human and organizational changes. Several examples of such changes such as fatigue due to long hours, less competence and more indifference, rapid job rotation, retirement, job insecurity, time pressure, bad maintenance, less inspection by government, *etc.* have been reported in the incident investigation reports. Process hazards are mainly observed to be responsible for consequences such as fire, explosion, or toxic release. It has been observed that a holistic analysis of the entire system that is missing from the current hazard and risk analysis techniques has resulted in a failure to identify the anatomy of incidents that have led to major catastrophes (Rathnayaka et al., 2011b). Some of the remarkable incidents in process and hazardous materials storage industries, such as the Bhopal tragedy (Eckerman, 2005; Khan and Abbasi, 1999; Willey et al., 2007), the Piper Alpha (Flin, 2001; Flin et al., 1996; Pate-Cornell, 1993), the Flixborough disaster (Kletz, 2001; Tauseef et al., 2011), BP Texas city (Holmstrom et al., 2006; Le Coze, 2008), the West fertilizer explosion (Pittman et al., 2014), and the Tianjin explosion, are examples of sociotechnical systems failures. According to Rathnayka et al., one of the leading causes of process system failures is increased complexity of system elements (people, equipment, procedures, software, and hardware) and their interactions (Rathnayaka et al., 2011a).

Essential initial steps in process safety and risk management of any facility are hazard identification and hazard analysis. A large volume of work can be found in the literature on different hazard identification and analysis techniques and advanced methodologies, as summarized in Section 2.1. (Dunjó et al., 2010; Khan et al., 2015). However, these methods have been considered inadequate in identifying and analyzing the hazards involved in most incidents

* Corresponding author.
E-mail address: mannan@tamu.edu (M.S. Mannan).

https://doi.org/10.1016/j.psep.2018.01.016
0957-5820/

(Baybutt, 2015b; Kaszniak, 2010). This is because these techniques require competence to overcome incompleteness in identifying potential technical causes and ignored the contribution of human, procedures or organizational elements that affected the analysis results (Baybutt, 2015a; Suokas, 1988; Suokas and Rouhiainen, 1989). Most traditional methods use a linear approach and a single cause-consequence pair (Bruce and Vaughen, 2016). These methods are not complete and lack a comprehensive assessment approach for the system. According to Zhao et al., humans work with technology, social structures, and environment, which can be designated complex systems. In case of an accident system interdependencies must be addressed, and to prevent such accidents, the complete sociotechnical system must be evaluated (Zhao et al., 2015). Therefore, a socio-technical systems perspective covering proper and adequate hazard identification including both technical and social factors is paramount in development of preventive measures for catastrophic incidents. The socio-technical systems theory has been developed and explored by numerous researchers in the past (Katz and Kahn, 1978; Kleiner, 2006; Pasmore and Sherwood, 1978; Rasmussen, 1997). A socio-technical system is characterized as a complex organization with interaction among its elements of human and technology/equipment.

In the present work, a systems-based approach is further developed by including resilience engineering aspects. This results in creation of a holistic view of the hazard identification and analysis process called RIPSHA (Resilience-based Integrated Process Systems Hazard Analysis). This approach is applicable to different modes and subsystems of the process system. To show the usefulness of the proposed approach, RIPSHA is applied to the hazard identification and analysis of a liquefied natural gas (LNG) process system.

2. Background and motivation

This section presents a review of selected, existing hazard identification and analysis techniques gathered from the literature. Further, it presents a brief summary of system and process hazard analysis.

2.1. Overview of existing hazards identification and analysis techniques

There are a number of hazard evaluation techniques used by the process industry as a systematic method to identify influences or causes that may result in incidents or process upsets. (Gressel & Gideon, 1991) presented a review of the eight most commonly used hazard analysis techniques. These included checklists, what-if analysis, safety reviews, preliminary hazard analysis, failure mode and effect analysis (FMEA), fault tree analysis (FTA), event tree analysis (ETA), and hazard and operability study (HAZOP).

It was found that earlier researchers focused mainly on the conventional methods of hazard analysis (Hoepffner, 1989; Knowlton, 1987; Lawley, 1974). Later, researchers extended the work to include new types of deviations, automating the methods, or exploring the development of expert systems (Khan and Abbasi, 1997a,b, 2000; Venkatasubramanian et al., 2000; Wang et al., 2012). Considering batch processes as more critical, some authors focused their work in this area to identify and analyze hazards by developing advanced methods (Palmer and Chung, 2008; Srinivasan and Venkatasubramanian, 1996, 1998a,b; Viswanathan et al., 1999). Also, researchers established hybrid approaches by combining HAZOP with dynamic simulation. (Viswanathan et al., 2000). Furthermore, a comprehensive function based, systems framework approach called Blendid HAZID including system components as plant components, procedural aspects, and people was introduced (Cameron et al., 2007, 2008; Seligmann et al., 2010). A summary of selected hazard identification and analysis methods is presented in Table 1 highlighting system/human/process based approach. More details are given in (Cameron et al., 2017)

Summarizing, it can be concluded that a considerable amount of work has been conducted through exploring and applying various methods. Some examples of these methods are knowledge bases, combined with process models, such as Petri nets, signed digraphs, and dynamic simulation, with focus on improving and semi-automating hazard identification. Nevertheless more research focused on systems thinking is needed for more comprehensive hazard identification and loss prevention control. Of the various methodologies to identify and analyze hazards, particular consideration has been given to HAZOP. The HAZOP methodology is relatively convenient to implement and has been used by the risk assessors in process industry for very long time (Cagno et al., 2002).

2.2. Systems hazard analysis vs process hazard analysis

Process Hazard Analysis (PHA) is a methodical identification, assessment, and documentation of potential process hazards and incident scenarios related to a process plant. It is the most commonly used and easy to implement method used by process industry. It can be performed by using various techniques, such as HAZOP, What-if analysis, safety review, and more.

It has been documented that numerous incidents in the process industry including the chemical, petrochemical, and offshore oil and gas platforms occurred as a result of multiple causes or interdependent failures. The incidents occurred because of breakdown of various system components, such as organizational behavior, human errors, or procedural elements (Baybutt, 2016; Kariuki and Löwe, 2007; Kennedy and Kirwan, 1998; Raman et al., 1991; Rasmussen, 1997). Hence, it is critical to understand and analyze the human, procedures, and other social factors along with the technical factors like process parameters. It has been observed that PHA has a significant limitation where it lacks social and organization factors associated with the operations in a single approach (Schurman and Fleger, 1994).

Various research works have been carried out in field of system safety. The concept of safety culture and its relation to the system property has been explained. (Reiman and Rollenhagen, 2014). Researchers have proposed different accident models demonstrating the influence of human, organizational, and managerial factors (Leveson, 2004; Reason, 1990; Svenson, 1991). Furthermore, aspects such as design, risk analysis informed anticipation, early detection, learning from incidents, and emergency response time are critical to prevent catastrophic incidents. Previous research (Palazzi et al., 2015; Venart, 2007) has demonstrated the importance of these aspects.

The highly complicated and hazardous launching and landing operations at U.S. Navy aircraft carriers emphasize on tracking and monitoring small failures, less oversimplification, sensitivity towards operations, ensuring resilience capabilities (such as adaptive, absorptive, restorative *etc.*) and taking benefit of shifting locations of expertise. Inspired by the smoothness of U.S. Navy aircraft carrier operations several researchers have proposed the High Reliability Organization (HRO) concept. Weick and Sutcliffe (2011) described the concept in extension and explained the (HRO) Principle of "Preoccupation with Failure", which focuses on several small errors that conditionally can lead to a bigger disaster. Hence, by reducing smaller errors a catastrophic incident could be prevented (Weick and Sutcliffe, 2011).

As defined by Stephans, "System safety analysis is the formal analysis of a system and interrelationships among its various parts (including plant and hardware, policies and procedures, and personnel) to determine real and potential hazards within the system