Journal of Loss Prevention in the Process Industries 53 (2018) 61–73

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management

Prerna Jain [a, b, c], Hans J. Pasman [a], Simon Waldram [a], E.N. Pistikopoulos [b, c], M. Sam Mannan [a, b, c, *]

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

ARTICLE INFO

Article history:
Received 16 February 2017
Received in revised form
29 June 2017
Accepted 4 August 2017
Available online 7 August 2017

Keywords:
Risk management
Chemical industry
Socio-technical systems
Resilience engineering
Process safety
Uncertainty
Process modeling

ABSTRACT

Risk management challenges and continuous increase of global public aversion to hazards and risks associated with the process industry have been observed in the recent years. In order to manage process industry risk, several studies and methods have been developed and are currently used. The authors believe that two types of interacting factors: 1) technical (equipment malfunction, process parameter variation), and 2) social (regulations/policy, human and organizational factors) are important in assessment of risk for a process system. However, current methods are based on analysis of either technical factors, often quantitatively, or social factors, usually qualitatively. Apart from failure to establish all critical scenarios due to either factors, their combined and interactive effects are seldom considered. This research need calls for the development of a holistic and integrated systems framework for effective risk management, although full coverage of possible mishaps will be utopian. The application of the resilience engineering perspective is gradually being explored as an approach for considering the dynamics of socio-technical aspects based on systems theory to provide a safety net. This paper presents a novel framework - Process Resilience Analysis Framework (PRAF) for incorporating both technical and social factors in an integrated approach. This is based on four aspects: Early Detection (ED), Error Tolerant Design (ETD), Plasticity (P) and Recoverability (R). The resilience methodology emphasizes dynamics, unforeseen and even unknown types of threats, uncertainty, systems degradation and complex interactions. With resilience metrics a combined framework for predictability, survivability and recoverability, all via dynamic analysis, is introduced. PRAF primarily focuses on early detection of unsafe domains of operation, assessment of aggregate risks and prioritization of safety barriers during process upset situations and reduction in response time resulting in a reduced frequency of loss of containment events (LoC), reduced consequences and enhanced recovery. The paper describes the concepts and principles of the PRAF as a first step.

1. Introduction

Catastrophic incidents and failures of complex infrastructure and systems have led to an increased significance of a systems approach to risk management (Madni and Jackson, 2009). These complex systems can be characterized as a combination of several technical and social sub-systems interacting with each other in specific, usually non-linear patterns. One example of such complex socio-technical systems is the process industry that includes chemical plants, oil and gas platforms, and onshore and offshore installations. The process industry (PI) is an indispensable part of today's modern society considering the critical products it provides for consumption, for sustenance of its members, and maintenance of the infrastructure. However, over decades due to disastrous loss of containment (LoC) incidents, augmented risk and challenges to process safety management of such systems has been acknowledged. Social factors like regulations or policy related matters, human, and organizational factors have been acknowledged to play a crucial role in process safety and also in maintaining the efficiency

* Corresponding author. Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University System, College Station, TX 77843-3122, USA.
E-mail address: mannan@tamu.edu (M.S. Mannan).

http://dx.doi.org/10.1016/j.jlp.2017.08.006
0950-4230/

of technical barriers to prevent high consequence events. Consequently, an interest in an integrated systems based approach of resilience engineering has arisen which considers both technical and social factors in a single methodology and aims to strike a balance between various performance requirements of such systems (Madni and Jackson, 2009). Increased research and application of the resilience engineering concept is evident in various sectors such as ecology, the environment, psychology, *etc.*, in past years. However, process systems resilience has substantial need for a quantified framework to exhibit standardization and development of process resilience aspects and principles (Youn et al., 2011). Typical property of a system is that the whole is more than the sum of its parts, which makes it complex. Process safety incidents emerge due to inability or failure to understand these complex interactions. A resilient process system will be able to survive better when subjected to such unknown and unforeseen threats.

In this paper, a framework of process system resilience analysis is established and the paper is organized as follows. Section 2 describes the limitations in current risk assessment methodologies, the global impact of incidents, and examples of complex system failures that lay down the motivation for this work on development of process system resilience. Section 3 presents the reviewed literature on various related concepts such as process risk analysis and reduction, systems thinking, early fault detection, dynamic simulation, process optimization, and major events modeling. Section 4 presents the Process Resilience Analysis Framework (PRAF) along with details of phases, aspects and metrics. Section 5 summarizes the methods to measure resilience using the aspects and metrics developed and these can be applied to industrial problems for risk management. The paper concludes in Section 6 with remarks and pointers for possible future research.

2. Motivation

Statistics for incidents and LoC events show that they have continued to happen globally and have occurred across a wide variety of industrial sectors. Also, there are limitations in existing risk management methods. For this research, a systems-based resilience approach is proposed to address the gaps identified from literature and to answer the following questions:

- How to predict or find frequency of occurrence of LoC events with developing technology, complexities and stringent regulations?
- How to assess risk with existing safety barriers?
- How to prioritize emergency barriers, and signals from them, in order to reduce response time?

In the next sub-sections, the limitations of risk assessment methods, incident statistics and failure of complex systems are briefly described.

2.1. Limitations of risk assessment and management

There are different types of risk assessment methods: Deterministic and Probabilistic, or Qualitative and Quantitative (Tixier et al., 2002). Some of the major risk identification, estimation and evaluation methods used currently for risk assessment and management are (White, 1995):

- Risk identification: HAZOP: Hazard and operability study, What-if analysis.
- Risk estimation: Fault tree analysis (FTA), Failure mode and effect analysis (FMEA), Human reliability analysis (HRA), Event tree analysis (ETA), Cost benefit and risk benefit analysis (CBA/RBA), Sensibility analysis (SA), Expert systems, databases.
- Risk evaluation: Monte-Carlo simulation, Hertz-type simulation.

Two main observations follow:

- In general risk assessments are based on a mechanistic approach for problem solving. In such cases, the emergent properties arising from the whole system are not recognized.
- Thus far, social factors related to regulations, humans and organizations are not considered in an integrated way during the risk assessment.

The general methods ignore specificities of the studied scenario and complexities of scenarios are generally simplified. The knowledge background of the people, who are participating in the risk analysis, is critical (*e.g.,* as with the main hazard identification technique of HAZOP), and is susceptible to bias and ignorance. Additionally, in HAZOP studies, analysts may miss half of the significant scenarios resulting from a variety of causes such as failure to anticipate human errors and often miss the interconnections between various system elements (Tixier et al., 2002); not discovering design errors (Kidam et al., 2015; Taylor, 2007); and weaknesses of the method itself and team competency (Baybutt, 2015). Furthermore, there is a great disconnection between risk analysis methodologies and social factors (human and organization). The most comprehensive method is quantitative risk analysis, however, analysts have a tendency, to model only equipment failures that appear in databases whereas failure modes may differ widely and historical data may be orders of magnitude different from actual values for a case at hand. Apart from that there are many assumptions made on the nature and follow-up of unintentional hazardous material releases and consequence effects that leads to uncertainty. Often, uncertainty boundaries are vaguely defined. Also, in practice, a thorough review of risk assessment studies is rare.

2.2. Incidents over the years

Developments and advancements in areas of process safety and risk management have arisen and been implemented over the years in the industry. However, a retrospective look at the major incidents in the process industry as shown in Figs. 1 and 2 reveal that incidents continue to happen globally (Marsh, 2016). This data is supporting the fact that there is an increasing trend of incidents, complexity and degradation of the process systems.

2.3. Complex systems failure

Evaluating and managing risk for complex systems such as infrastructure – power, transport; the aerospace industry; the nuclear and energy sector; process industries; medical units; financial and business divisions, *etc.,* is critical for the survival and growth of the nation and its people. However, in the modern world one of the major challenges in the risk management of these is the relative lack of knowledge and expertise to deal with the uncertainties. Hence, looking at the risk problem from a systemic viewpoint will be conducive in effective risk management and thus avoid the conventional notions of risk independence. It is evident that it is the relationships between various components and parts of the systems and their structure that lead to many failures (Dalziell and McManus, 2004). Examples of such failures of complex systems are summarized in Table 1.

The research questions that need to be answered are - how do we address the systemic issues and elevate them to the attention of