Journal of Loss Prevention in the Process Industries 45 (2017) 88–101

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

Understanding industrial safety: Comparing Fault tree, Bayesian network, and FRAM approaches

Doug Smith, Brian Veitch, Faisal Khan*, Rocky Taylor

Faculty of Engineering and Applied Science, Memorial University of Newfoundland, St. John's, NL, Canada

ARTICLE INFO

Article history:
Received 17 June 2016
Received in revised form
15 September 2016
Accepted 30 November 2016
Available online 1 December 2016

Keywords:
FRAM
Bayesian network
Accident modeling
Fault tree analysis
Safety analysis

ABSTRACT

Industrial accidents are a major concern for companies and families alike. It is a high priority to all stakeholders that steps be taken to prevent accidents from occurring. In this paper, three approaches to safety are examined: fault trees (FT), Bayesian networks (BN), and the Functional Resonance Analysis Method (FRAM). A case study of a propane feed control system is used to apply these methods. In order to make safety improvements to industrial workplaces high understanding of the systems is required. It is shown that consideration of the chance of failure of the system components, as in the FT and BN approaches, may not provide enough understanding to fully inform safety assessments. The FT and BN methods are top-down approaches that are formed from the perspective of management in workplaces. The FRAM methodology uses a bottom-up approach from the operational perspective to improve the understanding of the industrial workplace. The FRAM approach can provide added insight to the human factor and context and increase the rate at which we learn by considering successes as well as failures. FRAM can be a valuable tool for industrial safety assessment and to consider industrial safety holistically, by providing a framework to examine the operations in detail. However, operations should be considered using both top-down and bottom-up perspectives and all operational experience to make the most informed safety decisions.

1. Introduction

Understanding industrial accidents will always be at the forefront of industrial safety assessments. This understanding provides the information necessary to apply accident preventative measures to industrial processes. It is unlikely that complete understanding will ever be achieved, given the continual evolution of workplaces. With constantly evolving technologies and societal values, accident theories must also evolve to reflect the current state of knowledge. It is important to understand the evolution of industrial safety assessments and how they are influenced by technologies, societal values, and history.

Societal values are often reflected by the actions of governments and societal leaders. The Code of Hammurabi (Circa 1750 B.C.) is one of the earliest extant codes reflecting the laws of 18th century BC Mesopotamia. This document describes some 300 laws that should be enforced, including “appropriate” punishments for worker malpractice or early industrial accidents. The code was largely based on the retribution principle and also prescribes punishment by the societal level of the victim. This type of legislation would be completely inadequate in today's societies, although it provided some sense of accountability against negligence. The code violates today's standards of human rights, but does reflect what was acceptable in one of the most influential civilizations of the time. This effort to shape human behavior is cited as an early document that addressed health and safety (Speegle, 2012).

Societies have evolved a great deal since then, creating industries which in turn brought about industrial safety assessments. During the industrial revolution, workplaces started to resemble what is seen in today's industries. Safety was approached at that time by using science and engineering to design technologies. Improvements in safety were achieved by adapting first principles and technological advancements to existing systems. An early example of this is the Railroad Safety Appliance Act of 1893 (Hollnagel, 2014a). This act was formed because of public outcry in response to the many casualties of railway work at the time (Louisell and Anderson, 1953). The US

* Corresponding author.
E-mail address: fikhan@mun.ca (F. Khan).

http://dx.doi.org/10.1016/j.jlp.2016.11.016
0950-4230/

government implemented the Railroad Safety Appliance Act to legislate the use of technological advancements, such as air brakes and automatic car couplers, on American railroads. This would reduce the number of injuries to, and fatalities of, railway workers by eliminating manual car coupling. This combination of technological advancement and societal pressures resulted in one of the most significant documents with respect to industrial safety.

In 1979, the Three Mile Island Nuclear Power plant suffered a partial meltdown. A valve that was stuck open in the water cooling system for the secondary core was leaking the cooling water. When control room operators noticed warning lights, the possibility of water cooling failure was dismissed because normal water pressure was measured upstream of the leak. A series of actions was taken to deescalate the situation, but all failed due to improper assessment (US Nuclear Regulatory Commission, 2013). This accident changed the way we understand accidents. Retrospective Analysis uncovered a missing element in accident analysis and human factors became an integral part of formal safety assessments thereafter. Shortly after, the US Nuclear Regulatory Commission published a handbook on Human Reliability (Swain and Guttman, 1983).

In 1986, two accidents occurred that brought attention to another element that was missing in safety assessments. On January 28, 1986, the Challenger space shuttle exploded during its take off, resulting in the loss of life of the six astronauts and one school teacher onboard. While there is consensus that the explosion resulted from an O-ring failure, the subsequent investigation would reveal many questions about the understanding of the risks by the shuttle's management team (Feynman, 1999). On April 26, 1986, the explosion of reactor 4 at the Chernobyl nuclear power plant devastated the area with effects that are still being felt today. Again this accident brought attention to the human factor, but also to the organization's role in human reliability assessments (Meshkati, 1991). It was seen from these accidents that organizations can shape human behavior, and their role has since been considered in formal safety assessments.

History, technology and societal values have shaped our current understanding of industrial accidents. Modern safety assessments require consideration of technological, human and organizational factors, which represent the so-called, socio-technological system. This evolution of safety assessments is a direct result of learning from past accidents in evolving industries and societies. As we learn from accidents retroactively, there is lag between the rates at which industries evolve and safety assessments evolve: Is there a way to reduce this lag time and perform safety assessments that are more representative of the current states of the industries? In this paper, we compare how modern accident analysis techniques process information of industrial workplaces, using a propane feed control system as an example, and examine how that relates to the current understanding of accident processes and industrial operations.

2. Background

Much as safety policy has evolved, so too has the background knowledge that influence safety methodologies. This has been described in terms of the ages of safety, respectively: The age of technology, the age of human factors, and the age of safety management (Hale and Hovden, 1998). Each age is characterized by the consideration of a new class of factors that are revealed as important as past accidents are studied. The age of technology refers to safety assessments that are approached by consideration of technical factors. The age of the human factor refers to the adoption of the human element in safety assessments. The age of safety management refers to incorporation of organizational factors and understanding how organizations can shape human behavior. It has been stated that there has been another age of safety since, the age of integration (Glendon et al., 2006). This age is defined by the integration of the previous three ages into more holistic accident models. There is now a movement to bring about a new age of safety, the adaptive age (Borys et al., 2009). This age refers to the use of systemic accident theories to produce adaptive safety systems. The current age of safety is somewhere between the age of integration and the adaptive age, with practitioners lagging behind researchers and academics (Underwood and Waterson, 2013).

The age of integration is a natural progression of the past principles that have been adopted from risk analysis and reliability engineering. Reliability engineering built a framework that has been quite successful in describing and understanding technical factors. Failure rates of technical components are used to form reliability assessments, and causal relationships are studied for said technologies. The failure rates can then be translated to failure probabilities and used in risk assessments and cost-benefit analysis. This methodology extended into the age of human factors and age of safety management. This produced human reliability assessments. Methods such as THERP (Swain, 1963), ATHEANA (Cooper et al., 1996), CREAM (Hollnagel, 1998) and HEPI (Khan et al., 2006) have been developed to predict human error. Predicting human failure probabilities allowed the human element to be adopted in the risk framework. There is more to consider when examining accidents than technical, human and organizational factors. There are also extreme weather events, political situations, harsh environments, and unexpected deviations from normal operations. These are external factors that cannot be controlled by the stakeholders of the operation, although they must be managed. This has led to the use of Bayesian Networks as a tool to incorporate these complexly interrelated factors into probabilistic models that are updatable and allow the accident risk to be quantified.

The adaptive age of safety, while still building on the information from past ages, requires a shift in the way we view accidents. Accidents are not viewed as resultant of direct causes, but rather as emergent from system variability or from gaps in system control. This is an important distinction because many of the system components that are labeled causes are also present during successful operations. Appropriate actions can be easy to prescribe after the outcome is known, but outcomes are not known in advance. When considering the human factor, emergent accident theories are appropriate because actions cannot be prescribed for all possible conditions found in modern workplaces. This perspective leads to the realization that accident scenarios are not completely preventable and predictable, which makes sense given the continual evolution of industrial workplaces. In the adaptive age, focus is placed on designing safety systems that are adaptable and resilient against emergent accident scenarios.

To examine the difference between the integrative and adaptive age, the following section will examine the case of a propane feed control system. The safety of the system will be examined first by probabilistic approaches: Fault Tree (FT) and Bayesian Network (BN). The system safety will then be examined using adaptive accident model, the Functional Resonance Analysis Method (FRAM).