Journal of Loss Prevention in the Process Industries 49 (2017) 319–325

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

Accidents and the technology

Elisio Carvalho Silva

ECS Consultorias - Rua Dr José Peroba, Edf Metrópolis Empresarial, Sala 610, 41770-235, Salvador, Bahia, Brazil

ARTICLE INFO

Article history:
Received 30 May 2017
Received in revised form
28 July 2017
Accepted 31 July 2017
Available online 2 August 2017

Keywords:
Accident
Technology
Knowledge
FPSO
Failure

ABSTRACT

This paper presents a case study on an accident that occurred in the interior of a floating production, storage, and offloading vessel (FPSO) in order to verify whether this major accident was related to the loss of technological knowledge. In addition to the accident report study, a broad theoretical background has been elaborated to support the hypothesis that major accidents are related to loss of technological knowledge. The outcome of this study shows that the accident occurred at an FPSO in February 2015 had a direct relationship with the loss of technological knowledge, either in the production processes or in process risk management. With the results extracted in this study, it is intended to contribute to the companies that deal with dangerous processes. This will enhance the awareness of actions that can be taken to avoid the loss of technological knowledge, thus reducing the probability of major accidents.

1. Introduction

1.1. Importance of the theme

Major accidents are rare, and people therefore believe that they will never occur. Indeed, for a major accident to happen, several barriers must successively fail. History shows that companies with long safety histories can be surprised by catastrophic accidents. Recent examples are the Deepwater Horizon Rig (DWH) explosion on the Macondo well in the Gulf of Mexico, where there were 11 fatalities, 17 people injured, and where serious environmental damage occurred. Two other examples are the Fukushima nuclear power plant (NPP) accident in Japan, which resulted in extensive radioactive contamination, and the accident in a floating production, storage, and offloading vessel (FPSO) in Brazil, where 9 workers died.

The technology involved in any dangerous process is fundamental to reducing the probability of an accident. From history, it is evident that accidents tend to increase when a loss of knowledge occurs. At the beginning of the industrial revolution, accidents were considered unavoidable events; however, government regulations eventually forced those responsible for such processes to deepen their technological knowledge and thus improve safety. Examples of 19th century accidents include steam engine (boats and locomotives) explosions, crushing accidents due to train coupling, and human exposure to the moving parts of several machines.

In the 20th century, generally beginning in the 1940s, new processes and equipment were constantly being invented, and this process of continuous innovation remains in place today. These new plants and products were designed to meet the needs of societal consumption; leading to mass production. Industrial production had to be transformed into a large-scale operation for the products to become more competitive, because the large production volume would reduce the cost of finished goods. Ongoing changes increased the inventory of hazardous products and the frequency of their transportation. Thus, there was a robust creation of new manufacturing technologies for chemical products, process controls, and storage and distribution. In addition, the systems became increasingly complex. These changes have contributed to the increase in major accidents because of the greater amount of energy involved in the processes, as in the Three Mile Island (1979), Chernobyl (1986), and Fukushima NPP (2011) accidents. Related to industrial accidents are some incidents like the BASF Chemical tank wagon explosion (1948), the Thiokol-Woobine explosion (1971), the Flixborough explosion (1974), and the Seveso (1976) and Bhopal disasters (1984). Analyses of these accidents indicated that the processes involved were typically complex, tightly coupled, and highly interactive systems (Perrow, 1984; Reason, 1997; Leveson, 2011). The individuals who handle such these systems must therefore possess a high level of operational knowledge such that the systems can be operated appropriately and the workers can adequately manage an emergency situation (Silva, 2014).

To the extent that systems become complex, it is necessary to

E-mail address: elisio@ecsconsultorias.com.br.

http://dx.doi.org/10.1016/j.jlp.2017.07.015
0950-4230/

find techniques for making them easy to operate. One such technique is to create a friendly human–machine interface to avoid errors during human intervention, mostly in emergency situations. Furthermore, a worker should undertake deep training in order to properly perform his/her function, because he/she will require high cognitive abilities to promptly understand problems and provide effective solution. This implies good technological knowledge that facilities the ability to associate dissimilar facts, with the aim of reaching a wise decision (Silva, 2015). When this does not happen and layers of protection fail, the accident will take place or the effects of the accident will worsen (Silva, 2014).

The term technology herein is not related only to industrial processes; it also includes the management systems to deal with dangerous processes. In recent paper, Amyotte et al. (2016) corroborate with this line of thinking when quoting seven core concepts extracted from lessons learned from 1984 Bhopal accident, providing invaluable contributions to this matter. In turn, Amir-Heidari et al. (2016) present a new approach to risk assessment to reduce the possibility of accident in the drilling industry.

1.2. The problem

The major accidents are still happening even in high safety-pattern companies. Recent events show this facet as evidenced through the Chemical Safety Board's (CSB) reports regarding to La Porte and Macondo well accidents. (CSB, 2014a, 2014b; CSB, 2014c). These disasters, besides taking lives, cause huge damages to the companies and the environment. Due to the importance of these harmful effects to the society caused by a major accident, it arises the need to deepen their formation mechanism to prevent them. Several theories about accident causation have already been presented and one of them is regarded to the loss of technological knowledge through (Silva, 2015). This paper proposes confirming this argument using a case study. The following question emerges: was the accident that occurred in an FPSO in Brazil related to the loss of technological knowledge? In answering this question, this paper intends to draw attention to the individuals who deal with dangerous processes, to allow action to be taken to avoid the loss of technological knowledge, thus contributing to reducing the probability of major accidents.

1.3. Objective of this paper

This paper presents a case study of the accident that occurred in an FPSO in Cidade de São Mateus, using an evaluation of the accident report issued by Brazil's National Agency of Petroleum, Natural Gas, and Biofuels (NAP). The main causes will be analyzed, with a focus on the loss of technological knowledge in industrial processes. This will be done in comparison with current knowledge provided by several authors and globally recognized organizations.

2. Theoretical reference

2.1. Failures and major accidents

An initiating event is the starting point of an accident. If accident chain is not blocked, an undesirable consequence will occur. Layers of protection are effective mechanisms for interrupting the chain of an accident. If the layers of protection are in place and working properly, the frequency of occurrence of the event (preventive layers) will be reduced to low values. Thus, the accident will probably never occur during the lifetime of the industrial process, or the layers of protection will lessen the consequences of an accident (mitigating layers).

Reason (1997) refers to major accidents as organizational accidents. They are rare, because for the initiating event to occur, the accident will need to challenge several IPLs (scenarios with high severity require multiple IPLs to reduce the frequency of occurrence of the accident). Nevertheless, in some instance IPLs can fail simultaneously, even when they are independent, and a major accident will occur.

IPL failures may arise because of random or systematic failures (Silva, 2014; IEC, 2003; ISA, 2002; ISA, 2005). However, it is unlikely that several IPLs will fail simultaneously because of random failures. Systematic failures are most likely to occur because they are caused primarily by human error (Silva, 2014; IEC, 2003; ISA, 2002; ISA, 2005). This is particularly true for complex systems, because complexity provides a greater potential for human error (Summers, 2015). Also, systematic failures can occur because of direct human action, such bypassing IPLs; this flaw is also called active failure (Reason, 1997). Other significant systematic failures are common cause failures (CCF), because these failures disable even redundant systems or equipment. A pragmatic example of a CCF was the crash of Air France flight 447, in which the initiating event was the failure of both pitot probes, probably because of clogging with ice crystals (BEA, 2012).

Hardware failures are also referred to as dangerous or safe failures (IEC, 2010). A dangerous failure takes an IPL to unsafe mode, because the layer of protection will not prevent an accident, while a safe failure will maintain the hardware in the mode to protect the system. For instance, a safety valve stuck in an open position is a safe failure, while a safety valve stuck in a closed position is a dangerous failure.

Among dangerous failures, the most significant are those that are undetected (IEC, 2010), which can be referred to as latent failures (Reason, 1997), because the IPL can fail without detection, and will therefore not prevent an accident when it is needed.

2.2. Technological knowledge

According to Silva (2015), technological knowledge is related to industrial process technologies and the management systems of those processes. When this knowledge is reduced, the probability accidents increases. Knowledge reduction can arise for several reasons: 1) new technologies; 2) loss of knowledge due to inadequate training, procedures, or information; and 3) failure to incorporate new knowledge, for instance, learned lessons from accidents that have already occurred.

New technologies are vital for global development. Innovations improve human living conditions. However, when innovations involve dangerous processes (chemical, petrochemical, oil and gas industries, nuclear power plant, aviation, etc.) care must be taken, because these cross the boundaries of the known (Silva (2015)). If such innovations are not well-evaluated, latent risk conditions can occur (Reason, 1997). Latent risk conditions come from inadequate design or procedures, incomplete or inconsistent training, possible risk conditions not detected during risk analysis phases, and high process complexities that hamper human diagnosis and subsequent decision-making (Summers, 2015).

New processes occasionally use IPLs that are not well-proven to be in compliance with a work environment. In the Gulf of Mexico accident in 2010, there was strong evidence that the IPL used to prevent well blow out, known as a blowout preventer (BOP), failed because the drillpipe buckled, per the effect of high pressure on the seabed. In addition to the BOP failure, others IPLs also failed (CSB, 2014a; CSB, 2014b).

Even with a known technology, it is possible for loss of knowledge to occur because of deficient or inadequate training, procedures, and information (Silva (2015)). Kemeny (1979) showed that in an accident report for Three Mile Island, in 1979, the lack of