Engineering Failure Analysis 36 (2014) 121–133

Contents lists available at ScienceDirect

Engineering Failure Analysis

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

Texas City refinery accident: Case study in breakdown of defense-in-depth and violation of the safety–diagnosability principle in design ☆

Joseph H. Saleh [a,*], Rachel A. Haga [a], Francesca M. Favarò [a], Efstathios Bakolas [b]

[a] *School of Aerospace Engineering, Georgia Institute of Technology, Atlanta, USA*

[b] *Department of Aerospace Engineering and Engineering Mechanics, The University of Texas at Austin, Austin, USA*

ARTICLE INFO

Article history:
Received 15 June 2013
Received in revised form 5 September 2013
Accepted 20 September 2013
Available online 2 October 2013

Keywords:
Defense-in-depth
Refinery explosion
Safety–diagnosability principle
Accident pathogens

ABSTRACT

In 2005 an explosion rocked the BP Texas City refinery, killing 15 people and injuring 180. The company incurred direct and indirect financial losses on the order of billions of dollars for victims' compensation as well as significant property damage and loss of production. The internal BP accident investigation and the Chemical Safety Board investigation identified a number of factors that contributed to the accident. In this work, we first examine the accident pathogens or lurking adverse conditions at the refinery prior to the accident. We then analyze the sequence of events that led to the explosion, and we highlight some of the provisions for the implementation of defense-in-depth and their failures. Next we identify a fundamental failure mechanism in this accident, namely the absence of observability or ability to diagnose hazardous states in the operation of the refinery, in particular within the raffinate splitter tower and the blowdown drum of the isomerization unit. We propose a general safety–diagnosability principle for supporting accident prevention, which requires that all safety-degrading events or states that defense-in-depth is meant to protect against be diagnosable, and that breaches of safety barriers be unambiguously monitored and reported. The safety–diagnosability principle supports the development of a "living" or online quantitative risk assessment, which in turn can help re-order risk priorities in real time based on emerging hazards, and re-allocate defensive resources. We argue that the safety–diagnosability principle is an essential ingredient for improving operators' situation awareness. Violation of the safety–diagnosability principle translates into a shrinking of the time window available for operators to understand an unfolding hazardous situation and intervene to abate it. Compliance with this new safety principle provides one way to improve operators' sensemaking and situation awareness and decrease the conditional probability that an accident will occur following an adverse initiating event. We suggest that defense-in-depth be augmented with this principle, without which it can degenerate into an ineffective defense-blind safety strategy.

☆ This research builds on and extends previous work presented at the joint ESREL–PSAM conference of 2012.

* Corresponding author. Tel.: +1 404 385 6711.
E-mail address: jsaleh@gatech.edu (J.H. Saleh).

1350-6307/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.engfailanal.2013.09.014

1. Introduction

On March 23, 2005 an explosion rocked the BP Texas City refinery,[1] killing 15 people and injuring 180 after the blowdown drum of the isomerization unit overflowed (loss of containment of hydrocarbons), and a heat source ignited the ensuing vapors resulting in an explosion and subsequent pool fire. Three different investigation panels were convened and generally agreed that the accident resulted from a combination of factors, including design and operational flaws, technical and organizational factors, and more broadly a weak safety culture.

In this work, we reexamine the BP Texas City refinery accident as a case study in breakdown of defense-in-depth, and we identify a fundamental failure mechanism in this accident, namely the absence of observability or ability to diagnose hazardous states in the operation of the isomerization unit. We first examine the accident pathogens or lurking adverse conditions at the refinery prior to the accident. We then analyze the sequence of events that led to the explosion, and we highlight some of the provisions for the implementation of defense-in-depth and their failures. This failure mechanism identified leads us to propose a new principle for supporting accident prevention, the safety–diagnosability principle, which requires that all safety-degrading events or states that defense-in-depth is meant to protect against be diagnosable. We propose that defense-in-depth be augmented or complemented with this principle, without which it can degenerate into an ineffective defense-blind safety strategy [2].

A brief discussion of defense-in-depth is in order, after which we examine its implications on the observability of a system. Defense-in-depth is a fundamental principle/strategy for achieving system safety. First conceptualized within the nuclear industry and rooted in elements of military strategy, defense-in-depth is the basis for risk-informed decisions by the US Nuclear Regulatory Commission [16,23] and is recognized under various names in other industries (e.g., layers of protection) in the chemical industry [1,12,24]. Accidents typically result from the absence or breach of defenses or violation of safety constraints [15,17,25]. The principle of defense-in-depth embodies the idea of multiple lines of defense and safety barriers along accident scenarios, and this principle shuns the reliance of safety on a single element (hence the "depth" qualifier). Defense-in-depth, typically realized by successive and diverse safety barriers, technical and procedural, is designed to: (1) prevent incidents or accident initiating events from occurring, (2) prevent these incidents or accidents sequences from escalating should the first barriers fail, and (3) mitigate or contain the consequences of accidents should they occur because of the breach or absence of the previous "prevention" barriers [21].

Defense-in-depth however is not without its critics. For example, Reason [18] noted that "defences-in-depth" are a mixed blessing. One of their unfortunate consequences is that they "make systems more [...] opaque to the people who manage and operate them." He further explained that "the main problems that defences-in-depth pose [...] is that they can conceal both the occurrence of their errors and their longer term consequences. A characteristic of such defences is that they do not always respond to individual failures. These can be either countered or concealed, and in neither case need the individuals directly concerned be aware of their existence. This allows for the insidious build-up of the latent condition." In other words, by placing multiple defenses along a postulated accident sequence, the signals that may be triggered by these "individual failures" indicating that a safety intervention is warranted are no longer available. As a result, system operators may be left blind to the possibility that hazard escalation is occurring, thus decreasing their situational awareness and shortening the time they have to intervene before an accident is released. Several accident reports identified hidden failures or unobservable accidents pathogens as important contributing factors to the accidents—the Three Mile Island accident being a well known such case [10]—and they lend credence to Reason's statements [17,18]. In this work, we address this particular problem, and propose that defense-in-depth ought to be augmented in such a way as to ensure observability and avoid potential "blind spots" for hazardous states.

The ability to observe and diagnose a hazardous state of a system or the occurrence of a safety-degrading event is crucial in maintaining system safety. Roughly speaking, operators make decisions during system operation that are both based on and affect the internal conditions/states of the system [13]. If process monitoring fails to provide information regarding the actual conditions/states of a system, there is a distinct possibility that operators will make flawed decisions (omission or commission), which in turn can compromise the safe operation of the system or fail to check the escalation of an accident sequence. The absence of observability, or inability to diagnose hazardous states, during the operation of the BP Texas City refinery was a fundamental failure mechanism that contributed to the accident, as we will show in this work.

The remainder of this work is organized as follows. In Section 2, we review the functioning of the raffinate splitter section at the refinery (where the accident occurred), and we examine the accident pathogens and sequence of events that led to the explosion. In Section 3, we introduce the safety–diagnosability principle, and examine its violation within the splitter section. We conclude this work in Section 4.

2. Texas City refinery explosion: anatomy of a system accident

The isomerization unit's function is to separate and refine oil to provide higher-octane components for unleaded gasoline. The unit was comprised of multiple sections; we only focus on the raffinate splitter section (RSS), which is where the accident occurred. The purpose of the RSS is to separate incoming raffinate feed into light and heavy components. In this section

[1] The refinery was previously owned by Amoco prior to the merger of BP and Amoco in 1998. In October 2012, BP sold the refinery to Marathon Petroleum.