Reliability Engineering and System Safety 99 (2012) 105–113

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

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

Review

From learning from accidents to teaching about accident causation and prevention: Multidisciplinary education and safety literacy for all engineering students

Joseph H. Saleh*, Cynthia C. Pendley

Georgia Institute of Technology, Atlanta, GA 30332, USA

ARTICLE INFO

Article history:
Received 20 May 2011
Received in revised form
24 October 2011
Accepted 30 October 2011
Available online 7 November 2011

Keywords:
Engineering education
Accident causation
Prevention
Safety literacy
Safety value chain

ABSTRACT

In this work, we argue that system accident literacy and safety competence should be an essential part of the intellectual toolkit of all engineering students. We discuss why such competence should be taught and nurtured in engineering students, and provide one example for how this can be done.

We first define the class of adverse events of interest as system accidents, distinct from occupational accidents, through their (1) temporal depth of causality and (2) diversity of agency or groups and individuals who influence or contribute to the accident occurrence/prevention. We then address the question of why the interest in this class of events and their prevention, and we expand on the importance of system safety literacy and the contributions that engineering students can make in the long-term towards accident prevention. Finally, we offer one model for an introductory course on accident causation and system safety, discuss the course logistics, material and delivery, and our experience teaching this subject. The course starts with the anatomy of accidents and is grounded in various case studies; these help illustrate the multidisciplinary nature of the subject, and provide the students with the important concepts to describe the phenomenology of accidents (e.g., initiating events, accident precursor or lead indicator, and accident pathogen). More importantly, the case studies invite a deep reflection on the underlying failure mechanisms, their generalizability, and the various safety levers for accident prevention. The course then proceeds to an exposition of defense-in-depth, safety barriers and principles, essential elements for an education in accident prevention, and it concludes with a presentation of basic concepts and tools for uncertainty and risk analysis.

Educators will recognize the difficulties in designing a new course on such a broad subject. It is hoped that this work will invite comments and contributions from the readers, and that the journal will support the publication of exchanges on this subject.

Contents

1. Introduction: motivation and scope . . . 106
2. Conceptual background: learning loops and the safety value chain . . . 107
   2.1. Learning loops . . . 107
   2.2. Safety value chain . . . 108
3. Why accident causation and system safety should be taught to engineering students . . . 108
   3.1. Content-centric arguments: memory of past failure modes, safety competency, and contribution to accident prevention . . . 108
   3.2. Process-centric arguments: multidisciplinary awareness, collaboration, and safety culture . . . 109
   3.3. Reasoning scheme: new designs, new technology, and new failure mechanisms . . . 109
   3.4. Accident case studies and the value of teaching history . . . 109
4. What to teach about accident causation and system safety to engineering students, and how? . . . 109
   4.1. Anatomy of accidents: case studies . . . 110
   4.2. Defense-in-depth and safety barriers . . . 110

* Corresponding author.
E-mail address: jsaleh@gatech.edu (J.H. Saleh).

0951-8320/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2011.10.016

4.3. Uncertainty and risk analysis . . . 111
4.4. Broader themes, missing ingredients in the course? . . . 111
4.5. Course logistics and ancillary objectives . . . 111
5. Conclusion . . . 112
Appendix . . . 112
References . . . 112

1. Introduction: motivation and scope

The recent mining disaster at Upper Big Branch, West Virginia, and the explosion on the drilling rig in the Gulf of Mexico and the ensuing catastrophic oil spill are stark reminders of the importance of safety competence at the technical, organizational, and regulatory levels. This article discusses why and how such competence should be taught and nurtured in engineering students.

Before delving into the details of our arguments, it is important first to motivate the interest in accident causation and system safety, and to delineate the scope of the present work and the class of adverse events it seeks to tackle.

High-visibility accidents such as the Bhopal, Piper Alpha, and Chernobyl tragedies, accidents that result in dramatic casualty tolls, significant financial losses, and environmental damage are often invoked to motivate an interest in accident prevention and system safety. Unfortunately, industrial accidents, also known as or subsumed under the broader designation of *organizational* or *system accidents*, happen much more frequently than what may be conveyed by the "high-visibility" above-the-media-radar-screen accidents. Examples of such accidents abound in many industries, such as the chemical, oil and gas, mining, and transportation industries to name a few. For instance, in the U.S. chemical industry alone, 1970 industrial accidents occurred in the last 5-year EPA-mandated reporting period. These accidents resulted in excess of $1 billion in property damage,[1] and affected large communities with over 200,000 people who had to be evacuated. In addition, approximately 2000 deaths and injuries were reported as a result of these accidents [44]. The propensity for this class of adverse events—officially termed a "disaster" in the U.S. mining industry when five or more fatalities are involved—may be indicative of theoretical deficiencies in the understanding of system accident causation and prevention. However, when carefully analyzed, many system accidents share a conceptual sameness in the way they occur, through a combination of system design and technical flaws, operational or workforce failings, compromised organizational behaviors and management shortcomings, and/or deficient regulatory oversight. This observation of a conceptual sameness in the way system accidents occur suggests an additional dimension to the previous hypothesis in accounting for the propensity of this class of adverse events, namely that system safety education may be limited in effectiveness, not reaching its target audience, or not conducted at a scale commensurate with the importance of the subject.

To summarize, the previous discussion provided three complementary parts for the answer to the question: "why an interest in accident causation and system safety?" These were as follows: (1) safety is more often compromised and system accidents occur much more frequently than what may be conveyed by the media; (2) the pattern of occurrence of these accidents suggests an important role of education in contributing to the prevention of such accidents; (3) the potential consequences of system accidents, high casualty tolls, environmental damage, and economic losses, along with ethical/moral considerations, are strong incentives for a careful interest in accident prevention and system safety.

The discussion that follows will be tailored or made more specific to engineering students. The reason for this tailoring is that different groups or stakeholders may be interested in this topic for different reasons. For example, accident causation has an intrinsic litigation aspect to it, and it invites a backward-looking approach with the dual objective of identifying culprit(s) and distributing penalties [46]. Thus law students for example may be exposed to this subject for training purposes specifically to handle this litigation aspect. This aspect is not explored in this work. However, an interest in accident causation can also have a forward-looking objective of identifying and eliminating failure causes and mechanisms, thus contributing to future system safety and accident prevention. The role of safety education of engineering students will be explored in this latter context.

What class of adverse events are we interested in? The risk analysis and system safety literature reports on a distinct class of adverse events initially termed "industrial accidents" or "man-made disasters" [54], and later characterized as "organizational accidents" [41] or "system accidents" [36]. These two qualifiers of accidents, "organizational" and "system", are used to indicate on the one hand an organizational contribution to accident causation beyond the traditional technical and human error factors, and on the other hand a recognition that accidents can result "from dysfunctional interactions among system components" [31], not just component failures, hence the qualifier "system". The Department of Energy, in its accident investigation guide, defines an accident as an "unwanted transfer [or release] of energy that, due to the absence or failure of barriers and controls, produces injury to persons, damage to property, or reduction in process output" [13]. What is distinctive about system accidents is the following:

1. The chain of causality, or chain of influence, leading to the accident extends beyond the temporal vicinity of the moment the accident occurred, with build-up of accident pathogens occurring over different time-scales before an initiating event triggers an accident sequence. This characteristic can be termed the *temporal depth of causality* of system accidents.
2. The safety value chain (see Fig. 1 and Section 2), that is, groups and individuals who influence or contribute to the accident occurrence/prevention, extends far beyond the immediate victims, who may or may not have contributed to the accident. This characteristic can be termed the *diversity of agency* in system accidents.

This class of adverse events, system accidents, is different from occupational accidents, for example a "slip, trip, and fall" in which the agent and the victim are the same individual. The latter, occupational accidents, of particular interest to epidemiologists, are not discussed in this article. System accidents, typically but not exclusively associated with large-scale releases of energy, are the focus of this work.

This article explores the role of engineering education in improving system safety and contributing, in the long term, to accident prevention. The theme of "learning from accidents" is often explored in the literature (see for example [29,37,38]).

[1] "Not including other form of losses such as business interruption costs, shareholder value, and lost business associated with accidents. These latter costs are likely to be larger, perhaps much larger, than losses due to property damage" [27].