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

* 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

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].

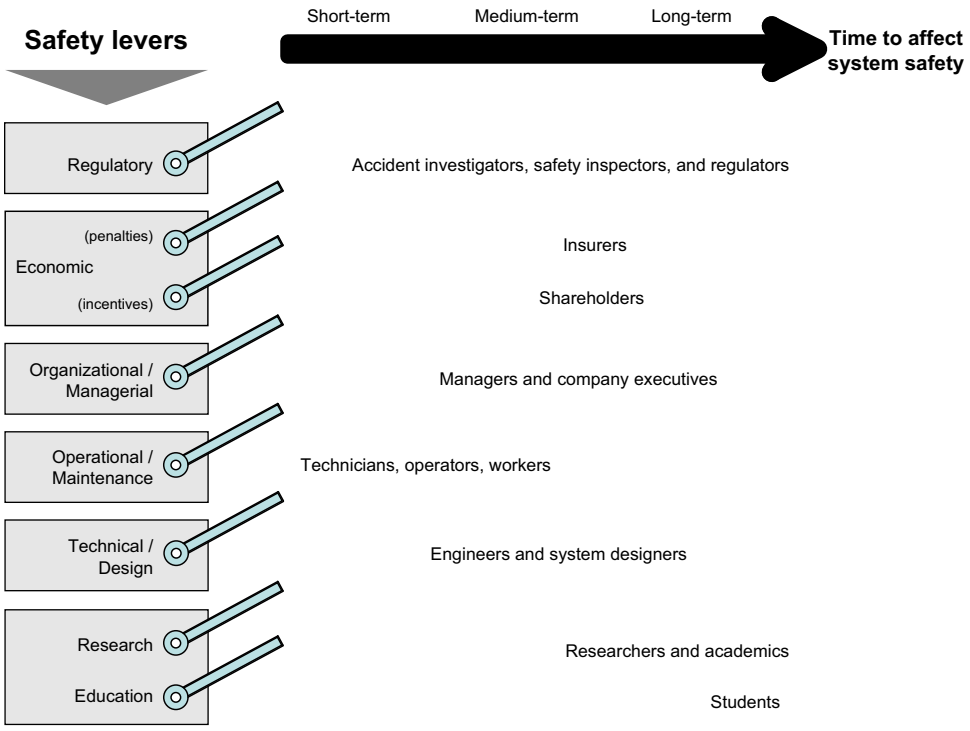

Fig. 1. Safety levers and stakeholders in the safety value chain (not meant to be exhaustive).

Learning however is multileveled and it can take place for example at the organization level, the broader sector or industry level, and the regulatory level [24]. In this work, we explore what can be learned from system accidents at the engineering students' level, and in essence, we shift the focus from "learning from accidents" to "teaching about accidents and system safety".

The remainder of this article is organized as follows. Section 2 provides the conceptual background, of learning loops and safety value chain, within which the role of engineering education in accident prevention is discussed. Section 3 advances several arguments for why accident causation and system safety should be taught to engineering students. Section 4 proposes a set of themes that can be taught about this subject and how this multidisciplinary teaching can be structured and delivered. Section 4 also discusses the author's experience with the teaching of such a course for the past several years at the Georgia Institute of Technology. Section 5 concludes this work.

2. Conceptual background: learning loops and the safety value chain

This section provides a general overview of the context within which we discuss the role of engineering education in accident prevention, and why safety competence should be taught and nurtured in engineering students. The two central notions are those of learning loops and safety value chain, and they are discussed next.

2.1. Learning loops

Consider the post-event activity of accident investigation[2]: accident investigations have fundamentally backward-looking objectives of determining the facts surrounding accidents and identifying causes ad contributing factors to the event. In addition, accident investigations have an intrinsic forward-looking objective of providing clear "learning monads" and requesting changes for improving future system safety and accident prevention, through various recommendations and corrective actions at the technical, operational, organizational, and sometimes regulatory levels. Thus learning and the notions of feedback or "learning loops" are intrinsic to accident investigations[3] [19]. The discussion in this work fits within the notion of "learning loops." In effect, we propose to extend a "learning loop" to engineering students, and start it not from a particular accident investigation but from a multidisciplinary synthesis of various accidents analyses and works on system safety.

What is learning? In addition to acquisition of knowledge or skill, learning can be loosely defined as the modification of behavior due to (the understanding of) previous experience (Merriam-Webster). According to Sterman [51], "learning is a feedback process in which our decisions alter the real world, we receive information feedback about the world and revise the decisions we make and the mental models that motivate those decisions." This definition provides a good link between the two concepts, learning loops and safety value chain, within which we place our discussion of the role of engineering education in accident prevention. Multiple feedback loops are extended following an accident event, and safety-related learning can occur at different time-scales for different stakeholders. The stakeholders are the agents who partake in the safety value chain, discussed next.

[2] Activities related to disasters and system accidents are classified on a temporal basis as "pre-(adverse) event" and "post-event", the former pertaining among other things to prevention and inspection activities, and the latter to disaster response and management activities and accident investigations.

[3] In their enthusiasm for this idea, some authors have written about the "gift of failures" (e.g., [15]). We believe this is a wrong metaphor for system accidents on both a cognitive and emotional level.

2.2. Safety value chain

Accident investigations typically seek the "root cause" of, and "contributing factors"[4] to, an accident. There is however often a degree of arbitrariness in interpreting what is an error and in choosing where to stop going back in the causal chain. At any point in the causal analysis, a failure or an error can be conceived of as a "result", not a "cause",[5] a consequence of something prior or more fundamental. The notion of safety value chain highlights the agency in influencing and contributing to accident prevention and sustainment of system safety. Instead of emphasizing that, which partakes in accident causation, the safety value chain identifies those who contribute to accident prevention and sustainment of system safety—a more inclusive and irenic concept than the litigious "contributors" to accident causation, and as such, it may be more enticing for various stakeholders to accept and actively participate in, including companies' management, senior executives, and shareholders. In this sense, the safety value chain includes operators, technicians/maintenance professionals, engineers, system designers, managers and executives, shareholders, regulators, safety inspectors, and accident investigators (see Fig. 1), groups of individuals who affect and contribute to system safety over different time-scales. The short time-scale is sometimes referred to as the "sharp-end of safety", e.g., a nuclear power plant operator for example is said to "operate" at the sharp-end of the safety of the plant, whereas a manager at that plant for example operates at the "blunt-end of the safety" [41]. Our discussion in this work expands the scope of the system safety value chain, and we propose that engineering students are important stakeholders in the safety value chain. It is often said that the best technology transfer mode is "wearing shoes"; by educating and engaging engineering students in the multidisciplinary issues of accident causation and system safety, educators can help infuse their students, the future contributors, managers, and leaders of technology-intensive or hazardous industries, with a proper safety competence and accident awareness before they enter the workforce, and in so doing, they will contribute, in the long-term, one small step towards accident prevention. In the following sections, we delve into the details of why and how this can be done.

3. Why accident causation and system safety should be taught to engineering students

This section discusses reasons for teaching engineering students about accident causation and system safety.

Intrinsically related to this question of "why" teach this subject is the more difficult question of "what to teach" about this subject, and how such multidisciplinary teaching can be devised and delivered. For example, can such teaching be done in a manner that is domain-independent and relevant across all engineering departments and their respective industries, or should it be based within established engineering departments and its content narrowly defined and tailored to a specific department and its respective industry (e.g., aviation safety, chemical safety, and nuclear safety)? We discuss these issues in Section 4 although some aspects of that discussion are noted in this section.

There are several reasons why engineering students should be exposed to and taught about accident causation and system safety. In the following, we propose several arguments in support of this teaching. These arguments are not meant to be exhaustive nor are they mutually exclusive.

3.1. Content-centric arguments: memory of past failure modes, safety competency, and contribution to accident prevention

The first argument in support of teaching engineering students about accident causation and system safety has been noted earlier in this work: it concerns their contribution, in the long term, to accident prevention. Holloway and Johnson [20] made broadly similar arguments in discussing why safety professionals should read accident reports, and Johnson [21] discussed the education and competency requirements for accident investigators—different stakeholders in the safety value chains than the ones we target in the present work, engineering students, but with related end-objective nonetheless.

Structural engineering has been a strong proponent of "failure literacy" [11,12] for engineering students. "This literacy entails knowing about the critical historical failure cases that have shaped the profession", Delatte [11,12] explains, and he proceeds to expand on a list "landmark structural failures" or case studies, which should be taught, such as the Tacoma Narrows bridge collapse and several other bridge and building collapses. Petroski [37] has been an early proponent of learning from structural failures in his landmark "To Engineer Is Human" book, and he proposed that the concept of failure is a unifying theme central to engineering education and practice: "[t]o understand what engineering is and what engineers do is to understand how failures can happen and how they can contribute more than successes to advance technology". A recent special issue of the journal Engineering Structures (July 2010) was devoted to "Learning from Structural Failures", a popular theme judging by the growing number of publications devoted to the subject.[6]

Recall that our focus is why teach engineering students about accident causation and system safety, a topic adjacent to but different nonetheless from the well-trodden "learning from accidents". The first argument for teaching engineering students about accident causation and system safety extends beyond structural engineering failures, and it boils down to teaching about past failure modes in engineering systems to prevent their recurrences. More precisely, the first argument builds on the role of memory in education, and it seeks to make engineering students the agents and repository of a particular type of memory—of previous accidents as well as their failure causes and mechanisms—to fend off technical amnesia and help avoid repetition of similar accidents. For example, following the Tacoma Narrows bridge collapse, accounting for wind conditions and aeroelastic flutter effects became standard in civil engineering courses pertaining to design of suspension bridges.[7] However, it should be noted that memory of past accidents and their lessons learned are not only encoded in education, but they are often "institutionalized", in building codes for example or Occupational Health and Safety regulations. As a result, instilling the memory of past accidents and their lessons learned in engineering students can be seen as serving the function of diversity in redundancy (where memory resides and who recalls and exercises it) to help to avoid a repetition of similar accidents. Teaching engineering students about accident causation and system safety can serve to complement and reinforce institutionalized safety requirements, and it can empower students to later advocate for

[4] Several terms are used in accident investigations such as "direct cause", "root cause", and "contributing cause". Details on these terms can be found in [13,26].

[5] This is a basic idea in psychotherapy, of error as a consequence not a cause. This observation can be stated casually as "one person's *cause*, (i.e., what one person identifies as a "cause") is another person's *consequence*".

[6] Using the search engine Google Scholar, some 1380, 476, and 352 articles were found to have in their titles "learning from failures", "learning from accidents" or "learning from disasters", respectively, and some 347, 25, and 17 peer-reviewed articles using Web of Science® (retrieved August 16, 2010).

[7] This is an example of what was previously termed a "learning monad" from accident investigations.

safety considerations, especially when unlegislated, in their organization's behavior and decision-making.

3.2. Process-centric arguments: multidisciplinary awareness, collaboration, and safety culture

Why teach engineering students about accident causation and system safety? Beyond the argument of the usefulness of specific lessons learned and technical content noted in the previous section, teaching this subject can make an important process-centric contribution by

> "equip[ping] graduates with a broader perspective on their disciplines, in order to be able to look beyond the technical issues and integrate multidisciplinary safety considerations into their decision-making [later in their professional careers] as designers or managers" [18]

This multidisciplinary awareness can help engineering students later in their careers contribute to accident prevention by seeking or facilitating coordination between themselves (the technical specialists), management, and workers/operators over system safety issues. In other words, it will help them seek and engage in productive conversations pertaining to accident prevention and system safety with different stakeholders.

It was noted previously that system accidents have an intrinsic organizational contribution to their occurrence beyond the technical and human error contributions, and that such accidents can result from dysfunctional interactions between system components (and stakeholders), not just component failures. Equipping engineering students with a multidisciplinary perspective on accident causation and system safety can help them be more attuned to these characteristics of emergent phenomena in system accidents, and encourage them to communicate and collaborate with others to prevent safety issues from falling through the proverbial organizational cracks.

Swuste and Arnoldy [53] discuss the role of safety advisors/managers in a company as agent of changes for improving safety management; the argument in this section posits a similar role, although over a longer timeframe, for engineering students.

Finally, the connection between safety education and safety culture should be pointed out. There is an extensive literature on "safety culture", its constitutive elements, and the important roles it plays in accident prevention [10,17,39]. Safety culture earned its recognition following the Chernobyl accident, when the International Atomic Energy Agency identified the poor safety culture at the plant as the primary cause of the accident. A commonly accepted definition of safety culture is the following:

> "the product of individual and group values, attitudes, perceptions, competencies, and patterns of behaviors that determine the commitment to and the proficiency of an organization's health and safety management" [1].

It is fair to assume that teaching engineering students about accident causation and system safety can help instill in them a proper safety culture before they enter the workforce or it can accelerate their acquisition of an organization's safety culture.

3.3. Reasoning scheme: new designs, new technology, and new failure mechanisms

Engineering students will often be involved in the development of new technologies or in the design of new systems. Design and innovation are intrinsic to the engineering education mindset.

In addition to the previous content- and process-centric arguments for teaching engineering students about accident causation and system safety, one can advance that teaching this subject is also useful in a different way: it can complement the engineering design mindset with a meta-cognitive insight, or reasoning scheme about the possibilities of failures and failure mechanisms. Engineering students would come to think simultaneously about new designs and the possibilities of new failure mechanisms. Design creativity in engineering students would be complemented with an instinctive concern for the possibilities of new failure mechanisms and creativity in mitigating or eliminating them.

Concern with system failures and accidents should be central to the engineering profession and to engineering education. It can lead to accident prevention not only through the memory of past failure mechanisms and lessons learned, but also through constant safety vigilance and the development of new knowledge for the prevention of accidents and the sustainment of system safety, especially when faced with new situations with new systems and technologies.

Our academic experience to date suggests there is an unfortunate growing reliability and safety illiteracy in engineering education, and it deserves serious consideration to be tackled and reversed.

3.4. Accident case studies and the value of teaching history

Teaching about accident causation and system safety through case studies of past major accidents, for example, is in a way teaching a particular kind of history. The case for teaching this subject can therefore borrow arguments from why teach and study history:

> "History should be studied because it is an absolutely necessary enlargement of human experience, a way of getting out of the boundaries of one's own life and culture and of seeing more of what human experience has been". [6]

The study of accident causation and system safety, through case studies, can engage engineering students, cognitively and emotionally, in ways that educators cannot necessarily foresee, but that are likely to have a positive and enduring effect on their minds. This constitutes an important role for education, beyond the "overly instrumental [utilitarian] model of the university, [which] misses the genius of its capacity, [and] devalues the zone of patience and contemplation the university creates in a world all but overwhelmed by stimulation" [16].

4. What to teach about accident causation and system safety to engineering students, and how?

In the previous sections, we defined the class of adverse events we are interested in and advanced several arguments for why accident causation and system safety should be taught to engineering students. The more difficult questions of what to teach about this subject, and how, remain to be addressed. More specifically, what should be taught, and how, in an introductory one-semester course on accident causation and system safety, which all engineering undergraduate Seniors and first year graduate students should take? These issues are discussed in this section. We restrict the scope to a one-semester course because in an already crowded engineering curriculum, it is unlikely that this subject would be given more ample time in a common-core syllabus.[8]

In the following, we present one model for the structure and content of such a course. Other models are possible, and

[8] Some advanced optional courses already exist in graduate engineering programs and their contents are tailored to specific departments and industries (e.g., chemical hazards and safety).

educators will no doubt recognize the difficulties in designing a new course subject to a variety of constraints. It is hoped that the following discussion will invite comments and contributions from the readers, and we hope that the editor(s) of this journal will encourage the publications of comments and exchanges on this subject. The purpose of these exchanges would be to bring a collective educational wisdom to bear on the development and refinement of a course on accident causation and system safety, a course that can be taught broadly in all engineering schools.

4.1. Anatomy of accidents: case studies

Before discussing concepts and abstractions in accident causation and system safety, it is important to motivate and ground the course in case studies of actual accidents. We believe the use of case studies is particularly important for this course in general, and for the introduction to this course in particular. The use of case studies, or case-based learning, is widely adopted in business, law, and medical schools, and it deserves careful consideration in engineering education as well. The arguments in their support are that case studies "make schooling more relevant to the subsequent workplace" [9], they offer a wealth of information about context and realistic real-world problems, and they are more engaging and intellectually enriching for students. Many choices are accidents case studies are possible. An extensive list can be found in Kletz [29] for example. We selected for our course the following accidents:

1. Piper Alpha.
2. Challenger.
3. TWA Flight 800 and Alaska Airlines Flight 857.
4. Three Mile Island.
5. The Jim Walter Resources (JWR) No. 5 mine disaster.
6. Therac-25 accidents.

These accidents provide a diverse set of case studies, and they introduce the students to the multidisciplinary nature of accident causation and system safety. Each accident highlights specific failure mechanisms, and although in different industries, these accidents provide an opportunity to illustrate several concepts that help describe the phenomenology of accidents, such as the important notions of *initiating events*, *accident precursor* or *lead indicator*, *accident pathogen*, and *accident sequence* or *trajectory*. These are essential elements for a basic education in accident causation and system safety. In addition, these case studies help students better appreciate the notions of safety levers and safety value chain discussed in Section 2, and they invite a deep reflection on prevention mechanisms for counteracting their failure causes and mechanisms.

Material and delivery: although the accident reports are made available to the students, the class discussion is based on the following documents, provided to the students at the beginning of the semester:

- [34] Pate-Cornell E. Learning from the Piper Alpha accident: a postmortem analysis of the technical and organizational factors. Risk Analysis 1993;13(2):215–32.
- [2] Anon. Safety report on the treatment of safety-critical systems in transport airplanes. National transportation safety board report. NTSB/SR-06/02. Washington, DC.
- [22] Hopkins A. Was the three mile island a "normal accident?" Journal of Contingencies and Crisis Management 2001;9(2):65–72.
- [43] Saleh JH, Cummings, AM. Safety in the mining industry and the unfinished legacy of mining accidents. Safety Science 2011;49(6):764–77.
- [30] Leveson NG, Turner CS. An investigation of the Therac-25 accidents. Computer 1993;(7):18–41.

The following two videos are also screened and discussed in class (both are publicly available online):

- Piper Alpha: spiral to disaster (American Institute of Chemical Engineers, AIChE [4]).
- Challenger: go for launch [BBC documentary].

Each case study is covered in one or two hours. The discussion of the accident is initiated by a student, assigned to the particular case study at the beginning of the semester. Typical prompts include the following: how did the accident unfold (to make sure that the accident sequence is properly understood by everyone)? What caused the accident? This question, which usually makes for a very lively and interesting discussion in class, invites a deep reflection of the concept of causality in system accident as well as the appreciation of the idea of chain of influence and network of contributing factors to system accidents. What contributed to the accident? How could the accident have been prevented? What can be done or put in place to avoid similar accidents in the future?

The case studies prepare the students for the following theme in the course, safety barriers, and defense-in-depth.

4.2. Defense-in-depth and safety barriers

The importance of the concepts of defense-in-depth and safety barriers in accident prevention cannot be underestimated. We believe these concepts are essential elements for a basic education in accident causation and system safety.

[9]Defense-in-depth is a fundamental principle or strategy for achieving system safety. First conceptualized within the nuclear industry, defense-in-depth is the basis for risk-informed decisions by the U.S. Nuclear Regulatory Commission [33,50], and it is recognized under various names in other industries (e.g., *layers of protection* in the chemical industry [4,28,52]). Accidents typically result from the absence or breach of defenses or violation of safety constraints [31,40,23]. The principle of defense-in-depth embodies the idea of multiple lines of defense and safety barriers along accident scenarios, and requires that ensuring system safety should not rely 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 initiators 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). The concept of safety barriers is an embodiment of the "defense" part of defense-in-depth safety principle, in the sense that *defenses* are realized through *barriers*, that is functions and "safety systems deliberately inserted" [14] along potential accident sequences.

The discussion of defense-in-depth and safety barriers emphasizes the idea that for proper hazard control and accident prevention, it is important to understand the ingredients of hazard build-up and escalation, as well as the "signatures" of these hazardous states and transitions—the operational recognition and awareness that an accident sequence may be unfolding, which should prompt intervention (precursors or warning signs). The previous case studies (Section 4.1) provide the students with a solid basis for understanding accident sequences (hazard escalation)

[9] This paragraph is an excerpt from a discussion in [44].

and appreciating the different types of safety barriers that can be thought of and put in place to prevent or contain accidents.

It was noted in Section 3 that a course on accident causation and system safety can complement the engineering design mindset, or design creativity in engineering students with an immediate concern for the possibilities of failure mechanisms and creativity in mitigating or eliminating them. This can be achieved in part through the presentation and discussion of defense-in-depth and safety barriers; these concepts entail or force the thinking about possible accident scenarios and specific design and operational choices to address them. This can be viewed as the promotion of a safety design and innovation mindset.

The following material is used for the class discussion of safety barriers and defense-in-depth (typically covered in four hours):

- [47] Sklet S. Safety barriers: definition, classification, and performance. Journal of Loss Prevention in the Process Industry 2006;19(5):494–506.
- [14] Duijm NJ. Safety-barriers diagrams as a safety management tool. Reliability Engineering and System Safety 2009;94(2):332–41.
- [50] Sorensen JN, Apostolakis GE, Kress TS, Powers DA. On the role of defense in depth in risk-informed regulation. In: Proceedings of PSA '99, international topical meeting on probabilistic safety assessment. Washington, DC; August 22–26; 1999. p. 408–13.
- [7] Bakolas E, Saleh JH. Augmenting defense-in-depth with the concepts of observability and diagnosability from control theory and discrete event systems. Reliability Engineering and System Safety 2011;96(1):184–93.[10]

The discussion of defense-in-depth and safety barriers addresses two complementary themes in the course, namely technical safety principles (safety by design, safety margins, and fail-safe principles) and organizational contributions to system accident causation and prevention.

4.3. Uncertainty and risk analysis

The course then proceeds to introduce and discuss risk analysis. The lectures cover tools such as Failure Mode, Effects, and Criticality Analysis (FMECA), Fault Tree Analysis, and Probabilistic Risk Analysis (PRA). The discussion modules cover more fundamental issues pertaining to risk analysis and expose to the student to broader issues and debates in the risk community. The following material is used for the class discussion of risk analysis:

- [25] Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Analysis 1981;1(1):11–27.
- [35] Pate-Cornell E. Uncertainties in risk analysis: six levels of treatment. Reliability Engineering and System Safety 1996;54(2):95–111.
- [5] Apostolakis GE. How useful is quantitative risk analysis? Risk Analysis 2004;24(3):515–20.
- [40] Rasmussen J. Risk management in a dynamic society: a modeling problem. Safety Science 1997;27(2/3):183–213.

The risk module in the course is typically covered over a two-week period (six to eight hours), and if more time remains before the end of the semester, some of the following broader themes are briefly discussed.

[10] This article provides an additional case study of the BP Texas City Refinery accident in 2005.

4.4. Broader themes, missing ingredients in the course?

The previous three modules in the course, anatomy of accidents, defense-in-depth, and risk analysis, cover an extensive amount of material, all of which we believe is essential for engineering students to be exposed to. There remains however a number of important topics, which are not directly addressed in the course, and given its time constraints, we are still exploring how best to incorporate them, if possible. Feedback from the safety community on these issues would be particularly appreciated. The broader themes are the following:

- Risk communication.
- Models of human errors, and human reliability.
- Post-event activities and elements of disaster management.
- Safety culture.
- Judgment in risk decisions, in particular the critical assessment of cost–benefit analysis and the ALARP[11] principle.

The last two themes have occasionally been covered in class, through the discussion of the following articles (a more extensive bibliography is provided to the students):

- [49] Sorensen JN. Safety culture: a survey of the state of the art. Reliability Engineering and System Safety 2002;76(2):189–204.
- [48] Smyth AW et al. Probabilistic benefit–cost analysis for earthquake mitigation: evaluating measures for apartment houses in Turkey. Earthquake Spectra 2004;20(1):171–203.
- [32] Melchers RE. On the ALARP approach to risk management. Reliability Engineering and System Safety 2001;71(2):201–8.

4.5. Course logistics and ancillary objectives

In addition to the weekly presentations and discussions, the students turn in a short two-page critical summary of each assigned article. The purpose of this weekly assignment is threefold: (1) it provides the students with repeated opportunities to write technical notes and improve their skills at it[12]; (2) it requires them to identify and synthesize key ideas in their readings and it prepares them for the critical assessment of the reading material during the class discussion; (3) it prepares them for researching and writing their own term-paper for the course.

The term-paper is a major deliverable in the course, and it is particularly important in a course with a broad scope such as accident causation and system safety. The idea of the term-paper is to provide a venue and an opportunity for students in this course to identify a topic of their own choosing and interest, and to research it and write about it. Two positive side-effects of this assignment is that it invites students to interact more closely with the instructor as they are researching the topic, almost on an advisor–advisee relationship (more personalized instruction), and it helps them build a proficiency in conducting literature searches and writing with sources.[13] Term-papers to-date have included case studies of previous accidents, survey papers of particular themes in accident causation and system safety, and for some of the more analytically mature students, stochastic modeling and analysis of particular events or topics.

[11] As low as reasonably practicable.

[12] Technical writing is often identified as a weakness in engineering graduates.

[13] The following document is shared and discussed in class: Harvey G. "Writing with sources: a guide for students." Hackett Publishing Company, Indianapolis IN/Cambridge MA, 1998.

Other options for assignments are being considered for the course, such as group term projects, and some form of interaction with government regulatory agencies, and accident investigation boards.

When devising a new course, it is important to reflect on the material to be delivered, how to deliver it, and how to evaluate the teaching effectiveness and impact. The course has not been taught long enough to assess what is known in education research as "far transfer" or its long-term impact [8]. A brief discussion of the approach and challenges to this assessment of long-term impact is provided in the appendix. But the short-term evaluation of the teaching effectiveness is covered in anonymous surveys students fill out at the end of the course. The students' feedback to date has been positive: the "overall class structure and organization of the material" is rated very high, the "overall class experience" is rated as high, and the "overall class difficulty" is rated as moderate. The interactive format of the class is particularly well liked, and the case studies are noted as particularly engaging and "eye openers". Criticism of the course included the following: not enough focus on probabilistic modeling and risk analysis; some students wrote that more case studies were needed, while others suggested that fewer case would do; some students asked that fewer reading and writing assignments and a couple of analytical homework in their stead. These comments are carefully reviewed and some changes to the course are considered. The course is still evolving. Some of the criticism however reflects the diversity of interest and background of different students, and in multidisciplinary courses such as this one, it may not be possible to tailor the content to satisfy everyone.

One student wrote in the course evaluation, "I feel like there's just so much more to learn"; we consider this realization a worthy educational outcome of the course.

5. Conclusion

This article discussed why system safety competence should be taught and nurtured in engineering students, and offered one example of how it can done through a course on accident causation and system safety. The article argued that system accident literacy and safety competence should be part of the intellectual toolkit of all engineering students.

We first defined the class of adverse events of interest as "system accidents", distinct from occupational accidents, and having the following characteristics: (1) *temporal depth of causality*: the chain of causality, or chain 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; (2) *diversity of agency*: the safety value chain or the groups and individuals who influence or contribute to the accident occurrence/prevention extend far beyond the immediate victims, who may or may not have contributed to the accident.

We then addressed the question of why the interest in this class of events and their prevention, and we expanded on the importance of safety literacy and the contributions that engineering students can make in the long-term towards accident prevention. The role of engineering education in accident prevention was discussed within the broad concepts of learning loops and safety value chain. It is often said that the best technology transfer mode comes "wearing shoes"; by educating and engaging engineering students in the multidisciplinary issues of accident causation and system safety, educators can help infuse their students, the future contributors, managers, and leaders of technology-intensive or hazardous industries, with a proper safety competence and accident awareness before they enter the workforce, and in so doing, they will contribute, in the long-term, one step towards accident prevention.

Finally, we offered one model for the structure and content of an introductory course on accident causation and system safety. The course starts with the anatomy of accidents and is grounded in various case studies. These are particularly important as they help illustrate the multidisciplinary nature of accident causation and system safety, and they provide the students with the important concepts to describe the phenomenology of accidents (e.g., initiating events, accident precursor or lead indicator, accident pathogen, and accident sequence). The course then proceeds to an exposition of defense-in-depth and safety barriers, which we believe are essential elements for a basic education in accident causation and system safety. The discussion of defense-in-depth and safety barriers addresses two complementary themes in the course, namely technical safety principles and organizational contributions to system safety and accidents. The course ends with a presentation of basic concepts and tools in risk analysis. We conclude the discussion of the course with a mention of broader themes and possible missing ingredients in the course. Other course models are possible, and educators will no doubt recognize the difficulties in designing a new course subject to a variety of constraints. We hope that our course structure and content will invite comments and contributions from the readers, and we hope that this journal will encourage the publications of exchanges on this subject.

Appendix

Assessing the long-term impact of the course on students' contributions to workplace safety would be broadly similar to assessing a workplace safety intervention (see for example Shannon et al. [45]). A safety intervention in the workplace is defined as "any new program, practice, or initiative intended to improve safety" such as a safety training program or a change in safety policies or procedures [42]. In our case, the "intervention" is conducted prior to the target audience reaching the workplace, and as such, its effectiveness and impact on attitudes, behavioral changes, and outcomes would manifest themselves over longer timescales than a typical workplace intervention.

Designing an experimental protocol for such assessment would be challenging, not only because of the long timescales involved, but also because of the many variables and confounding factors that cannot be controlled for (in the classroom and afterwards in the workplace), and the difficulty of having a control group for such an assessment. Nevertheless, a qualitative approach can be developed to follow students who took this course into the workplace, and implement an interview protocol to assess the effect of their safety education on workplace safety issues.

References

[1] ACSNI. Organizing for safety. London: Advisory Committee on the Safety of Nuclear Installations: Study Group on Human Factors; 1993.
[2] Anon. Safety report on the treatment of safety-critical systems in transport airplanes. National transportation safety board report. NTSB/SR-06/02. Washington, DC.
[4] AIChE. Layers of protection analysis: simplified process risk assessment. New York, NY: American Institute of Chemical Engineers: Center for Chemical Process Safety; 2001.
[5] Apostolakis GE. How useful is quantitative risk analysis? Risk Analysis 2004;24(3):515–20.
[6] Bailyn B. On the teaching and writing of history: responses to a series of questions. Hanover, NH: University Press of New England; 1994.
[7] Bakolas E, Saleh JH. Augmenting defense-in-depth with the concepts of observability and diagnosability from control theory and discrete event systems. Reliability Engineering and System Safety 2011;96(1):184–93.

[8] Barnett SM, Ceci SJ. When and where do we apply what we learn? A taxonomy for far transfer Psychological Bulletin 2002;128(4):612–37.
[9] Bransford JD. How people learn: brain, mind, experience, and school. Washington, DC: National Acad. Press; 2001.
[10] Cooper MD. Towards a model of safety culture. Safety Science 2000;36(2): 111–36.
[11] Delatte NJ. Learning from failures. Civil Engineering Practice, Journal of the Boston Society of Civil Engineers Section, ASCE 2006;21(2):21–38.
[12] Delatte NJ. Failure literacy in structural engineering. Engineering Structures 2010;32(7):1952–7.
[13] DOE. Implementation guide for use with DOE order 225.1A, accident investigations, DOE G 225.1A-1. Washington, D.C.: U.S. Department of Energy; 1997.
[14] Duijm NJ. Safety-barriers diagrams as a safety management tool. Reliability Engineering and System Safety 2009;94(2):332–41.
[15] Fahlbruch B, Carroll JS, editors. Safety science, 49; 2011. p. 1–4.
[16] Faust DG. The role of the university in a changing world. Presented at the royal Irish academy. Dublin, Ireland: Trinity College; June 30, 2010.
[17] Guldenmund FW. The nature of safety culture: a review of theory and research. Safety Science 2000;34(1–3):215–57.
[18] Hale AR, de Kroes J. System in safety 10 years of the chair in safety science at the Delft University of Technology. Safety Science 1997;26(1):3–19.
[19] Hale A, Wilpert B, Freitag M. After the event: from accident to organisational learning. Oxford: Pergamon; 1997.
[20] Holloway CM, Johnson CW. Why system safety professionals should read accident reports. In: Proceedings of the first IET international conference on system safety. Savoy Place, London: Institute of Engineering and Technology; 6–8th June 2006.
[21] Johnson CW. Competency management systems to support accident and incident investigators. In: Proceedings of the 29th international systems safety society. Las Vegas, USA; 2011.
[22] Hopkins A. Was the three mile island a "normal accident"? Journal of Contingencies and Crisis Management 2001;9(2):65–72.
[23] Hollnagel E. Barriers and accident prevention. VT: Aldershot Publishing Company; 2004.
[24] Hovden J, Stroseth F, Tinmannsvik RK. Multilevel learning from accidents—case studies in transport. Safety Science 2011;49(1):98–105.
[25] Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Analysis 1981;1(1):11–27.
[26] Kjellen U, Larsson TJ. Investigating accidents and reducing risks—a dynamic approach. Safety Science 1981;3(2):129–40.
[27] Kleindorfer PR, Belke JC, Elliott MR, Lee K, Lowe RA, Feldman HI. Accident epidemiology and the US chemical industry: accident history and worst-case data from RMP*Info. Risk Analysis 2003;23(5):865–81.
[28] Kletz TA. Hazop and hazan: identifying and assessing process industry hazards. 4th ed. Philadelphia, PA: Taylor and Francis; 1999.
[29] Kletz TA. Learning from accidents. 3rd ed. Oxford: Gulf Professional Publishing; 2001.
[30] Leveson NG, Turner CS. An investigation of the Therac-25 accidents. Computer 1993;26(7):18–41.
[31] Leveson NG. A new accident model for engineering safer systems. Safety Science 2004;42(4):237–70.
[32] Melchers RE. On the ALARP approach to risk management. Reliability Engineering and System Safety 2001;71(2):201–8.
[33] US Nuclear Regulatory Commission. Causes and significance of design basis issues at US nuclear power plants. Draft report. Washington, DC: US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research; 2000.
[34] Pate-Cornell E. Learning from the piper alpha accident: a postmortem analysis of the technical and organizational factors. Risk Analysis 1993;13(2):215–32.
[35] Pate-Cornell E. Uncertainties in risk analysis: six levels of treatment. Reliability Engineering and System Safety 1996;54(2):95–111.
[36] Perrow C. Normal accidents: living with high-risk technologies. New York: Basic Books; 1984.
[37] Petroski H. To engineer is human: the role of failure in successful design. NY: First Vintage Books; 1992.
[38] Petroski H. Success through failure: the paradox of design. Princeton, NJ: Princeton University Press; 2006.
[39] Pidgeon N. Safety culture: key theoretical issues. Work and Stress 1998;12(3):202–16.
[40] Rasmussen J. Risk management in a dynamic society: a modeling problem. Safety Science 1997;27(2–3):183–213.
[41] Reason JT. Managing the risks of organizational accidents. VT: Aldershot Publishing Company; 1997.
[42] Robson LS, Shannon HS, Goldenhar LM, Hale AR. Guide to evaluating the effectiveness of strategies for preventing work injuries: how to show whether a safety intervention really works. DHHS (NIOSH) publication no. 2001-119. OH: Center for Disease Control/National Institute for Occupational Safety and Health; 2001.
[43] Saleh JH, Cummings AM. Safety in the mining industry and the unfinished legacy of mining accidents. Safety Science 2011;49(6):764–77.
[44] Saleh JH, Marais KB, Bakolas E, Cowlagi RV. Highlights from the literature on system safety and accident causation: review of major ideas, recent contributions, and challenges. Reliability Engineering and System Safety 2010;95(11):1105–16.
[45] Shannon HS, Robson LS, Guastello SJ. Methodological criteria for evaluating occupational safety intervention research. Safety Science 1991;31(2):161–79.
[46] Shavell S. Risk sharing and incentives in the principal and agent relationship. Bell Journal of Economics 1979;10(1):55–73.
[47] Sklet S. Safety barriers: definition, classification, and performance. Journal of Loss Prevention in the Process Industry 2006;19(5):494–506.
[48] Smyth AW, et al. Probabilistic benefit–cost analysis for earthquake mitigation: evaluating measures for apartment houses in Turkey. Earthquake Spectra 2004;20(1):171–203.
[49] Sorensen JN. Safety culture: a survey of the state of the art. Reliability Engineering and System Safety 2002;76(2):189–204.
[50] Sorensen JN, Apostolakis GE, Kress TS, Powers DA. On the role of defense in depth in risk-informed regulation. In: Proceedings of the international topical meeting on probabilistic safety assessment (PSA). Washington, DC; August 22–26, 1999. p. 408–13.
[51] Sterman JD. Learning in and about complex systems. System Dynamics Review 1994;10(2–3):291–330.
[52] Summers AE. Introduction to layers of protection analysis. Journal of Hazardous Materials 2003;104(1–3):163–8.
[53] Swuste P, Arnoldy F. The safety adviser/manager as agent of organisational change: a new challenge to expert training. Safety Science 2003;41(1):15–27.
[54] Turner BA. Man-made disasters. London, England, New York: Wykeham Publications (London); Crane, Russak; 1978.