AC 2011-1435: SYSTEM SAFETY LITERACY AND MULTIDISCIPLINARY ENGINEERING EDUCATION: TEACHING ACCIDENT CAUSATION AND PREVENTION

Cynthia C. Pendley, Georgia Institute of Technology

Biographical sketch: Cynthia Cox Pendley

Cynthia C. Pendley is a Program Coordinator for the Center for Space Systems in the School of Aerospace Engineering at Georgia Institute of Technology where she has served since 2005. Prior to joining Georgia Tech Ms. Pendley was a product developer at Kimberly-Clark Corporation where she was awarded two patents for specialized filtration products. She received her B.S. in Textiles from Georgia Tech and is currently pursuing a Masters in Educational Psychology at Georgia State University. Ms. Pendley's primary research interest is engineering education, specifically how motivation, interest and cognitive strategies affect problem-solving performance. She is a Senior Member of the American Institute of Aeronautics and Astronautics (AIAA) and the American Society of Engineering Education (ASEE).

Joseph Homer Saleh, Georgia Institute of Technology

Joseph H. Saleh is an Associate Professor of aerospace engineering at the Georgia Institute of Technology. He received his Masters degree from Harvard University and his PhD from the Department of Aeronautics at MIT. Prior to Joining Georgia Tech, Dr. Saleh served as the Executive Director of the Ford-MIT Alliance, a research partnership between MIT and the Ford Motor Company. Dr. Saleh's current research revolves around three broad topics: 1) satellite reliability and multi-state failure analysis, 2) programmatic engineering as it pertains to space programs (including a focus on space responsiveness, schedule risk and slippage, and system obsolescence); and 3) accident causation and system safety. Dr. Saleh is the author or co-author of some 100 technical publications, including two articles in the Encyclopedia of Aerospace Engineering (Wiley) and 44 journal publications. He is an Associate Fellow of the American Institute of Aeronautics and Astronautics (AIAA) and a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE). Dr. Saleh has received several awards for his teaching and mentoring, including the Lockheed Dean's Excellence in Teaching Award (2010) and the Most Valuable Professor (MVP) Award from the School of Aerospace Engineering at Georgia Tech (2008).

SYSTEM SAFETY LITERACY AND MULTIDISCIPLINARY ENGINEERING EDUCATION: TEACHING ACCIDENT CAUSATION AND PREVENTION

1. Introduction: motivation and scope

The recent 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.

In this work, we focus on system accident causation and prevention. Why the interest in this class of adverse events and how can these be characterized?

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. 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 that the propensity of this class of adverse events, namely that system safety education may be limited in effectiveness, not reaching their target audience, or not conducted at a scale commensurate with the importance of the subject.

Three complementary responses address the question of why an interest in accident causation and prevention? These are:
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 accident, 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.

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"[37], and later characterized as "organizational accidents"[30] or "system accidents"[25]. 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"[22], 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".[10] What is distinctive about system accidents is the following:

1. 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. This characteristic can be termed the **temporal depth of causality** of system accidents.

2. The safety value chain (see Fig. 1), 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 (the concept of safety value chain is further explained in Section 2). 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 literacy and contributing, in the long term, to accident prevention. The theme of "learning from accidents" is often explored in the literature.[20,26,27] 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 with a discussion of the role of the University as a stakeholder in system safety literacy.

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: Different academic and professional communities have grappled with the multidisciplinary issues of accident causation and system safety, including psychologists, sociologists, economists, engineers (from various disciplines), and management/organizational scientists. In addition, safety inspectors, accident investigators, lawyers, insurers, policy-makers and regulators are also closely involved in these issues. One of the primary sources of information about an accident, the accident investigation, has both a backward-looking objective to better understand why the event occurred and a forward-looking objective focused on providing recommendations to improve future system safety and accident prevention at the technical, operational, organization and sometimes regulatory levels. Thus learning and the notions of feedback or "learning loops" are intrinsic to accident investigations.[16]
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, "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."[34] 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. But who are these stakeholders? They are the agents who partake in the safety value chain.

2.2 Safety value chain: 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 Figure 1), groups of individuals who affect and contribute to system safety over different time-scales. 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 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 system safety literacy 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.

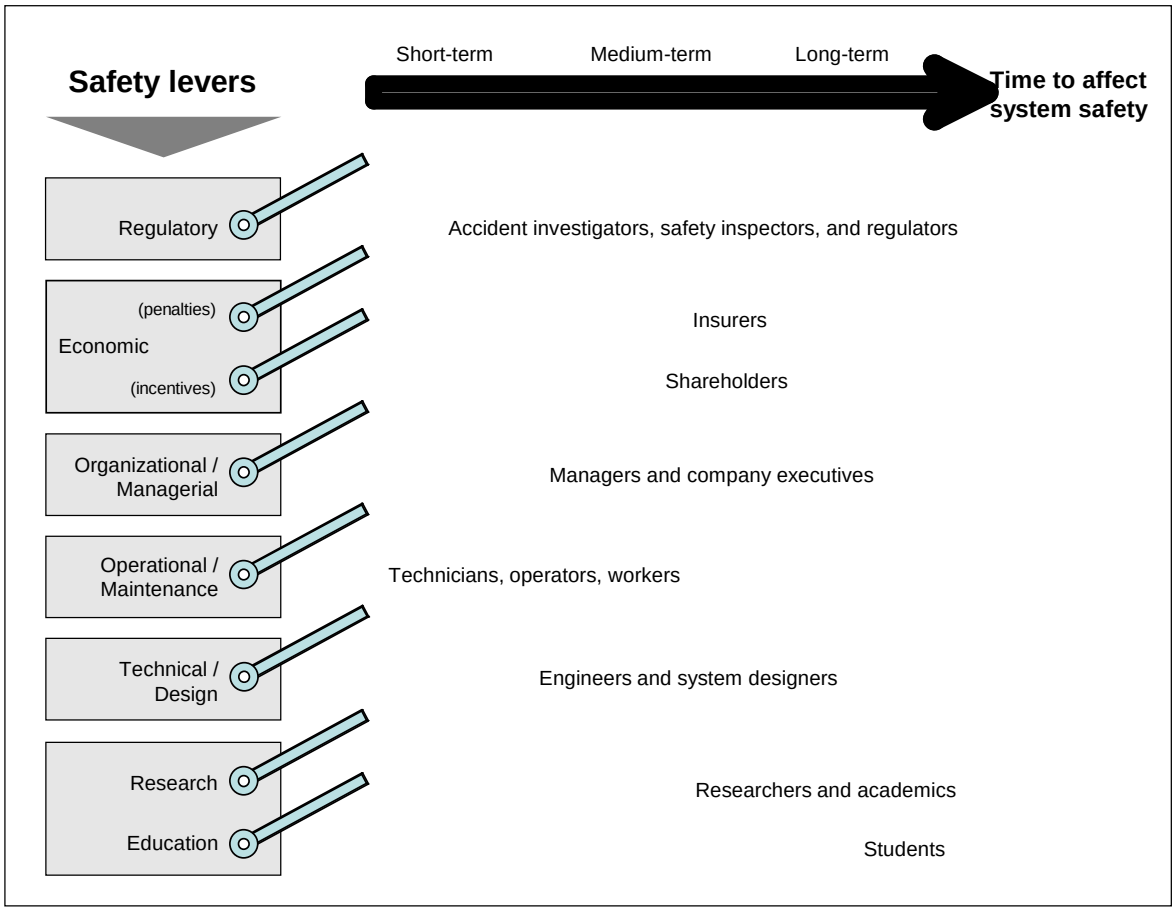

Figure 1. Safety levers and stakeholders in the safety value chain (not meant to be exhaustive)

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, 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; overlap exists between them and they are presented under different sub-heading for clarity purposes.

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 the contributing, in the long term, to accident prevention.

Structural engineering has been a strong proponent of "failure literacy" for engineering students. "This literacy entails knowing about the critical historical failure cases that have shaped the profession", Delatte 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 (1940) and several other bridge and building collapses.[9] In contrast, this work proposes a "system safety literacy" which is developed, in part, by viewing historical failure cases across various industries through a "system" lens, extracting the conceptual sameness that system accidents share and learning how to discuss failure modes using a multidisciplinary language[*].

Petroski has been an early proponent of learning from (structural and mechanical) failures in his landmark book "To Engineer Is Human", in which 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."[26] 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[†].

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 repeat 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.

---

[*] Extensive discussion of the taxonomy of system safety is outside the scope of this work. Some examples of terms which transcend specific engineering disciplines are defense-in-depth, safety barriers, accident pathogens and system accident.

[†] 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].

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 repeat 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 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 subsection, 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"*[15]

This multidisciplinary awareness builds system safety literacy which 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 from different backgrounds.

It was noted in the Introduction of this work that system accidents, also termed "organizational 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 system safety issues from falling through the proverbial organizational cracks.

In addition, teaching engineering students about accident causation and system safety, and the complexities involved, brings up some ethical challenges in the workplace. It invites students to reflect on these ethical challenges, and prepares students to their future ethical responsibilities, in their behavior and decision-making roles in accident prevention.

> *"A key ethical problem can be described as "design process" failures where engineers wrongfully assume that another party will cope with a risk. Engineers must be taught to recognize and deal with ethical problems in product design."*[6]

Swuste and Arnoldy discuss the role of safety advisors/managers in a company as agents of change for improving safety management; the argument in this subsection posits a similar role, although over a longer timeframe, for engineering students.[36]

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[8,14,28]. 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 proper safety culture.

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

Engineering students will often be involved, later in their careers, 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, it can be argued 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. Reflective thinking or metacognition prompts one to engage in an internal dialogue and other self-regulating strategies that promote better problem solving.[21] 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 automatic 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.

[‡] In 2000 the Accreditation Board of Engineering and Technology introduced the requirement of incorporating ethics and professional responsibility into engineering education. This will be discussed in more detail in Section 4.6.

Our academic experience to date suggests there is an unfortunate growing reliability and system 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 teaching and studying 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."*[4]

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".[13]

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, must still 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. Following each lecture module we have identified the specific ABET Criterion 3 student outcomes[§] that are supported by the course instruction and activities. ABET student outcomes will be discussed in more detail in Section 4.6.

We restrict the scope to a one-semester course because in an already crowded engineering curriculum, it is unlikely that this subject, accident causation and system safety, would be given more ample time in a common-core syllabus[**].

In the following, we present one model for the structure and content of such a course. Other models are possible, and educators will no doubt recognize the difficulties in designing a new

---

[§] A complete list of the ABET criterion 3 student outcomes is in the Appendix.

[**] 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, nuclear criticality safety engineering).

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 are that case studies "make schooling more relevant to the subsequent workplace"[7], they offer a wealth of information about context and realistic real-world problems, and they are more engaging and intellectually enriching for students. Educational researchers have noted that when students are encouraged to elaborate on and integrate new information, as occurs in case-based learning, it can result in construction of a distinct new concept or line of reasoning.[24] Many choices of accident case studies are possible. An extensive list can be found in Kletz' "Learning from Accidents" for example.[20] We have selected the following accidents for our course:

1. Piper Alpha
2. Challenger
3. JWR No.5 mine disaster
4. Three Mile Island
5. TWA Flight 800 and Alaska Airline Flight 857
6. Therac-25 accidents

These accidents provide a diverse set of case studies, and they introduce the students to multidisciplinary nature of accident causation and system safety. Each accident highlights particular 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 very important notions of *initiating events*, *accident precursor* or *lead indicator*, and *accident pathogen*. Case studies help students better understand and appreciate abstractions and concepts such as these, concepts that we believe are essential elements for system safety literacy. In addition, these case studies help students better appreciate the notions of safety levers and safety value chain discussed in Section 2.

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 a week ahead of each discussion:

- Pate-Cornell, E. "Learning from the Piper Alpha accident: A postmortem analysis of the technical and organizational factors." Risk Analysis, vol. 13, No. 2, 1993, pp. 215–232.
- Hopkins, A. "Was the Three Mile Island a "Normal Accident?" Journal of Contingencies and Crisis Management, Vol. 9, No. 2, 2001, pp. 65–72.

- Leveson, N. G., Turner, C. S. “An investigation of the Therac-25 accidents.” Computer Vol. 26, No. 7, 1993, pp. 18-41.
- The Jim Walter Resources (JWR) No. 5 mine disaster. Personal notes.
- Anon. “Safety report on the treatment of safety-critical systems in transport airplanes”. National Transportation Safety Board report, NTSB/SR-06/02. Washington, DC.

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, 2001)
- Challenger: Go for Launch (BBC documentary, 2001)

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 accidents 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.

Criterion 3 student outcomes: a, c, e, f, g, h, i, j, k

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.

[††]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[23], and it is recognized under various names in other industries (e.g., *layers of protection* in the chemical industry.[3,19,35] Accidents typically result from the absence or breach of defenses or violation of safety constraints.[22,29,18] 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”[11] along potential accident sequences.

[††] This paragraph is an excerpt from a discussion in Saleh *et* al., 2010.

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. The previous case studies (subsection 4.1) provide the students with a solid basis for understanding accident sequences (hazard escalation) 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 automatic 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.

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

- Sklet, S. "Safety barriers: Definition, classification, and performance." Journal of Loss Prevention in the Process Industry, Vol. 19, No. 5, 2006, pp. 494–506.
- Duijm, N. J. "Safety-barriers diagrams as a safety management tool." Reliability Engineering and System Safety, Vol. 94, No. 2, 2009, pp. 332–341.
- Sorensen, J.N., Apostolakis, G. E., Kress, T.S., and Powers, D.A., "On the Role of Defense in Depth in Risk-Informed Regulation." Proceedings of PSA '99, International Topical Meeting on Probabilistic Safety Assessment, pp. 408-413, Washington, DC, August 22 - 26, 1999.
- Bakolas, E., Saleh, J. H. "Augmenting defense-in-depth with the concepts of observability and diagnosability from Control Theory and Discrete Event Systems." Reliability Engineering and System Safety, Vol. 96, Issue 1, 2011, pp. 184–193[‡‡].

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 safety and accidents.

Criterion 3 student outcomes: g, h, j

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). And 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:

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

- Kaplan, S., Garrick, B. J., "On the quantitative definition of risk." Risk analysis, Vol. 1, No. 1, 1981, pp. 11–27.
- Pate-Cornell, E., "Uncertainties in risk analysis: Six levels of treatment." Reliability Engineering and System Safety, Vol. 54, No. 2, 1996, pp. 95–111.
- Apostolakis, G. E. "How useful is Quantitative Risk Analysis?" Risk Analysis, Vol. 24, No. 3, 2004, pp. 515–520.
- Rasmussen, J., "Risk management in a dynamic society: A modeling problem." Safety Science, Vol. 27, No. 2/3, 1997, pp. 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 touched upon.

Criterion 3 student outcomes: a, c, e, k

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 parameters and 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;
- Role of software in system accidents;
- 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[§§] principle;

Time permitting, the last two themes have occasionally been broached in class, but not in an in-depth way, through the discussion of the following articles (a more extensive bibliography is provided to the students):

1. Sorenson, J. N. "Safety culture: A survey of the state of the art." Reliability Engineering and System Safety, Vol. 76, Issue 2, 2002, pp. 189–204.
2. Smyth, A. W. *et* al., "Probabilistic benefit-cost analysis for earthquake mitigation: Evaluating measures for apartment houses in Turkey." Earthquake Spectra, Vol. 20, No. 1, 2004, pp. 171–203.
3. Melchers, R. E. "On the ALARP approach to risk management." Reliability Engineering and System Safety, Vol. 71, Issue 2, 2001, pp. 201–208.

We have not yet managed to explore the remaining themes in class. We are still being debated whether they fit in a one-semester course on accident causation and system safety, and if they

[§§] As Low As Reasonably Practicable.

can be taught in a manner that is relevant and addresses fundamentals points, but does not delve into details that are more appropriate in more specialized graduate courses.

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; 2) it requires them to identify and synthesize key ideas in their readings which helps prepare 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.[17] 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 an analysis of particular events or topics.

Criterion 3 student outcomes: f, g, h, j, k

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

4.6 Assessment and Evaluation

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.[5] But the short-term evaluation of the teaching effectiveness is covered by anonymous surveys that students complete 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; absence of important accidents in the case studies (Chernobyl was noted repeatedly); some students wrote that more case studies were needed, while others suggested that fewer case would do; and some students asked that fewer reading and writing assignments and a couple of analytical homeworks in their stead. These comments are carefully reviewed and some changes to the course are considered. Some of the criticism, however, reflects the diversity of interest and background of different students, and in multidisciplinary courses such as the one here discussed, it may not be possible to tailor a course 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.

ABET's Criterion 3 student outcomes were noted for each lecture module. ABET criteria contains 6 subsequent criterions that are used as the standard by which engineering programs are accredited. Criterion 3 focuses on student outcomes that should be attained prior to graduation. Each engineering program develops its own strategy for how its curriculum addresses these outcomes and properly prepares students for professional careers. The model course proposed in this work, using Criterion 3 as a basis for evaluation, seems to do an adequate job of exposing students to many of the student outcomes; some are explored in depth as is discussed in the following paragraphs.

A consistent theme in this work has been the importance of multiple channels of communication (Criterion 3g) – within companies to establish a proper safety culture, between stakeholders to discuss and resolve system safety issues, and as advocates for regulatory involvement when safety considerations may have been overlooked. Effective multidisciplinary communication is both why we teach and what we teach students in system safety education. Through case study analyses of accidents students learn that poor communication can become an accident pathogen. As students are prompted to facilitate class discussions about accidents, explaining and defending their viewpoints, they learn how to express themselves in the multidisciplinary language of system safety. And finally, through the multiple writing assignments, students gain experience in communicating effectively which is a necessary skill for their future careers (Criterion 3k).

When the National Academy of Engineering introduced the National Grand Challenges in 2010 to help prepare students for the 21st century, they cited the following as one of the goals: "Underscore the importance of recognizing that engineering education must be coupled to policy/ business/ law and must be student-focused". A similar concept is echoed in this student outcome (Criterion 3h) which states "the broad education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context. No single course can accomplish such a broad and complex outcome, but we do believe that system safety education makes an important contribution toward this goal. By introducing students to the multidisciplinary nature of accident causation and system safety, they gain a better understanding of the tools needed to reduce the frequency of system accidents. At the same time they become aware, as stakeholders, of their own agency in both the challenges and the solutions, broadening their perspective to the global, economic, environmental and societal context. As stated earlier, we view this introductory course in accident prevention and system safety as the first installment in what we hope will be a lifelong commitment of future engineers to continue to grow in their understanding of the complexities of accident prevention and system safety (Criteria 3i).

5. The University's role as a stakeholder in system safety literacy

In section 2 we referenced the role of the University as a stakeholder in the safety value chain with relationships on both sides, the students on the one hand, balanced by the remaining stakeholders such as managers, government agencies and others. We also discussed the benefits

of extending the learning loop to the students, which is facilitated at the university level. In section 3 we proposed several arguments for why engineering students should be taught about accident causation and system safety and in section 4 we presented an introductory course to serve as a model for the content and delivery of this subject matter to students. In this way we have defined an important role of the university - educating and nurturing engineering students in the issues of accident prevention and system safety. In addition to its role in the classroom we also argue that the university can play a leadership role in connecting academia with other stakeholders, thus reinforcing learning loops. We encourage all stakeholders in the safety value chain to reflect on the value of these recommendations and consider how they might be implemented.

1.[***] More fundamental research and cross-talk across several academic disciplines (especially between systems engineering, computer science, psychology, and organizational sciences) must be supported and incentivized for tackling the multi-disciplinary issues of accident causation and system safety. The creation of "academic hubs" and collaborative environments for a diverse group of academics to address system safety issues would be an especially powerful tool in the "safety war". Research funding agencies, such as the National Science Foundation (NSF) and the National Institute of Occupational Health and Safety (NIOSH) in the United States can play a major role in supporting these "academic hubs" or "centers of excellence" dedicated to system safety.

2. More interactions and partnerships between academia and various sectors on accident causation and system safety issues would be useful for all involved in advancing the safety agenda, from both research and (continuing) education perspectives, and for disseminating research results, safety recommendations, and lessons learned from accident investigations. In addition, partnerships between academia and accident investigation agencies, such as the National Transportation and Safety Board (NTSB) in the United States, would be extraordinarily useful in bringing the reality of accidents to the academic environment and helping guide research in this area.

6. 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 safety 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; and 2) Diversity of agency: The safety value chain or the groups and individuals who influence or contribute to the

[***] These two recommendations are made in a discussion in Saleh et al., 2010.

accident occurrence/prevention, extends 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 system 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.

A model for the structure and content of an introductory course on accident causation and system safety was outlined. The course starts with the anatomy of accidents and is grounded in various case studies. It 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 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. Following each lecture module the applicable student outcomes from ABET's Criterion 3 were noted and later discussed. 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 the editor(s) of this journal will encourage the publications of exchanges on this subject.

Finally we discussed the role of the University as a stakeholder in system safety literacy. We argued that the university's role is composed of two primary components: 1) the education of engineering students in accident prevention and safety competence 2) outreach to other stakeholders in the safety value chain. The first component was discussed in detail in Sections 3 and 4. We expounded on how this outreach could be structured in two recommendations: 1) more fundamental research and cross-talk across academic disciplines 2) partnerships between academia and other sectors on accident causation and system safety issues for the purpose of advancing the safety agenda.

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.

References

1. ACSNI. Organizing for safety. London: Advisory Committee on the Safety of Nuclear Installations: Study Group on Human Factors; 1993
2. Adam J.M. Francisco J.P.(Eds.) Learning from Structural Failures. Engineering Structures 2010:32(7) 1791-1956.

3. AICHE. Layers of Protection analysis: simplified process risk assessment. New York, NY: American Institute of Chemical Engineers: Center for Chemical Process Safety; 2001.
4. Bailyn B., E.C.Lathem(Ed.) On the teaching and writing of history: responses to a series of questions. Hanover, NH: Montgomery Endowment, Dartmouth College, University Press of New England;1994.
5. Barnett, S. M., Ceci, S. J. When and Where Do We Apply What We Learn? A Taxonomy for Far Transfer. Psychological Bulletin 2002: 128(4) 612– 37.
6. Brannigan, V.M.; , "Teaching ethics in the engineering design process: a legal scholar's perspective," Frontiers in Education, 2003. FIE 2003. 33rd Annual , vol.3, no., pp. S2A- 19-24 vol.3, 5-8 Nov. 2003 doi: 10.1109/FIE.2003.1265936
7. Bransford, J. D. How People Learn: Brain, Mind, Experience, and School. Washington, DC: National Acad. Press, 2001. Print.
8. Cooper, MD. Towards a model of safety culture. Safety Science 2000:36(2):111-36.
9. Delatte NJ. Learning from failures. Civil Engineering Practice, J Boston Soc Civ Eng Sect, ASCE 2006;21(2):21_38. Boston, MA, F/W 2006.
10. 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.
11. Duijm NJ. Safety-barriers diagrams as a safety management tool. Reliability Engineering and System Safety 2009:94(2):332–41.
12. Fahlbruch B. Carroll J.S.(Eds.) "The gift of failure: New approaches to analyzing and learning from events and near misses." – Honoring the contributions of Bernhard Wilpert. Safety Science 2011:49(1):1-4.
13. Faust, D.G. The Role of the University in a Changing World. Presented at the Royal Irish Academy, Trinity College; Dublin, Ireland; June 30, 2010.
14. Guldenmund FW. The nature of safety culture: a review of theory and research. Safety Science 2000:34(1-3):215-57.
15. Hale A.R. de Kroes J. System in Safety 10 years of the chair in safety science at the Delft University of Technology. Safety Science 1997:26:26(1):3-19.
16. Hale, A., Wilpert, B., & Freitag, M. After the event: From accident to organisational learning. Oxford: Pergamon; 1997.
17. Harvey, G. "Writing with sources: a guide for students." Hackett Publishing Company, Indianapolis IN/ Cambridge MA, 1998.
18. Hollnagel E. Barriers and accident prevention. Aldershot, Hampshire, England; Burlington, VT: Ashgate; 2004.
19. Kletz TA. Hazop and hazan: identifying and assessing process industry hazards. 4th ed.. Philadelphia, PA: Taylor & Francis; 1999.
20. Kletz, T. A., & ScienceDirect (Online service). Learning from accidents. Oxford: Gulf Professional; 2001.
21. Kuiper R.A. and Pesut D.J. Promoting cognitive and metacognitive reflective reasoning skills in nursing practice: self-regulated learning theory. Journal of Advanced Nursing: 2004; 45(4): 381–391.
22. Leveson NG. A new accident model for engineering safer systems. Safety Science 2004;42(4):237-70.
23. N.R.C., US 2000. 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.
24. Ormrod, J.E. Human Learning. 5th ed. Upper Saddle River, New Jersey: Pearson; 2008.
25. Perrow C. Normal accidents: living with high-risk technologies. New York: Basic Books; 1984.
26. Petroski, H. To Engineer is Human: the role of failure in successful design. 1st Vintage Books Ed.; 1992. Originally published in hardcover, in somewhat different form, by St. Martin's Press, New York, in 1985.
27. Petroski, H. Success through Failure: the paradox of design. Princeton, NJ: Princeton University Press; 2006.
28. Pidgeon N. Safety culture: key theoretical issues. Work and Stress 1998:12(3):202-16.
29. Rasmussen J. Risk management in a dynamic society: A modeling problem. Safety Science 1997: 27(2-3): 183–213.
30. Reason JT. Managing the risks of organizational accidents. Aldershot, Hants, England; Brookfield, Vt., USA: Ashgate; 1997.
31. Saleh, J. H., Marais, K. B., Bakolas, E., Cowlagi, R. V. 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):1105–1116.
32. Society of Manufacturing Engineers Education Foundation, Manufacturing Education Plan: Phase I Report - Industry Identifies Competency Gaps Among Newly Hired Engineering Graduates, Dearborn, MI, Society of Manufacturing Engineers, 1997.

33. Sorensen JN, Apostolakis GE, Powers DA. On the role of safety culture in risk- informed regulation. In: Kondo S, Furuta K, editors. Psam 5: Probabilistic Safety Assessment and Management, vols. 1–4; 2000. p. 2205–10. p.
34. Sterman, J. D. Learning in and about complex systems. Cambridge, Mass: Alfred P. Sloan School of Management, Massachusetts Institute of Technology;1994.
35. Summers AE. Introduction to layers of protection analysis. Journal of Hazardous Materials 2003:104(1–3):163–8.
36. 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.
37. Turner BA. Man-made disasters. London, England, New York: Wykeham Publications (London); Crane, Russak; 1978.

Appendix

Criteria for Accrediting Engineering Programs
Effective for Evaluations during the 2011-2012 Accreditation Cycle
ABET Engineering Accreditation Commission

"Student Outcomes" describe what students are expected to know and be able to do by the time of graduation. These relate to the skills, knowledge, and behaviors that students acquire as they progress through the program.

Criterion 3. Student Outcomes
The program must have documented student outcomes that prepare graduates to attain the program educational objectives.
Student outcomes are outcomes (a) through (k) plus any additional outcomes that may be articulated by the program.

a) an ability to apply knowledge of mathematics, science, and engineering
b) an ability to design and conduct experiments, as well as to analyze and interpret data
c) an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability
d) an ability to function on multidisciplinary teams
e) an ability to identify, formulate, and solve engineering problems
f) an understanding of professional and ethical responsibility
g) an ability to communicate effectively
h) the broad education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context
i) a recognition of the need for, and an ability to engage in life-long learning
j) a knowledge of contemporary issues
k) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice.