Perspective

Systemic Failures: Challenges and Opportunities in Risk Management in Complex Systems

Venkat Venkatasubramanian
Laboratory for Intelligent Process Systems, School of Chemical Engineering,
Purdue University, West Lafayette, IN 47906

DOI 10.1002/aic.12495
Published online November 30, 2010 in Wiley Online Library (wileyonlinelibrary.com).

Keywords: risk analysis and management, process safety, systemic risks, complex systems, financial disasters

Introduction

The BP Deepwater Horizon oil spill disaster has reminded us, once again, the fragility of complex engineered systems. We have been here before but we do not seem to have learnt all the important lessons yet. This is a Santayana moment — "Those who cannot learn from the past are condemned to repeat it!"

In the history of chemical plant accidents, a few disasters have served as wake up calls. The Flixborough accident in the U.K. in 1974, where a Nypro plant explosion killed 26 people, was one such call. The worst was Union Carbide's Bhopal Gas tragedy, in 1984, in which some 5000–25,000 were killed, and about 120,000–500,000 were seriously injured by the accidental release of methyl isocynate (Jasanoff, 1994). Another important one was Piper Alpha, an offshore oil platform operated by Occidental Petroleum in the North Sea, U.K., which exploded in 1988 killing 167 people and resulted in about $2 billion losses (Piper Alpha, 2005). Even though the human casualties were low, this list would also include the 1989 Exxon Valdez oil spill and, now, the BP oil spill, both of which are very serious from an environmental damages perspective.

Such systemic failures are not limited to the chemical and petrochemical industries alone. The Northeast electrical power blackout (Fox-Penner, 2004; LaPedis, 2004) and Schering Plough's inhalers recall (Simons, 2002) are systemic failures. Financial disasters such as Enron, WorldCom, subprime mortgage derivatives market (Plotz, 2002; Johnson and Neave, 2007), Madoff Ponzi scheme (Markopolos, 2010), as well as some other events also belong to the same class (see Table 1).

V. Venkatasubramanian's e-mail address is venkat@ecn.purdue.edu.

© 2010 American Institute of Chemical Engineers

While these are different disasters that happened in different domains, in different facilities, triggered by different events, involve different ingredients, and so on, there are, however, certain common underlying patterns behind such systemic failures. There is an alarming sameness about such major accidents, which underscores important fundamental lessons that need to be learned in order to prevent such events from recurring.

To understand these patterns and learn from them, one needs to go beyond analyzing them as independent one-off accidents, and examine them in the broader perspective of the potential fragility of all complex engineered systems. One needs to study all these disasters from a common systems engineering perspective, so that one can thoroughly understand the commonalities as well as the differences, in order to better design and control such systems in the future. Furthermore, such studies need to be carried out in concert with public policy experts, so that all the scientific and engineering lessons get translated into effective policies and regulations. All these have important implications for process systems engineering research and teaching, as outlined in this perspective article.

Different Disasters, Different Domains, but Similar Patterns

Typically, systemic failures occur due to fragility in complex systems. Modern technological advances are creating a rapidly increasing number of complex engineered systems, processes, and products, which pose considerable challenges in ensuring their proper design, analysis, control, safety, and management for successful operation over their life cycles. It is their scale, nonlinearities, interconnectedness, and interactions with humans and the environment that can make these

Table 1. Examples of Systemic Failures in Various Domains

Chemical	*BP Oil Spill* (*2010*): Off-shore oil platform explosion leading to a large oil spill: 11 people killed; > \$20 bilion losses; incalculable damage to the environment
	BP Texas City (*20O5*): Explosion in the isomerization unit; 15 people killed; ~180 people injured; \$10 billion law suit pending
	Exxon Valdez (*1989*): Oil tanker accident; ~\$1 billion in losses in law suits/fines
	Piper Alpha Disaster (*1988*): Occidental Petroleum's off-shore oil platform explosion; 167 killed; ~2 biilion in losses
	BhopalGas Tragedy (*1984*): Methyl isocyanate leak at Union Carbide's pesticide plant; 5000-15,000 killed; ~120,000 injured; ~1 billion in losses; Worst ever industrial disaster
Electrical	*North East Power Blackout* (*2003*): Massive power outage that affected an estimated 10 million people in Ontario and 45 million people in eight states in the U.S. ~\$6 billion in losses
Mining	*Massey Energy* (*2010*): W. Virginia mine explosion; 29 killed; worst mine disaster in four decades; ~\$130 million in losses
Pharmaceutical	*Schering Plough Inhalers Recall* (*2002*); 59 million inhalers for treating asthma were recalled; \$500 million in fines; largest in FDA history
Financial	*Madoff Scandal*(*2008–09*): Outright fraud; Ponzi scheme; estimated \$65 billion in losses; thousands of investors defrauded
	Subprime mortgage (*2007–08*): Caused by the end of the real estate bubble; precipitated a global financial crisis; trillions of dollars in losses; required governmental rescues in several countries
	Lehman Bros (*2008–09*): Collapse of a 158 year old tony Wall Street firm; one of the largest bankruptcies in the US, triggered by excessive risk taking and the collapse of the subprime mortgage market; ~26,000 employees lost their jobs
	WorldCom (*2002*): Accounting fraud; ~\$180 billion in market value lost; 57,000 employees lost their jobs; billions of dollars lost in retirement savings
	Enron (*2001*): Outright fraud – overstatement of profits through off-the-books partnerships aided by its auditor Arthur Andersen; one of the largest bankruptcies in the US; ~\$60 billion in market value destroyed; 20,000 employees lost their jobs; billions of dollars lost in retirement savings
	Savings and Loan (*1980s*): Caused by deregulation and real estate speculation; about 1000 S&L companies failed; ~\$160 billion in losses, bailed out by the U.S. tax payers
Societal	*Collapse of Mayan Civilization* (*~800–900 AD*): Several theories have been offered; most notable is environmental/ecological collapse
	Easter Island Civilization (*~1500 AD*): Several theories have been offered; most notable is environmental/ecological collapse

systems-of-systems fragile, when the cumulative effects of multiple abnormalities can propagate in numerous ways to cause systemic failures. In particular, the nonlinear interactions among a large number of interdependent components, and the environment, can lead to "emergent" behavior – i.e., the behavior of the whole is more than the sum of its parts, that can be difficult to anticipate and control. This is further compounded by human errors, equipment failures, and dysfunctional interactions among components and subsystems that make systemic risks even more likely if one is not vigilant all the time.

Postmortem investigations of many disasters have shown that systemic failures rarely occur due to a single failure of a component or personnel. Even though the senior management of a company typically tries to spin the blame on some unanticipated equipment failure, operator error, or rogue trader, this is rarely the case for major disasters. For instance, Union Carbide initially claimed that the Bhopal Gas tragedy was caused by a disgruntled employee, who had sabotaged the equipment (Jasanoff, 1994). Enron management initially blamed Andrew Fastow, Enron's CFO, as the sole culprit (Plotz, 2002). However, again and again, investigations have shown that there are always several layers of failures, ranging from low-level personnel to senior management to regulatory agencies, which have led to major disasters. Some typical examples of such failures are listed in Table 2.

Such investigations have shown that the safety procedures had been deteriorating at the failed facilities for weeks, if not for months, prior to the accident. For example, in the case of Piper Alpha, the Permit-to-Work system had been dysfunctional for months (Piper Alpha, 2005). In Bhopal, regular maintenance of safety backup systems had not been conducted for months (Jasanoff, 1994). Massey Energy ran up about 600 safety violations in its Upper Big Branch mine in 2009 and 2010 (MSNBC, 2010). OSHA statistics show that BP ran up 760 "egregious, willful" safety violations during 2008–2010 in Ohio and Texas. Compare this with the corresponding numbers for the other oil companies: Sunoco (8), Conoco-Phillips (8), Citgo (2), and Exxon (1) (Thomas et al., 2010). These are clear evidence of a breakdown of the corporate safety culture. One sees the same patterns in financial disasters as well. For example, in Enron, its senior management, led by Ken Lay and Jeff Skilling, created an extreme performance-oriented culture that seems to have tolerated unethical behavior, which resulted in many violations, market manipulations, and so on (Plotz, 2002). Thus, it was not a question of *if* a disaster would occur at these companies, but *when*.

Another common pattern is that people had not identified all the serious potential hazards. They had often failed to conduct a thorough process hazards analysis that would have exposed the serious hazards, which resulted in the disasters later. Such incomplete hazards analysis was highlighted in the Cullen enquiry of Piper Alpha (Piper Alpha, 2005), and was partially responsible for the meltdown of Bear, Stearns & Co., Lehman Brothers, Merrill Lynch, among others in the subprime market fiasco (Johnson and Neave, 2007). However, the few who had performed more thorough hazards analysis saw the crash coming and profited billions of dollars, as described in Michael Lewis' book *The Big Short*.

Yet another common cause is the inadequate training of the plant personnel to handle serious emergencies. All in all, typically, the responsibility for a systemic failure goes all the way to the top levels of company management, who had only paid a lip service to safety, tolerated noncompliant behavior, even encouraged excessive risk taking, all of which resulted in a poor corporate culture of safety (Olivea

Table 2. Some Typical Examples of Failures at Various Levels in a Systemic Failure

Individuals	• Poor operator training or inexperienced operators leading to human errors • Not enough personnel due to downsizing
Equipment	• Poor maintenance and wear-and-tear leading to equipment failure • Wrong material, capacity, or equipment
Procedures	• Standard operating procedures not followed, workers make up their own or perform short cuts • Past mini-accidents and warnings ignored • Process hazards analysis (PHA) not conducted thoroughly • Poor emergency planning and training
Safety Systems	• Safety systems not tested and maintained properly • Back-up and/or emergency systems not on automatic but on manual
Management	• Failure in communication between ranks • Safety is not made priority #1, cost cutting is • Senior management lacking the background to appreciate the risks inherent in complex process plants – too much emphasis on financial spreadsheets and not enough on process flowsheets • "Performance at all costs" culture encouraging excessive risk taking and unethical behavior among its employees
Corporate Board	• Rewarding short term performance instead of long term • Setting up perverse incentives that are detrimental to the long term survival of the company
Government: Policies and Regulators	• Laissez-faire regulatory policies, reliance on self policing • Policies not strictly enforced due to limited resources or inherent conflict of interests of the regulatory bodies (as seen in SEC and MMS)
National: Political	• Anti-government or anti-regulations sentiment dominant • Sustainability warnings ignored • Celebration of greed

et al., 2006; Baker Panel, 2007; Hopkins, 2009), which in turn paved the way for the disasters.

Despite all this, it is imperative to also consider the ineffectiveness of the regulatory, rating, and auditing agencies. All these were significant culprits in recent disasters. First and foremost, it does not matter whether the systems are chemical, petrochemical, or financial — *self-policing* does not work. This seems so obvious that people should not have to die, or lose all their money, to make us realize this. Sensible regulations are essential, but, more importantly, they must be audited and enforced by suitably trained personnel who have *no conflicts of interest*. The betrayal of public trust by Arthur Andersen, the supposedly independent auditor of Enron, who's aiding and abetting of Enron's cooked books was instrumental in its systemic failure (Plotz, 2002). The subprime market failures showed us that the rating agencies, which were supposed to make an independent assessment of the subprime-mortgage-backed securities, were so dependent on their Wall Street clients for their business that they merrily went stamping AAA ratings on junk. Of the AAA-rated securities issued in 2006, an astonishing 93% have now been downgraded to junk status (Krugman, 2010).

It is the same lesson one is now taught by the BP Deepwater Horizon oil spill — how the Minerals Management Service was inherently conflicted between its goals of awarding leases and enforcing safety regulations (Urbina, 2010). However, this lesson should have been learnt a long time ago after the Piper Alpha disaster. Based on the Cullen report's findings in 1988, the British government moved the responsibility for safety oversight from the Department of Energy to the Health and Safety Executive (HSE), the independent watchdog agency for work related health, safety and illness. A separate division was created within the HSE to monitor safety of the offshore oil and gas industry (Piper Alpha, 2005).

Indeed, the importance of addressing nontechnical common causes, as those described earlier, as an integral part of Systems Safety Engineering, was pointed out as far back as 1968 by Jerome Lederer, the former director of the NASA Manned Flight Safety Program for Apollo, who wrote: "System safety covers the entire spectrum of risk management. It goes beyond the hardware and associated procedures to system safety engineering. It involves: attitudes and motivation of designers and production people, employee/management rapport, the relation of industrial associations among themselves and with government, human factors in supervision and quality control, documentation on the interfaces of industrial and public safety with design and operations, the interest and attitudes of top management, the effects of the legal system on accident investigations and exchange of information, the certification of critical workers, political considerations, resources, public sentiment and many other nontechnical but vital influences on the attainment of an acceptable level of risk control. These nontechnical aspects of system safety cannot be ignored''.

Conceptual Challenges for Systems Engineers

Addressing all aspects of systemic failures and drawing appropriate lessons from them requires tackling this problem at all the levels outlined in Table 2. The challenges can be broadly classified into the following six categories: (1) *technological* — e.g., processing equipment, computing hardware and software; (2) *personnel* — quantity and quality of the work force; (3) *procedures* — standard operating procedures, best practices, etc.; (4) *management and culture* — communication, priorities, incentives, resources, safety culture, etc.; (5) *regulatory* —

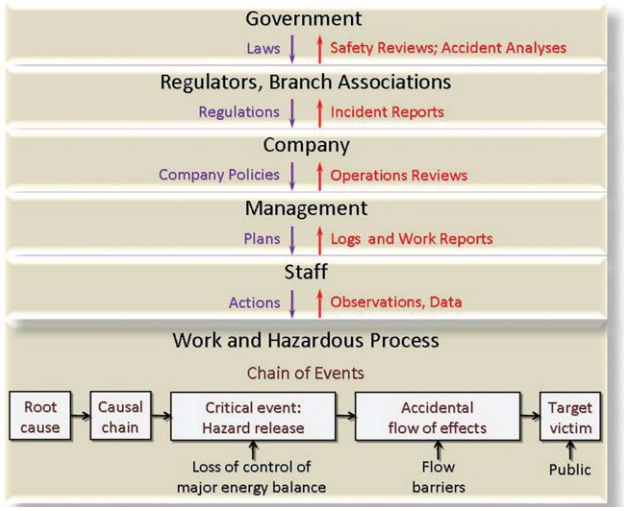

Figure 1. Socio-technical model of system operations (adopted from Rassmusen and Svedung, 2000).

effectiveness, conflict of interest, enforcement, etc.; and (6) *conceptual* — intellectual challenges.

While all these are important, and must all be addressed, this perspective will only focus on the conceptual challenges, as this is where academic researchers and educators can have the most impact. However, it is important to teach the students the other aspects as well and present a more complete and balanced picture. This instructional mission will be addressed in the next section.

As Rasmussen and Svedung (2000) have proposed, one needs a systems engineering view of risk management that addresses both the social and technical aspects of the overall problem. Figure 1 shows their socio-technical model of system operations.

Leveson has further developed this concept in her STAMP (Systems-Theoretic Accident Model and Processes) framework, shown in Figure 2 (Leveson, 2004). These approaches recognize the importance of the (1) integration of technical and social elements, (2) multilayer structure of feedback control mechanisms, (3) distributed monitoring functions at each layer, (4) distributed action functions at each layer, (5) preconditions for the operations at each layer, and (6) the overall interactions between the system and its environment in determining the degree of inherent risk and the associated safety of the overall system.

As these frameworks suggest, what might be a "complicated" system (which, at least in principle, can be modeled and analyzed given enough computational tools and time) can become a "complex" system that is potentially intractable due to the scope for dysfunctional interactions. Taking an algorithmic perspective, one may view this as polynomial vs. nonpolynomial (P vs. NP) level of difficulty in computational analysis. Thus, complex unsafe situations are likely to arise from undesirable and dysfunctional interactions among

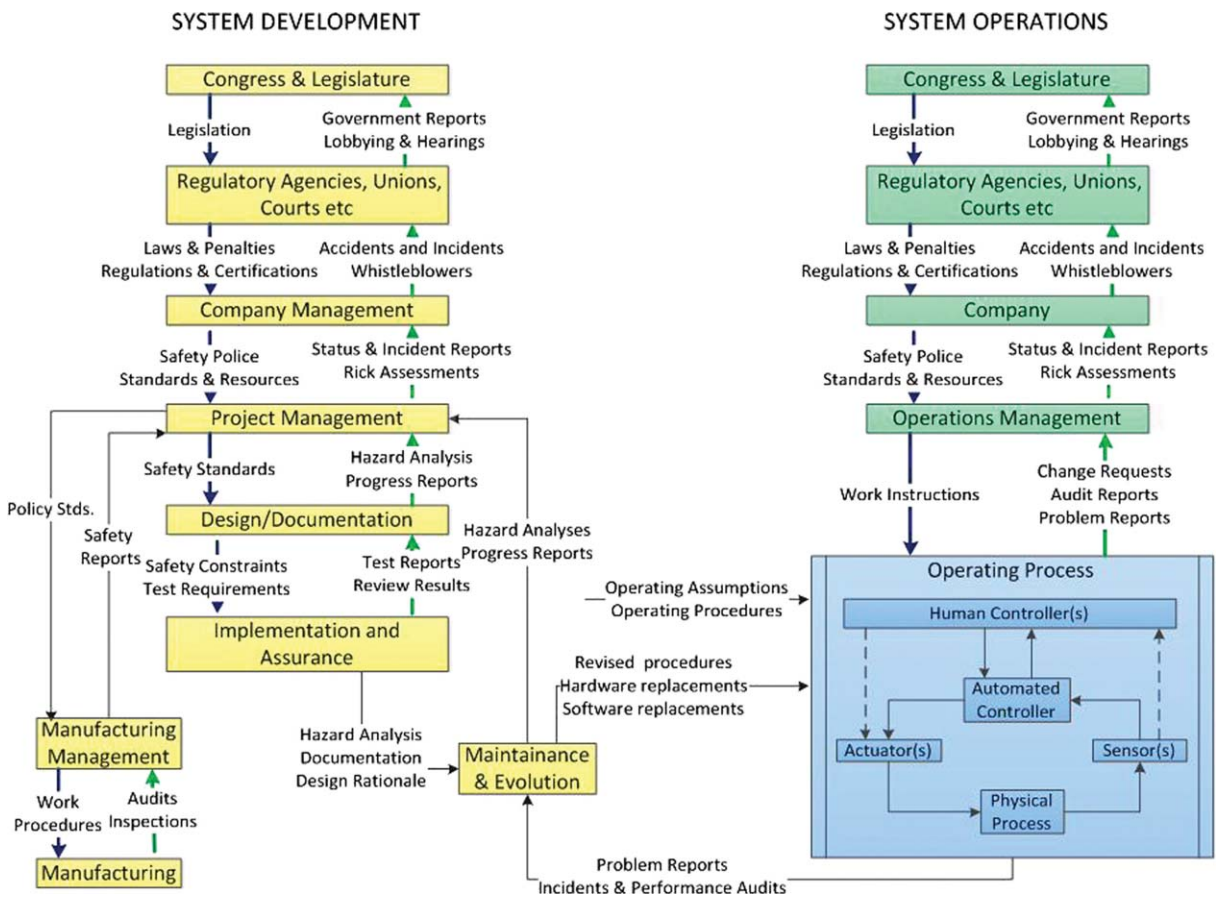

Figure 2. General form of a model of socio-technical control (adopted from Leveson, 2004).

the components, subsystems, feedback loops, humans, and the environment — not just from the failure of a single component or an operator mistake. These figures illustrate the enormity in the number of such interactions that need to be considered in process safety engineering and the challenges one faces at several levels.

Clearly, to cope with such complexity one needs concepts, methodologies, and automation tools to model, analyze, predict, explain, and control the behavior of such a system and its components in various environments. While there exists considerable literature on various methodologies from reliability engineering, such as fault tree analysis (Lapp and Powers, 1977), probabilistic risk assessment (Henley and Kumamoto, 1991; Pariani et al., 2010), failure mode and effects analysis (FMEA), process hazards analysis (Venkatasubramanian et al., 2000), etc., which do help in addressing some of these questions, further progress is needed to address newer aspects of the complexity in these systems-of-systems. The intellectual challenges associated with these questions can be categorized into three broad classes of conceptual problems: (1) complexity science, (2) multiperspective modeling, and (3) hybrid intelligent systems for real-time decision-making. Given the constraints of this *Perspective* article, only the key points will be briefly summarized here and the interested reader will be referred to more detailed discussions in the references cited below.

Complexity science

One central lesson that has come through from systemic failures is the need for a prognostic approach with which one can anticipate problems, rather than relying on the current "react-and-fix" methodology for managing systemic risks. In other words, one needs real-time intelligent decision support systems that can effectively monitor various aspects of process operations, and detect, diagnose and advise operators and engineers about incipient abnormal events. Such systems can be invaluable also in the design stage where they can be used in identifying potential hazards in the proposed design. However, in order to get there one needs to address first the crucial conceptual challenge of being able to predict how changes or dysfunctional interactions in a complex engineered system or its environment would propagate through the entire system — i.e., how does one systematically identify all potential hazards in a complex system and its environment under various conditions (Venkatasubramanian et al., 2000)? To answer this question, one needs fundamental conceptual advances in modeling and predicting *emergent* behavior in complex engineered systems — i.e., how does one go from the behavior of the *parts* to an effective description of the *whole* system behavior.

To be sure, not all systemic failures are due to emergent behavior. Many are simply due to failures at several levels, the net result of which could have been anticipated as in the cases of Piper Alpha, BP Texas City, BP Deepwater Horizon, Enron, and Madoff. There were enough warnings along the way to avoid these catastrophes. However, as one continues to engineer more and more complex distributed, networked, systems-of-systems, emergent behavior will become increasingly important. Researchers in the nascent field of complexity science are beginning to try to address this challenge. Even though complexity science is relatively new, important progress is being made (Ottino, 2005). Researchers are beginning to understand how complex systems can be robust yet fragile (Newman et al., 2002; Doyle et al., 2005; Venkatasubramanian, 2004; Venkatasubramanian, 2007]) to certain kinds of attacks and failures. Further research is very much needed along these lines.

Multiperspective modeling

Another area where progress is needed is multi-perspective modeling. This is different from multiscale modeling where the objective is to model a phenomenon at different length (or time) scales, at different levels of detail, in an integrated manner (de Pablo, 2005). In contrast, in multiperspective models (MPM), one develops *different views* of an entity from the perspectives of structure, behavior and function (SBF). For example, for a reactor embedded in a flow sheet, MPM would comprise of structural/connectivity information, models that predict the behavior of this reactor under various conditions, both normal and abnormal, and its final impact on the intended function (Srinivasan and Venkatasubramanian, 1998). Further research is needed to pursue this line of exploration using SBF modeling, ontologies, formal reasoning methods, and so on (Lind, 1994; Venkatasubramanian et al., 2006; Morbach et al., 2007).

Hybrid intelligent systems for real-time decision support

Finally, the need for a conceptual framework in using the multiperspective models of a system's components along with the insights gained from complexity science to develop intelligent systems that can assist humans with prognostic and diagnostic decision support in real-time is quite clear. As noted earlier, they can also be used for critiquing design choices and conducting thorough process hazards analysis. They can be used for developing intelligent dynamic simulators for operator training. Given the real-world constraints these systems will be hybrid in nature, mixing and matching first principles-based models with data-driven empirical methods. The hybridization will also occur due to the mix of continuous and discrete event modeling methodologies. Considerable progress has been made along these lines, which forms a natural base for further exploration (Stephanopoulos, 1994; Edgar and Davis, 2008; Saleh et al., 2010).

Neglect of Process Safety in Chemical Engineering Teaching and Research

Research

Accomplishing the goals stated above, requires innovative thinking, imaginative approaches, getting over some traditional misconceptions about modeling, and a broader vision of process control.

Generally speaking, when one discusses modeling with chemical engineers, people often think of a system of differential and algebraic equations (DAEs). However, there is a wider variety of knowledge representation concepts leading to other classes of models, which play an important role in

systemic risks analysis. Thus, while chemical engineers are quite familiar with real valued quantitative descriptions, such as, ODE/PDE, statistical regression, and mathematical programming models, they are less so with graph theoretical models, Petri nets, rule-based systems, semantic networks, ontology's, agents, and so on. Over the last 25 years, much progress has been made as these methodologies proved their value by addressing problems of practical importance, which were previously hard, even impossible, to solve using traditional modeling techniques. To be sure, DAE models will play their useful role wherever they are appropriate, but the other kinds of models will play an increasingly important role. Expanding the scope of modeling options produces important implications for the research and educational missions in chemical engineering. As these issues have been discussed at some length in another AIChE *Perspective* article (Venkatasubramanian, 2009), this perspective will not elaborate on them.

Process safety is really a problem in process control — it is only a broader version of the same theme and objectives underlying control. See, for example, the feedback structures in Figure 2, which are distributed at various layers of authority to ensure process safety. Unfortunately, for a long time, the academic process control community in chemical engineering has not embraced this philosophy and, as a result, has largely ignored safety issues in its work, both in teaching and in research. Process control researchers have largely preferred to stay in the realm of DAE models and the associated mathematical methods. This has limited their ability to address other classes of important research problems that arise in automated reasoning for process safety, systemic risks analysis, and supervisory control, as outlined previously. Instead, much of the work in process control has largely been restricted to regulatory control. For instance, the number of research articles written on regulatory control of chemical processes in the past three decades simply dwarfs that on process safety by about two-orders of magnitude. Of course, regulatory control problems are important and had to be addressed. However, they are only a part of the whole picture which naturally includes process safety issues. This is not so much a criticism as it is a lament about missed opportunities and lost time.

It is indeed quite unfortunate that such grand systems engineering intellectual challenges and research opportunities in the detection, analysis, and control of potential hazards in complex systems remain largely under appreciated by the chemical engineering community. This is further compounded by the extremely low level of funding for research on process safety at agencies such as the NSF. Is it any wonder, then, that out of some 1200+ chemical engineering faculty in the top 100 universities in the U.S., less than perhaps 10 professors are actively engaged in process safety research?

Teaching

The situation in teaching has been equally disturbing. Process safety is often treated in a perfunctory manner in chemical engineering courses even though good teaching aids are available through the Center for Chemical Process Safety (CCPS), Safety and Chemical Engineering Education Program (SaChE), Chemical Safety Board, and the works of Kletz (1999), Crowl and Louvar (2002), and others. Nevertheless, many chemical engineering academics seem to treat safety as goggles, hard hats, and perhaps a portable fire extinguisher. Of course, most departments do a good job of providing safety training to their students to avoid mishaps in the labs. However, this training focuses on *personal* or *occupational safety*, *not process safety*, and there are vital differences between the two. This is one of the crucial lessons that came out of the postmortem investigations of the BP Texas City accident in 2005, and is highlighted in the Baker Panel Report of the accident (Baker Panel, 2007). Process safety needs to be addressed properly in all chemical engineering courses. Industrial companies do generally provide a strong safety training to the chemical engineering graduates they hire, but again, that misses the point. The point is that chemical engineering programs need to do a better job of educating their students in process safety and not rely entirely on others to do it for them.

It is quite unfortunate that all these years ABET's program criterion defining the chemical engineering curriculum *did not even mention* process safety, hazards, or risk analysis, while such words were included for construction, mining and petroleum engineering programs. To be sure, ABET's *general* criteria, do include health and safety, in Criterion 3 defining program outcomes. However, this is a common requirement affecting *all* engineering programs. Nevertheless, construction, mining, and petroleum engineering programs saw the necessity to incorporate safety and risk *explicitly* in their particular *program criteria* as well, in addition to its mention in the general criteria. Fortunately, this neglect has finally been recognized by ABET, which is in the process of specifying that the analysis and control of process hazards be included in the program specific criteria for chemical engineering. The new requirement is expected to become official policy in about a year or so. Hopefully, this will lead to a more rigorous treatment of process safety issues in many courses, instead of the typical current regimen of a few lectures in design and/or control courses.

More broadly, though, the neglect of process safety in chemical engineering curricula is symptomatic of a deeper malaise in the teaching of chemical engineering — the "outsourcing" of design and control courses, in some departments, to adjunct faculty, typically from the industry. Admittedly, many of them do a good job, perhaps even a better job than that of the regular faculty, but that is not the point. By such "outsourcing" chemical engineering academics are implicitly acknowledging and broadcasting a message that these courses are not central to their educational mission — i.e., they are not core to the chemical engineering curriculum. Otherwise, would one do this? Would one even consider "outsourcing" the teaching of thermodynamics, transport phenomena, or reaction engineering courses to adjunct faculty all the time? Again, there are industrial visitors who can do a terrific job in these courses as well. However, this is not done. Why not? Because, these are valued as the intellectual core of the chemical engineering discipline.

In this spirit, should not process systems engineering be a required core competency for chemical engineers? Consider for a moment the following question. What is it that chemical engineers do which is not accomplished by academics in other disciplines? Chemical engineers engage in chemistry, of course, but so do chemists. Chemical engineers use thermodynamics, so do physicists, chemists, and some others.

Chemical engineers do transport, so do applied mathematicians, applied physicists, mechanical engineers, and so on. Ditto for biology. So, what is differentiating about chemical engineers? One may argue that chemical engineers use more quantitative modeling than chemists or biologists. A simple observation of the research output from these two disciplines would quickly dispel such a notion. However, chemical engineers integrate thermodynamics, transport phenomena and reaction engineering principles in defining the mathematical models for the description of various phenomena, more extensively than any other discipline, and in doing so they have established a competitive edge.

However, unquestionably, there is something else they do that others do not and cannot. Process systems engineering (PSE) — the analysis, design, control, and optimization of chemical, physical, and/or biological process systems, through the judicious quantitative integration of chemistry, biology, thermodynamics, transport phenomena, kinetics and reactions engineering. This is what sets the chemical engineers truly apart from chemists, physicists, biologists and mathematicians; and other engineers. *Systems' thinking is a core competency for all engineers and process-oriented systems thinking is a core competency for chemical engineers*. Not only PSE courses should not be "outsourced", PSE should be required as a core competency in the graduate programs as well. While this important message emerged from the Frontiers of Chemical Engineering workshop series that MIT organized (Rawlings and Edgar, 2004), it is a pity that this has not been widely adopted in academia.

In the rush to seize new opportunities in the emerging areas of nanotechnology and biomolecular engineering, chemical engineering departments seem to have deemphasized PSE in the last 15 years or so. This is most unfortunate on two counts. First of all, the discipline runs the risk of losing on a core competency area. Second, the timing of this "downsizing" in PSE is bad. Just when countries all over the world are getting ready to address the challenges in energy, environment, and sustainability — challenges which absolutely require a systems engineering approach without which they are impossible to solve, the discipline has "downsized" the PSE community. Just when even biology and chemistry, where the reductionist philosophy had dominated for well over 60 years, have turned around and recognized the value of systems thinking, as evidenced by the emergence of systems biology and systems chemistry as "hot" growth areas, many chemical engineering departments, and the funding agencies, were neglecting PSE.

Summary

As the BP Deepwater Horizon oil spill disaster reminds academic and practicing chemical engineers alike, one can never take process safety for granted. All of us, including individuals, corporate management, regulatory agencies, universities, and communities, need to learn the lessons from every accident, particularly from the systemic ones. It is imperative to study all these disasters from a common systems engineering perspective so that one can thoroughly understand the commonalities, as well as the differences in order to prevent or mitigate future ones.

This is where universities can, and should, play an important role, in creating and disseminating knowledge about abnormal events management in complex engineered systems, and their public and corporate policy implications. It is imperative that chemical engineering academics rise to the challenge and responsibility in fostering the education of the next generation of chemical engineers with higher sensitivity on the importance of safety, sustainability, and ethics. In this regard, it is encouraging to see the beginnings of a change in attitude in recent years. The increasing attention paid to process monitoring, fault diagnosis, fault-tolerant control, process hazards analysis, etc., in conference programs and textbooks is certainly a step in the right direction. This trend needs to be strongly encouraged and supported by the funding agencies.

Systemic failures are not limited to processes with hydrocarbons, although these represent the large majority of high-risk situations. Systemic risks are potentially inherent in many of the other areas where chemical engineers play a central role in, such as product design, design and operation of biological processes — e.g., imagine the consequences of a large-scale accident, or security breach, in a genetic engineering facility where a dangerous virus is released into the environment; biomedical devices; release of toxic nanoscale particles, and many others.

No contemporary engineered system with ever increasing complexity can be risk free. Minimizing inherent risks in our products and processes is a wonderful intellectual challenge for creative science and engineering, and one that could provide substantial differentiating competitiveness. The chemical/biological process is like a genie that grants our wishes — the quality of life enjoyed by many in modern times will be hard to contemplate without the products from the chemical (and allied) process industries. However, unlike Aladdin's genie, which grants one's wishes only when let out, this genie needs to be contained all the time to fulfill our desires. To accomplish this takes vigilance and effort all the time and across the board.

Safety is not the responsibility of just the environment, health and safety department. It is everyone's responsibility in the facility. There exists a need for systems, procedures, corporate and regulatory cultures that ensure this. In the long run, considerable technological help would come from progress in taming complexity, which would result in more effective prognostic and diagnostic systems for monitoring, analyzing, and controlling systemic risks. However, getting there would require innovative thinking, bolder vision, and overcoming some misconceptions in and about the process systems engineering community.

Acknowledgments

The author gratefully acknowledges the useful comments of Rakesh Agrawal, Thomas Edgar, Ignacio Grossmann, Karen Marais, Rex Reklaitis, Warren Seider, Jeff Siirola, and Erik Ydstie on the draft version of the manuscript. The author is especially indebted to George Stephanopoulos for his many valuable comments and editorial assistance. He also thanks his former and current students, and postdoctoral associates, who have helped him learn various aspects of systemic failures in complex systems over the past 25 years. He also thanks Aviral Shukla for his assistance with Figure 2. Finally, the author appreciates the financial support from Idaho National Laboratories, Department of Energy, and the NSF ERC on Structured Organic Particulate Systems.

Literature Cited

Baker Panel, The BP U.S. Refineries Independent Safety Review Panel Report (2007).

Crowl, D., and J. Louvar, *Chemical Process Safety: Fundamentals with Applications*, 2nd ed., Prentice Hall PTR, New York (2002).

Davis, J., and T. F. Edgar., "Smart Process Manufacturing - A Vision of the Future," *Design for Energy and the Environment* (Proc 7th Int. Conf. *FOCAPD 2009),* Breckenridge, CO, Taylor and Francis, Boca Raton, FL (June 2009).

de Pablo, J. J., "Molecular and Multiscale Modeling in Chemical Engineering - Current View and Future Perspectives," *AIChE J*., 51(9) (2005).

Doyle, J. C., D. L. Alderson, L. Li, S. Low, M. Roughan, S. Shalunov, R. Tanaka, and W. Willinger, "The "Robust Yet Fragile" Nature of the Internet," *PNAS*, 102(41) 14497–14502 (October 11, 2005).

Fox-Penner, P., "A Year Later, Lessons From the Blackout," *New York Times* (Aug 15, 2004).

Gruber, T. R., "A Translation Approach to Portable Ontology Specification," *Knowledge Acquisition*, 5(2), 199–220 (1993).

Henley, E. J., and H. Kumamoto, *Probabilistic Risk assessment: Reliability Engineering, Design, and Analysis*, IEEE Press, New York (1991).

Hopkins, A., "Failure to Learn The BP Texas City Refinery Disaster," CCH Publishing, Australia (2009).

Jasanoff, S., *Learning from Disaster: Risk Management after Bhopal*, U. Pennsylvania Press, Philadelphia (1994).

Johnson, L. D., and E. H. Neave, "The Subprime Mortgage Market: Familiar Lessons in a New Context," *Management Research News*, 31(1) 12–26 (2007).

Kletz, T. A., *What Went Wrong?: Case Studies of Process Plant Disasters*, 4th ed. Gulf Professional Publishing, Houston (1999).

Krugman, P., "Berating the Raters," *New York Times* (Apr. 26, 2010).

LaPedis, R., "Lessons Learned from the 2003 Northeastern Blackout," *HP Non Stop*, www.hp.com/go/nonstop (May 2004).

Lapp, S. A., and G. J. Powers, "Computer-Aided Synthesis of Fault Trees," *IEEE Trans on Reliability*, 26(1), 2–13 (1977).

Leveson, N.G., "A New Accident Model for Engineering Safer Systems," *Safety Science*, 42(4), 237–70 (2004).

Lind, M., "Modeling Goals and Functions of Complex Industrial Plants," *Applied Artificial Intelligence*, 8(2), 259–283 (1994).

Markopolos, H., *No One Would Listen*, Hoboken, NJ: Wiley (2010).

MSNBC, "Mine Owner Ran Up Serious Violations," http://www.msnbc.msn.com/id/36202623/ (Apr. 6, 2010).

Morbach, J., A. Yang, and W. Marquardt, "OntoCAPE-A Large-Scale Ontology for Chemical Process Engineering," *Engineering Applications of Artificial Intelligence,* 20(2), 147–161 (2007).

Newman, M. E. J., M. Girvan, and D. J. Farmer, "Optimal Design, Robustness, and Risk Aversion," *Phys Rev Lett*. 89:028301–1-4 (2002).

Olivea, C., T. M. O'Connora, and M. S. Mannan, "Relationship of Safety Culture and Process Safety," *J. Hazardous Materials*, 130(1–2), pp. 133–140 (2006).

Ottino, J. M., "New Tools, New Outlooks, New Opportunities," *AIChE J*., 51, 1840–1845 (2005).

Pariyani, A., W. D. Seider, U. G. Oktem, and M. Soroush, "Incidents Investigation and Dynamic Analysis of Large Alarm Databases in Chemical Plants: A Fluidized Catalytic-Cracking Unit Case Study," *Ind. Eng. Chem. Res*., 49, 8062–8079 (2010).

Piper Alpha Disaster, Building Process Safety Culture: Tools to Enhance Process Safety Performance, *Center for Chemical Process Safety*, AIChE, New York (2005).

Plotz, D., "Play the Enron Blame Game!," *Slate* (Feb. 1, 2002).

Rasmussen, J., and I. Svedung, *Proactive Risk Management in a Dynamic Society*, Swedish Rescue Services Agency (2000).

Rawlings, J. B., and T. F. Edgar, "Frontiers of Chemical Engineering: The Systems Approach," *Proc of DYCOPS*, paper no. 206, Boston, MA (2004).

Saleh, J. H., K. B. Marais, E. Bakolas, and R. V. Cowlagi, "Highlights from the literature on accident causation and system safety: Review of major ideas, recent contributions, and challenges," *Reliability Engineering and System Safety*, 95, 1105–1116 (2010).

Simons, J., "Bitter Medicine At Schering-Plough," *CNN Money and Fortune* (October 14, 2002). Available at: http://money.cnn.com/magazines/fortune/fortune_archive/2002/10/14/330051/index.htm

Srinivasan, R., and V. Venkatasubramanian, "Multi-Perspective Models for Process Hazards Analysis of Large-Scale Chemical Processes," in the Proc of the *European Symposium on Computer-Aided Process Engineering 8,* Brugge, Belgium (May 1998).

Stephanopoulos, G., "Knowledge, Computers, and Chemical Engineering: A Critical Synthesis," *CAST Communications*, 17(1) (Winter 1994).

Thomas, P., L. A. Jones, J. Cloherty, and J. Ryan, "BP's Dismal Safety Record," *ABC News* (May 27, 2010). Available at: http://abcnews.go.com/print?id=10763042

Urbina, I., "Inspector General's Inquiry Faults Regulators," *New York Times* (May 24, 2010).

Venkatasubramanian, V., S. R. Katare, P. R. Patkar, and F. Mu., "Spontaneous Emergence of Complex Optimal Networks Through Evolutionary Computation," *Comput. Chem. Eng*., 28, 1789–1798 (2004).

Venkatasubramanian, V., C. Zhao, G. Joglekar, A. Jain, L. Hailemariam, P. Sureshbabu, P. Akkisetti, K. Morris, and G. V. Reklaitis, "Ontological Informatics Infrastructure for Chemical Product Design and Process Development," *Comput. Chem. Eng*., 30(10–12), 1482–1496 (2006).

Venkatasubramanian, V., A Theory of Design of Complex Teleological Systems: Unifying the Darwinian and Boltzmannian Perspectives, *Complexity*, 12(3) (2007).

Venkatasubramanian, V., J. Zhao, and S. Viswanathan, "Intelligent Systems for HAZOP Analysis of Complex Process Plants," *Comput. Chem. Eng*., 24(9–10), 2291–2302 (2000).

Venkatasubramanian, V., "Drowning in Data: Informatics and Modeling Challenges in a Data Rich Networked World," *AIChE J*., 55(1), 2–8 (2009).