Systemic Failures and Process Systems Engineering

Venkat Venkatasubramanian

In the history of chemical plant accidents, a few disasters have served as wake up calls. The Flixborough accident in 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 2000+ were killed and about 100,000+ were seriously injured by the accidental release of methyl isocynate. 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. 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 and Schering Plough's inhalers recall are systemic failures. Financial disasters such as Enron, WorldCom, subprime mortgage derivatives market, Madoff Ponzi scheme, as well as some other events also belong to the same class.

While these are different disasters that happened in different domains, different facilities, triggered by different events, involve different chemicals, and so on, there are, however, certain common underlying patterns behind such systemic failures. In the Januray 2011 *AICHE Journal Perspective* article entitled " Systemic Failures: Challenges and Opportunities in Risk Management in Complex Systems", Venkat Venkatasubramanian says that these patterns teach us important fundamental lessons that we had better learn to avoid such disasters in the future. "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. Further, 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."

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, inter-connectedness, and interactions with humans and the environment that can make these 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 inter-dependent 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 sub-systems that make systemic risks even more likely if one is not vigilant all the time.

Postmortem investigations have shown that major disasters rarely occur due to a single failure of an equipment or personnel. Even though the senior management typically tries to spin the blame as some unanticipated equipment failure, an operator error, or a rogue trader, that is rarely the case for major disasters. Again and again, investigations have shown that there are always several layers of failures of equipment, systems, processes and people that led to major disasters. And often, the responsibility for the accident goes all the way to the top levels of company management who had only paid a lip service to safety, which resulted in a poor corporate culture regarding safety.

Venkatasubramanian argues that there is an important role for universities here 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.

Venkatasubramanian concludes: "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. But 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. 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. But getting there would require innovative thinking, bolder vision, and overcoming some misconceptions in and about the process systems engineering community."