APS1034H - Understanding Technological Catastrophes

Outline

Despite the best of engineering practices which include a focus on reliability, human factors and quality improvement, spectacular failures of complex technological systems occur regularly: bridges collapse, chemical plants catch fire and explode, airplanes crash and nuclear reactors melt down. Various theories have been proposed to explain this behavior. At two extremes are Normal Accident Theory which claims accidents are inevitable in highly complex and tightly coupled systems, and High Reliability Theory according to which such failures can be avoided by organizations that use appropriate management processes. This course describes these theories, highlights the limits of traditional event-chain models of causation in preventing disasters, and suggests that the safety of large sociotechnical systems can be enhanced using systems thinking and practice. The course comprises the following: (a) seminars that present and integrate the various theoretical approaches to understanding engineering accidents; (b) a demonstration of these concepts using case studies drawn from a range of industries and organizations; and (c) individual and/or group presentations by students analyzing specific disasters.

Syllabus

SESSION [a]	**TOPIC**
1	**Risk Management in a Dynamic Society** Introduction to the main elements of the course, an overview of a system-oriented approach to risk, and description of term paper and group project. *Case 1*(*a*): Herald of Free Enterprise Disaster
2	**Normal Accident Theory (NAT)** Claims that accidents in highly complex and tightly-coupled technological systems are inevitable. *Case Study 2*: Three Mile Island
3	**High Reliability Theory (HRT)** Organizations that succeed in avoiding accidents. *Case Study 3*: Aircraft Carrier Flight Operations
4	**Reliability, Conceptual Slack and Mindfulness of Organizations** Defining organizational reliability, and the importance of maintaining sufficient mindfulness and operational slack. *Case Study 4*: The Diablo Canyon nuclear power plant
5	**Epistemic Accidents** System accidents caused by technologies built around fallible theories, judgments and assumptions. Limits of regulation. *Case Study 5*: Aloha Flight 243

/ ..

6	**Critique of NAT and HRT** Studies supporting and rejecting Normal Accident Theory. Limitations of High Reliability Organizations.
7	**The HRT versus NAT Debate** Summarizes various sociological attempts to bridge the divide between the two theoretical approaches, including a proposed resolution via the incorporation of a temporal dimension and Disaster Incubation Theory.
8	**Traditional Safety Engineering versus Systems Thinking** Reviews the use of traditional event-chain models of causality in accident modelling and highlights the advantages of systems theory as formulated by Jens Rasmussen (Risø) and Nancy Leveson (MIT). *Case 1*(*b*): Herald of Free Enterprise Disaster (continued)
9	**Systems Theoretic Approach to Accident Modelling (STAMP)** Applying systems theory concepts to accident analysis and prevention requires inclusion of the social system overlying the technical system. *Case Study 6*: Walkerton (Ontario) Water Contamination Accident
10	**Student presentations 1**[b] 30 min individual/group accident case-study presentations
11	**Student presentations 2**[b] 30 min individual/group accident case-study presentations
12	**The Social Roots of Risk** The origins of disasters lie not in nature or technology but in the workings of society. Disasters serve as triggers to vulnerabilities. Conclusions and student feedback.

[a] Each session is of 2-3 hr duration.

[b] Additional time may be allocated during Session 12 depending on class size.

References

The following books provide a sociological perspective of disaster causation and management. Optional reading if time permits.

[1] C. Perrow, Normal Accidents: Living with High-Risk Technologies, 2nd Edition, Princeton University Press, Princeton, NJ, 1999.

[2] K.E. Weick and K.M. Sutcliffe, Managing the Unexpected: Resilient Performance in an Age of Uncertainty, 2nd Edition, Jossey-Bass, San Francisco, 2007.

[3] K. Tierney, The Social Roots of Risk: Producing Disasters, Promoting Resilience, Stanford Business Schools, 2014.

Textbook

The following is the recommended course textbook and is available at the U of T Bookstore at a competitive price. Specific reading material (in the form of available extracts from books and journal articles) covering each topic will be assigned additionally during the course.

N.G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, MIT Press, Cambridge, MA, 2001.

Evaluation

Participation	10%
Term Paper	40%
Team Project Presentation and Report†	50%

† Team members will be expected to contribute and present sections of the report.

Prerequisites

There are no prerequisites. The course is aimed at engineering students enrolled in the ELITE Program, but is open to graduate students from all faculties including Business Administration.