APS 1034H - 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, nuclear reactors melt down. Various theories have been proposed to explain this behavior. At two extremes are Normal Accident Theory which claims that accidents are inevitable in highly complex and nonlinear systems, and High Reliability Theory according to which such failures can be avoided by organizations that use complex management processes. This course highlights the limits of socio-technical systems in preventing catastrophic failures and the importance of incorporating such insights in engineering design. 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 catastrophic accidents.

Syllabus

SESSION	TOPIC
1	**Video: Herald of Free Enterprise Disaster** Capsizing of a ferry outside Zeebrugge harbor in Belgium, 1987. Introduction to the main elements of the course.
2	**High Reliability Theory (HRT)** Organizations that succeed in avoiding accidents. *Case Study 1*: Aircraft Carrier Flight Operations
3	**Reliability, Conceptual Slack and Mindfulness of Organizations** Difficulties in defining organizational reliability, and the importance of maintaining sufficient mindfulness and operational slack. *Case Study 2:* The Diablo Canyon nuclear power plant
4	**Normal Accident Theory (NAT)** Accidents in highly complex and nonlinear technological systems are inevitable. *Case Study 3*: Three Mile Island
5	**Systems Failure Analysis** Explores a connection between fault tree analysis and normal accident theory. *Case Study 4*: Deepwater Horizon Rig

/ ..

6	**Epistemic Accidents** System accidents caused by technologies built around fallible theories, judgments and assumptions. *Case Study 5*: Aloha Flight 243
7	**The HRT versus NAT Debate** Summarizes various inconclusive attempts to bridge the divide between the two theoretical approaches.
8	**Disaster Incubation Theory** Resolution of the HRT-NAT debate via incorporation of a temporal dimension.
9	**Mathematical Approaches to Modeling Accidents** Overview of traditional modeling approaches (Sequential Events Models, Chains of Time-Ordered Events Models and Risk Analysis Models). Catastrophe theory.
10	**Student presentations 1**[†] 30 min individual/group accident case-study presentations
11	**Student presentations 2** 30 min individual/group accident case-study presentations
12	**Conclusions** Perrow's response to the approach discussed in Session 8. Discussion and student feedback.

[†] Students will be expected to discuss a severe accident within the context of the advanced modeling approaches studied in the course. Additional time may be allocated depending on class size.

References

High Reliability Theory and Normal Accident Theory are introduced in the following two very readable monographs:

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

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

Additional reading material covering each topic will be assigned during the course.

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.