APS1034H - Understanding Technological Catastrophes

Summer 2016

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 sociological 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 but highlights the limits of traditional event-chain models of causation in preventing disasters and shows that the safety of large sociotechnical systems can be enhanced using systems thinking and practice. The course comprises the following: (a) lectures that present and integrate the various theoretical approaches to understanding accidents; (b) demonstration of these concepts using case studies drawn from a range of industries and organizations; and (c) group presentations by students analyzing specific disasters.

Syllabus

SESSION [a]	**TOPIC**
1	**Disasters as Sociotechnical Events** An overview of the main elements of the course, examples of some recent disasters, and the importance of a system-oriented approach to risk.
2	**Man-Made Disasters** Disasters arise from an interaction between the human and organizational arrangements of sociotechnical systems set up to manage complex and ill-structured risk problems. *Case Study 1*: Israeli Intelligence Failure in 1973 October War
3	**Normal Accident Theory (NAT)** Claims that accidents in highly complex and tightly-coupled technological systems are inevitable. *Case Study 2*: Three Mile Island
4	**Epistemic Accidents** System accidents caused by technologies built around fallible theories, judgments, and assumptions. Limits of regulation. *Case Study 3*: Aloha Flight 243
5	**High Reliability Organizations (HRO)** High-risk organizations that succeed in avoiding accidents. *Case Study 4*: Aircraft Carrier Flight Operations

6	**Tutorial: STAMP Analysis of an Accident** A preview of the System-Theoretic Accident Modeling and Processes methodology using the Vioxx drug recall in the US; needed for project.
7	**Reliability, Conceptual Slack and Mindfulness of Organizations** Defining organizational reliability, and the importance of maintaining sufficient mindfulness and operational slack. *Case Study 5*: The Diablo Canyon Nuclear Power Plant
8	**Critique of NAT and HRO Frameworks** Studies supporting and rejecting Normal Accident Theory. Limitations of High Reliability Organizations.
9	**Resolution of the HRT versus NAT Debate** Summarizes a proposed resolution of the debate via incorporation of a temporal dimension and Practical Drift Theory. Reframing of NAT using open systems concepts such as negentropy and requisite variety.
10	**Traditional Safety Engineering versus Systems Thinking** Reviews the use of traditional event-chain models of causality in accident modeling and highlights the advantages of systems theory as formulated by Jens Rasmussen (Risø) and Nancy Leveson (MIT). *Case 6*: Herald of Free Enterprise Disaster (continued)
11	**Systems Theoretic Approach to Accident Modeling** Applying systems theory concepts to accident analysis and prevention requires inclusion of the social system overlying the technical system. *Case Study 7*: Walkerton (Ontario) Water Contamination Accident
12	**Student Presentations 1** 30 min individual/group accident case-study presentations, followed by a 10 min critique by class members.
13	**Student Presentations 2** 30 min individual/group accident case-study presentations; peer critique.

[a] The duration of each session is 2-3 hours.

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.

Textbook

Required reading material (in the form of extracts from books and journal articles) covering each topic will be assigned during the course. This will include the systems approach needed for the group project although an excellent resource is the following book:

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

(Available in digital form through the U of T Library system and in print for short-term loan at the Eng. & Comp. Sci. Library.)

Evaluation

Exam[1]	30%
Term Paper[2]	20%
Team Project Presentation and Report[3]	50%

[1] The examination will consist of an essay on a topic requiring comprehensive understanding of the material taught in this course.

[2] A term paper on the application of Turner's disaster model to a severe accident.

[3] Application of the systems approach to the understanding of some technological catastrophe. Team members will be expected to contribute and present sections of the report, and selected class members will provide formal critique. Team size: 3-5.

Prerequisites

English-language proficiency and especially writing skills are required. The course is aimed at engineering students enrolled in the ELITE Program but is open to all graduate students.

Schedule and Important Dates

Sessions:	Mondays	6 PM – 9 PM	WB 219
	Thursdays	6 PM – 9 PM	WB 119
Duration:	July 4 – August 16		
Last Day to Add/Drop:	July 8/22		
Exam:	August 18	6 PM – 7:30 PM	WB 219

Instructor

(Dr.) Julian Lebenhaft, P.Eng. julian.lebenhaft@utoronto.ca