**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) 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 | **Disasters as Sociotechnical Events**<br>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**<br>Disasters arise from an interaction between the human and organizational arrangements of sociotechnical systems set up to manage complex and ill-structured risk problems.<br>*Case Study 1*: Israeli Intelligence Failure in 1973 October War |
| 3 | **Normal Accident Theory (NAT)**<br>Claims that accidents in highly complex and tightly-coupled technological systems are inevitable.<br>*Case Study 2*: Three Mile Island |
| 4 | **Epistemic Accidents**<br>System accidents caused by technologies built around fallible theories, judgments and assumptions. Limits of regulation.<br>*Case Study 3*: Aloha Flight 243 |
| 5 | **High Reliability Organizations (HRO)**<br>High-risk organizations that succeed in avoiding accidents.<br>*Case Study 4*: Aircraft Carrier Flight Operations |

| | |
|---|---|
| 6 | **Tutorial: STAMP Analysis of an Accident**<br>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**<br>Defining organizational reliability, and the importance of maintaining sufficient mindfulness and operational slack.<br>*Case Study 5*: The Diablo Canyon Nuclear Power Plant |
| 8 | **Critique of NAT and HRO Frameworks**<br>Studies supporting and rejecting Normal Accident Theory. Limitations of High Reliability Organizations. |
| 9 | **Resolution of the HRT versus NAT Debate**<br>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**<br>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).<br>*Case 6*: Herald of Free Enterprise Disaster (continued) |
| 11 | **Systems Theoretic Approach to Accident Modelling**<br>Applying systems theory concepts to accident analysis and prevention requires inclusion of the social system overlying the technical system.<br>*Case Study 7*: Walkerton (Ontario) Water Contamination Accident |
| 12 | **Student Presentations 1**<br>30 min individual/group accident case-study presentations, followed by a 10 min critique by class members. |
| 13 | **Student Presentations 2**<br>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

Specific reading material (in the form of available 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

| | |
|---|---|
| Quiz[1] | 10% |
| Term Papers[2] | 40% |
| Team Project Presentation and Report[3] | 50% |

[1] A short (30 min) test comprising a 1-2 page written commentary on some general aspects of the material taught in this course. (Might be eliminated if class participation is significant.)

[2] Two term papers on the application of Turner's disaster model and Epistemic Accident theory to a severe accident (20% each).

[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 formal critique will be provided by selected class members. Team size: 2-4 (ideally 3).

Prerequisites

There are no prerequisites other than English-language proficiency. 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 & Thursdays | 6 PM – 9 PM | RS310 |
| Duration: | July 4 – August 15 | | |
| Last Day to Add/Drop: | July 8/22 | | |

Instructor

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