APS1034H – Making Sense of Accidents **Summer 2022**

Outline

Despite the best engineering practices that rely on reliability, human factors, and continuous quality improvement, severe accidents involving complex technological systems occur regularly: bridges collapse, chemical plants catch fire and explode, airplanes crash, and nuclear reactors melt down. The most comprehensive approach to understanding the causes of such disasters is based on systems engineering that highlights the limits of traditional event-chain causation models. The course focuses on this approach using a group project but also provides an overview of various sociological theories that have attempted to elucidate the organizational and psychological factors underlying the failure of sociotechnical systems.

Syllabus

TOPIC
Accidents as Sociotechnical Events Accidents cannot be considered as strictly technical events and must be viewed within a social context. Review of traditional approaches to accident analysis.
Systems Thinking Shortcomings of chain-of-events accident causal analyses. The Rasmussen (AcciMap) system-engineering approach for understanding and preventing accidents. *Case Study 1*: The Ferry Capsizing Accident at Zeebrügge, Belgium
Systems-Theoretic Accident Modeling and Processes (STAMP) A significant enhancement of the Rasmussen systems methodology based on dynamic system modeling was formulated by Nancy Leveson (MIT). *Pre-case study*: An analysis of the Walkerton disaster using an AcciMap.
Causal Analysis Based on STAMP (CAST) A framework to guide the STAMP analysis of an accident with the goal of identifying the related systemic causal factors. *Case Study 2*: The Walkerton (Ontario) Water Contamination Disaster
Team Project The team project will consist of a CAST analysis of the sinking of the Ocean Ranger mobile offshore oil drilling unit in Canadian water on 15 February 1982.
Turner's 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 3*: Israeli Intelligence Failure in 1973 October War

Normal Accident Theory (NAT) Formulated by Charles Perrow (Yale), this theory claims that accidents in interactively complex and tightly coupled technological systems are inevitable. *Case Study 4*: Three Mile Island
High Reliability Organizations (HRO) A discussion of high-risk organizations that succeed in avoiding accidents. *Case Study 5*: Aircraft Carrier Flight Operations
Reliability, Conceptual Slack, and Mindfulness of Organizations Defining organizational reliability, and the importance of maintaining sufficient mindfulness and operational slack. *Case Study 6*: The Diablo Canyon Nuclear Power Plant
Critique of NAT and HRO Frameworks Studies supporting and rejecting Normal Accident Theory. Limitations of High Reliability Organizations.
Resolution of the HRT versus NAT Debate Summarizes a proposed resolution of the debate via the incorporation of a temporal dimension and Practical Drift Theory. Reframing of NAT using open systems concepts such as negentropy and requisite variety.
Social Regulation of Technology Agents regulating high-technology industry face an epistemic barrier that results in dependence on the regulated, compromises their autonomy, and prevents detection of organizational drift toward disaster. This leads to 'regulatory capture' as demonstrated by Aloha Airlines Flight 243 (*Case Study 7*).
Epistemic Accidents These are accidents related to the limits of knowledge. The use of composite materials in modern passenger airplanes creates the possibility of such accidents.
Project Presentations

Textbook

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.)

References

The following books provide a sociological perspective of disaster causation and risk management:

[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.

Other reading material consisting of journal articles covering each topic will be made available during the course.

Evaluation

Term paper	40%
Team project presentation and report	60%

Prerequisites

English-language proficiency and especially writing skills are required. The course is aimed at graduate students enrolled in the ELITE Program but is open to other engineering disciplines. APS1034H is the recommended prerequisite for APS1101H (System Dynamic Risk Assessment).

Attendance

The initial phase of the team project will be performed as a class-wide collaboration, and the participation of all the students is essential. Attendance is required.

Schedule and Important Dates

Sessions:	Monday, Tuesday, Thursday 6-8 PM
Duration:	Monday, May 2 – Thursday, June 16
Add:	Monday, May 9
Drop:	Friday, May 27

Instructor

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