APS440H1S/1034H – Making Sense of Accidents Winter 2020

Outline

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

Topics[1,2]

Accidents as Sociotechnical Events

Accidents cannot be considered as strictly technical events and must be considered within a social context. A 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)

Significant enhancement of the Rasmussen systems methodology based on dynamic system modeling 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 assist in 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

Dynamic Modeling

The Stella programming language is used for the dynamic modeling that underlies the STAMP methodology. An advanced topic aimed at graduate students but optional for undergrads.

Team Project

Discussion of the team projects that will consist of a Rasmussen AcciMaps or CAST/STAMP analysis of the Boeing company and the accidents involving the 737 Max passenger planes.

Turner's Disaster Incubation Model

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 the 1973 October War.

Normal Accident Theory (NAT) Formulated by Charles Perrow (Yale), this theory claims that accidents in highly complex and tightly coupled technological systems are inevitable. *Case Study 4*: Three Mile Island
High Reliability Organizations (HRO) High-risk organizations that consistently 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 HRO versus NAT Debate Summarizes a proposed resolution through the incorporation of a temporal dimension and Practical Drift Theory. Reframing of NAT using open systems concepts of negentropy and requisite variety.
Social Regulation of Technology Agents regulating high-tech 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*).
System Engineering Approach to Risk Analysis STPA is a hazard analysis technique based on STAMP that relies on system engineering rather than reliability theory. Demonstrated using the NASA independent regulatory framework.

[1] Most topics require 3-4 hours and are presented over two days. All PowerPoint presentations and related course material will be posted on Quercus after each two-hour session.

[2] Additional topics will be added depending on time availability and student interest.

Simulation

Dynamic modeling may be performed using the Stella programming language as part of the team project (required for the graduate students but optional for the undergraduates). For an overview of this simulation environment see:

https://www.youtube.com/watch?v=W29xpHRYXxA.

Textbook

N.G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*, MIT Press, Cambridge, MA, 2011.

(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. Optional reading for the interested students.

[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 in the form of extracts from books and journal articles covering each topic will be made available during the course.

Evaluation

Term tests (2)	50%
Team project presentation and report	50%

Prerequisites

English-language proficiency and especially writing skills are required. The course is aimed at undergraduate engineering students working toward the Forensic Engineering Certificate and graduate students enrolled in the ELITE Program.

Venue and Important Sessional Dates

Sessions:	Monday, Wednesday	1-3 PM
Room:	MY420 (Monday), MY330 (Wednesday)	
Enroll:	Sunday, January 19	
Drop:	Sunday, March 15	
Duration:	Monday, January 6 – Thursday, April 9	

Instructor

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