APS1034H – Making Sense of Accidents **Summer 2023**

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 a systems-thinking perspective 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 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) "soft" systems 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 control theory and system dynamics modeling was formulated by Nancy Leveson (MIT).
Causal Analysis based on Systems Theory (CAST) The methodology used to perform a STAMP-based analysis of an accident with the goal of identifying the related accident causal factors. *Case Study 2*: The Walkerton (Ontario) water contamination disaster.
Joint Cognitive System (JCS) The human and machine are considered together as a basic construct, and the focus is on what the JCS does, *i.e.*, its functions, and not on how it does it.
Functional Resonance Accident Model (FRAM) In FRAM, the systemic accident model describes the characteristic performance of the JCS rather than focusing on specific cause-and-effect mechanisms. It achieves this by extending the concept of stochastic resonance to normal system functions. *Case Study 3*: The RNAV flight area navigation for aircraft operation.

Turner's Man-Made Disasters Disasters arise from error accumulation resulting from a lack of information and the misinterpretation of warning signals by organizations managing technical systems. *Case Study 4*: Israeli intelligence failure in the 1973 October war.
Psychology of Decision-Making Our mental machinery underlies strategic surprise, human error, and faulty decision-making. This topic discusses how people process information to judge incomplete and ambiguous information.
Normal Accident Theory (NAT) This theory, formulated by Charles Perrow (Yale), claims that accidents in interactively complex and tightly coupled technological systems are inevitable. *Case Study 5*: Three Mile Island nuclear power reactor accident.
High Reliability Organizations (HRO) A discussion of high-risk organizations that succeed in avoiding accidents. *Case Study 6*: Aircraft carrier flight operations.
Mindfulness in Organizations An examination of the processes used by HROs to promote anticipation and resilience, thus achieving operational reliability. Includes a discussion of organizational culture. *Case Study 7*: Refueling at the Diablo Canyon Nuclear Power Plant.
Critique of NAT and HRO Frameworks Studies supporting and rejecting Normal Accident Theory. Limitations of High Reliability Organizations.

Textbook

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

E. Hollnagel, *FRAM: the Functional Resonance Analysis Method — Modelling Complex Socio-Technical Systems*, Ashgate, Burlington, VT, 2012.

(Both monographs are 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 various topics will be made available during the course.

Evaluation

Term paper	40%
Team project presentation and report	60%

Team Project

The project will consist of an analysis by competing teams of the 1987 Zeebrügge car ferry disaster using the STAMP or FRAM accident causation models.

Prerequisites

English-language proficiency, including writing and communication skills, is required. The course is aimed at graduate students enrolled in the ELITE Program but is open to other disciplines.

Schedule and Important Dates

Sessions: Monday, Tuesday, and Thursday 5 – 7 pm MY370

Duration: Monday, May 1 – Thursday, June 15

Drop: Friday, May 26

Instructor

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