APS1034H – Making Sense of Accidents **Summer 2024**

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 strictly technical events and must be viewed within a social context. Includes a review of traditional approaches to accident analysis.
The Human Mind and Perception 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.
Turner Disaster Model Disasters arise from an interaction between the human and organizational arrangements of sociotechnical systems that manage complex and ill-structured risk problems.
Systems Thinking – An Engineering Approach 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 dynamic system modeling was formulated by Nancy Leveson (MIT).
Causal Analysis using Systems Theory (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

Resilience Engineering Resilience engineering aims to understand how complex adaptive systems cope when they encounter surprise. Human-machine interaction is examined, cognitive systems are introduced, and an alternative view of human error and safety is discussed.
Functional Resonance Analysis Method (FRAM) Resilience engineering requires new methods to look at things that go right, analyze how they work, and manage performance variability instead of constraining it, as traditional risk analysis approaches. FRAM is such a methodology. *Case Study 3*: RNAV area navigation system for aircraft landing at an airport
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 4*: Nuclear accident at 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
NAT, HRO, and the Correct Perspective on Accidents Studies supporting and rejecting Normal Accident Theory. Limitations of High Reliability Organizations. The NAT versus HRO debate. Conclusions.

References

N.G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*, MIT Press, Cambridge, MA, 2001. (Available in digital form via the U of T Library system.)

E. Hollnagel and D. D. Woods, *Joint Cognitive Systems*: *Foundations of Cognitive Systems Engineering*, CRC Press, Boca Raton, FL, 2005.

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

C. Perrow, *Normal Accidents: Living with High-Risk Technologies*, 2nd Edition, Princeton University Press, Princeton, NJ, 1999.

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%

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, 6 – 8 PM, room TBD

Duration: Monday, May 1 – Thursday, June 13

Add / Drop: Monday, May 13 / Monday, June 3

Holiday: May 20 (Victoria Day)

Instructor

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