APS440H1/1034H – Making Sense of Accidents **Fall 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
Introduction The probability of a severe nuclear reactor accident like Fukushima is $\sim 10^{-5}\ yr^{-1}$, yet such accidents occur every few decades. Recent advances in probability theory show that complex nonlinear systems can experience extreme events not normally predicted.
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 1*: Three Mile Island
Turner's Man-Made Disasters Disasters arise from an interaction between the human and organizational arrangements of sociotechnical systems that manage complex and ill-structured risk problems.
Accidents as Sociotechnical Events Accidents are not strictly technical events and must be viewed within a social context. Review of traditional approaches to accident analysis.
Reality 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.
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 2*: The Ferry Capsizing Accident at Zeebrügge, Belgium

Systems-Theoretic Accident Modeling and Processes (STAMP) An accident causation model was formulated by Nancy Leveson (MIT), whose basic idea is that accidents are not caused by some events but rather result from the lack of controls on system design and operation.
Causal Analysis Based on STAMP (CAST) CAST is the methodology used to perform a STAMP analysis of an accident, aiming to identify the related inadequate control actions and accident causal factors. *Case Study 3*: 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 in traditional risk analysis approaches. FRAM is such a methodology.
High Reliability Organizations (HRO) A discussion of high-risk organizations that succeed in avoiding accidents. *Case Study 4*: Aircraft Carrier Flight Operations
Reliability, Conceptual Slack, and Mindfulness of Organizations This topic defines organizational reliability and discusses the importance of maintaining sufficient mindfulness and operational slack. *Case Study 5*: The Diablo Canyon Nuclear Power Plant
NAT, HRO, and the Correct Perspective on Accidents Studies supporting and rejecting Normal Accident Theory. The limitations of High Reliability Organizations. The NAT versus HRO debate and its relevance to the differing views of the STAMP-based and FRAM approaches to accident prevention.
Social Regulation of Technology Agents regulating high-tech industry face an epistemic barrier resulting in dependence on the regulated, compromises their autonomy, and prevents detecting organizational drift toward disaster. This dependence leads to 'regulatory capture' as demonstrated by Aloha Airlines Flight 243 (*Case Study 6*).
Epistemic Accidents These are accidents related to the limits of knowledge. Using composite materials in modern passenger airplanes creates the possibility of such accidents.

References

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

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.

S. Chandra, *Accidents and Disasters*: *Lessons from Air Crashes and Pandemics*, Springer, 2023.

The above books are available in digital form via the U of T Library system. Other reading material consisting of journal articles covering various topics will be made available during the course.

Evaluation

Term paper 1	20%
Term paper 2	30%
Team project report + presentation	40%
Participation	10%

Prerequisites

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

Schedule and Important Dates

Sessions:	Mondays 12 noon – 2 pm	MY 317
	Fridays 1 – 3 pm	SU 255
Duration:	Tuesday, September 3 – Tuesday, December 3	
Add / Drop:	Monday, September 16 / Monday, November 4	
Holiday:	Thanksgiving Day, Monday, October 14	
Reading Week:	Monday, October 28 – Friday, November 1	

Please note that APS440H1 is co-taught with APS1034H.

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