

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. Risk is a social construct.

Syllabus

TOPIC
Accidents as Sociotechnical Events Accidents are not strictly technical events and must be viewed within a social context. The topic includes a 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. <i>Case Study 1: The Ferry Capsizing Accident at Zeebrugge, Belgium</i>
Systems-Theoretic Accident Modeling and Processes (STAMP) A significant enhancement of the Rasmussen systems methodology incorporating an adaptive feedback control-loop strategy was formulated by Nancy Leveson (MIT).
Causal Analysis using Systems Theory (CAST) This topic presents a framework to assist in the STAMP analysis of an accident to identify the related systemic causal factors. <i>Case Study 2: The Walkerton (Ontario) Water Contamination Disaster</i>
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.

<p>Functional Resonance Analysis Method (FRAM)</p> <p>Resilience engineering requires new analysis 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 do. FRAM is such a methodology.</p> <p><i>Case Study 3: RNAV area navigation system for aircraft landing at an airport</i></p>
<p>Turner Disaster Model</p> <p>Disasters arise from an interaction between the human and organizational arrangements of sociotechnical systems that manage complex and ill-structured risk problems.</p>
<p>Normal Accident Theory (NAT)</p> <p>This theory, formulated by Charles Perrow (Yale), claims that accidents in interactively complex and tightly coupled technological systems are inevitable.</p> <p><i>Case Study 4: Nuclear accident at Three Mile Island</i></p>
<p>High Reliability Organizations (HRO)</p> <p>This topic discusses high-risk organizations that succeed in avoiding accidents.</p> <p><i>Case Study 5: Aircraft Carrier Flight Operations</i></p>
<p>Reliability, Conceptual Slack, and Mindfulness of Organizations</p> <p>This topic defines operational reliability and discusses the importance of maintaining sufficient mindfulness and operational slack in an organization.</p> <p><i>Case Study 6: The Diablo Canyon Nuclear Power Plant</i></p>
<p>NAT, HRO, and the Correct Perspective on Accidents</p> <p>Studies supporting and rejecting Normal Accident Theory. The limitations of High Reliability Organizations. The NAT versus HRO debate. Conclusions.</p>

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 Sociotechnical Systems*, Ashgate Publishing, Burlington, VT, 2012.

S. Chandra, *Accidents and Disasters: Lessons from Air Crashes and Pandemics*, Springer, 2023. (Available in digital form via the U of T Library system.)

Other reading material, including journal articles covering various topics, will be available during the course.

Project

The project will consist of a CAST analysis of the collapse of the Algo Mall on June 23, 2012, in Elliot Lake, Ontario. (Due to this accident, the PEO Practice Evaluation and Knowledge program was mandated for practicing professional engineers in Ontario.) Small teams of students will perform the study as a class-wide collaboration with guidance provided by the instructor.

Evaluation

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

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 SS581

Duration: Thursday, May 1 – Tuesday, June 17

Add / Drop: Monday, May 12 / Sunday, May 25

Holiday: May 19 (Victoria Day)

Instructor

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