APS1101H – System-Theoretic Accident and Risk Analysis Summer 2026

Outline

Risk assessments of sociotechnical systems identify hazards that can result in human, material or environmental losses, the likelihood of such hazardous events, and their consequences. Traditional methods typically rely on reliability-based techniques to anticipate accidents before they happen. However, these approaches cannot address social and organizational factors, the interactions between system components that include feedback loops, an organization's adaptation to a constantly changing environment, and human behaviour. Moreover, in automated and increasingly AI-driven systems, accidents frequently arise from complex and unexpected interactions between perfectly functioning, reliable components. This course integrates theory and practice to present a systems-theoretical approach to risk assessment.

Topics

Changes in technology Changes in technology since the 1950s have produced new hazards and led to fundamental changes in the etiology of accidents, mandating different approaches to explain them.
Traditional accident and risk analysis A review of traditional accident causation models and related approaches used in accident and risk analysis. Such approaches assume a critical chain of events and often rely on probability theory to determine the likelihood of physical component or human failures.
Systems thinking A discussion of the general framework of system engineering used to analyze accidents in modern complex systems. Introduces the notion of safety as a control problem.
Accident causal analysis using systems theory A study of the System-Theoretic Accident Model and Processes (STAMP) model of accident causation and its application using the 2004 Vioxx prescription drug recall as an example.
System dynamics System dynamics is used to analyze a sociotechnical system and understand how it evolves from a safe state to an unsafe one, potentially resulting in an accident or disaster.
System-theoretic process analysis (STPA) STPA is a hazard analysis method based on the STAMP model of accident causation. This method is demonstrated by using several examples, including aviation and rail transport.

STPA and the human-machine interface A discussion of how to incorporate the role of humans in complex automated systems using STPA, identify accident causal scenarios related to human-machine interaction (HMI), and understand the context of unsafe operator action. Automated Parking Assist is an example.
STPA and software safety Software safety is a subfield of system safety, and of particular interest is real-time software embedded in automated systems. This topic presents an approach that integrates STPA with software model checking to facilitate the formal verification of control system software.
Safety of AI-enabled control systems Falsification is a practical approach to finding safety violations in AI-enabled control systems. STPA can be used to identify the safety requirements needed in this methodology. This use of STPA is demonstrated for an autonomous unmanned aerial vehicle (UAV).

Team Project (50% of course grade)

The applicability of System-Theoretic Process Analysis (STPA) to prevent and mitigate natural disasters will be explored by student teams as a collaborative class-wide team project using Hurricane Katrina as an example. The instructor will guide this activity, and the students will be expected to present and discuss intermediate progress in the class.

Term Papers (50% of course grade)

The term papers (number TBD) will focus on (a) the meaning of risk and the relevance of social (*i.e.*, psychological, organizational, and political) factors to understanding the sources of failure contributing to major disasters and how such insight can inform risk assessment and prevention, and (b) the use of Large Language Models to assist in performing an STPA analysis.

References

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

This reference is available online via the U of T Library. Other reading material in the form of dissertations and journal articles covering each topic will be available during the course.

Prerequisite

APS1034H (Making Sense of Accidents) is a recommended prerequisite. The course is aimed at students enrolled in the ELITE program but is open to other disciplines.

Instructor

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