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, increasingly AI-driven systems, accidents frequently arise from complex, unexpected interactions among 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 fundamentally altered 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 illustrated with 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.
Causal pathways to AI loss of control Using a simple control system archetype, this topic explores how STPA can identify causal factors and pathways through which loss of control can manifest in AI systems.
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)

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

Term Papers (50% of course grade)

The two term papers 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 frontier AI 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, including dissertations and journal articles covering each topic, will be available during the course.

Schedule and Important Dates

Sessions: Mondays, Tuesdays, Thursdays 5 – 7 pm SS 2120

Duration: Thursday, July 2 – Thursday, August 20

Add / Drop: Monday, July 6 / Monday, July 27

Civic Holiday: Monday, August 3

Prerequisite

APS1034H (Making Sense of Accidents) is recommended as a prerequisite, but APS1101 can also be taken as a standalone course. The course is aimed at students enrolled in the ELITE program but is open to students from other disciplines as well.

AI Tools

AI-assisted tools for English grammar and spellchecking are permitted. Utilizing Large Language Models (LLMs) to summarize journal papers or monographs for essay writing is considered an academic offence. However, this course will explore using LLMs to assist with STAMP analysis and system dynamics modelling.

Instructor

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