APS441H1S/1101H – System-Theoretic Accident and Risk Analysis

Outline

Risk assessment of a sociotechnical system identifies hazards that can result in human, material or environmental losses, the likelihood of such hazardous events, and their consequences. Traditional methods rely on reliability-based techniques to identify the potential for an accident before it occurs. However, such approaches are limited in their ability to account for social and organizational factors, interactions between system components with feedback, the adaptation of an organization to a constantly changing environment, and human behaviour. This project-based course combines theory and practice to present a system-theoretic approach to risk assessment.

Syllabus

TOPIC
Changes in technology Changes in technology since the 1950s produced new hazards and led to fundamental changes in the etiology of accidents that mandate different approaches to explain accidents.
Traditional Accident and Hazard Analysis A review of the traditional accident causation models and related approaches used in risk management. Such approaches assume a critical chain of events and often rely on probability theory to determine the likelihood of physical or human 'component' failures.
Elements of STAMP A first look at the System-Theoretic Accident Model and Processes (STAMP) model of accident causation 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 and potentially results in an accident or disaster.
System dynamics simulation Overview of simulation with a visual program language like Vensim, Anylogic or Stella and its use in implementing a STAMP dynamic model.
Systems thinking 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.
Causal analysis based on systems theory (CAST) CAST is a procedure that uses STAMP to perform an accident analysis. The Wenzhou high-speed train collision in China on July 23, 2011, is used as an example.

System-theoretic process analysis (STPA) STPA is a hazard analysis method based on the STAMP model of accident causation. This is demonstrated by using an example from aviation.
The how-to of STPA Guidance is provided on how to specify or form: system goals, loss events, hazards, safety constraints; the safety control structure; inadequate control actions; context, and causality.
STPA example Demonstration of the application of STPA to a train control system using the IEEE Standard 1474 for the Communication Based Train Control (CBTC) system design.
The role of humans Discussion of how to incorporate the role of humans in complex automated systems using STPA, identify causal scenarios related to human-machine interactions, and understand the operational context of unsafe operator action. Automated Parking Assist is an example.

Team Project (40% of course grade)

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

Term Papers (60% of course grade)

Two term papers will focus on the relevance of social (i.e., psychological, organizational, and political) factors to understanding the sources of failure that contribute to major disasters and how such insight can inform risk assessment and prevention.

Simulation

System dynamics modelling can be optionally performed as part of the project using Vensim programming. The personal learning edition can be downloaded using the following link:

https://vensim.com/vensim-personal-learning-edition/

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 made available during the course.

Prerequisite

APS441H1S/1101H is the second of a two-course series on the systems-thinking approach to accident analysis and risk management. Although not required, APS440H1F/1034H is a recommended prerequisite. The course is aimed at students enrolled in the Forensic Engineering and ELITE programs but is open to all engineering students.

Instructor

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