APS1101H – System Dynamic Risk Assessment July - August 2021

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 feedbacks, the adaptation of an organization in a constantly changing environment, and human behaviour. This project-based course combines theory and practice to present a system-theoretic approach to risk management.

Syllabus

TOPIC
Changes in technology Changes in technology since the 1950s have produced new hazards and led to fundamental changes in the etiology of accidents that mandate different approaches to explain accidents.
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 in the US 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.
System dynamics simulation Overview of simulation with the AnyLogic visual program language and its use in the implementation of 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. It is demonstrated 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

A pandemic prevention and risk management system will be formulated collaboratively by the entire class using System-Theoretic Process Analysis (STPA). Project teams will be expected to present and extend in seminars an analysis from a recent journal article.

Simulation

System dynamics modeling will be performed as part of the project using AnyLogic programming. For a tutorial on this simulation environment see:

https://anylogic.help/tutorials/system-dynamics/index.html

The personal learning edition of AnyLogic can be downloaded using the following link:

https://www.anylogic.com/downloads/personal-learning-edition-download/

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.

Evaluation

Term paper	40%
Team project	60%

Prerequisites

APS1101H is the second of a two-course series on the systems-engineering approach to risk management. Although not required, APS1034H is a recommended prerequisite. The course is aimed at engineering students enrolled in the ELITE Program but is open to all graduate students.

Important Sessional Dates

Sessions:	Mondays, Tuesdays	6-8 PM
Seminars:	Thursdays	6-8 PM
Duration:	Monday, July 5 – Thursday, August 19	
Enroll:	Tuesday, July 13	
Drop:	Friday, July 23	
Civic Holiday:	Monday, August 2	

Remote Learning

The course will be conducted online synchronously and recorded using BB Collaborate. All course material will be posted on Quercus, including PowerPoint presentations and related references.

Instructor

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