

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 behavior. This project-based course combines theory and practice to present a system-theoretic approach to risk management.

Syllabus

TOPIC
<p>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.</p>
<p>Dynamic modeling Discussion of system dynamics modeling and its application to STAMP-based accident analysis. Demonstrated using the Vioxx drug recall.</p>
<p>Team project Discussion of the team project that consists of a STAMP analysis of the 1992 Westray coal mine disaster in Plymouth, Nova Scotia.</p>
<p>System dynamics modeling with Stella Overview of simulation with the STELLA® visual program language and its use in the implementation of a STAMP dynamic model.</p>
<p>Accident models Accident models are used to explain how accidents happen. However, simple models aimed at identifying events that caused an accident are inadequate for preventing future losses.</p>
<p>Traditional accident analysis Review of chain-of-events accident models that underlie the traditional approach to safety analysis, including the domino model, the Swiss cheese model, and root cause analysis.</p>
<p>Traditional hazard analysis Review of the traditional approaches used in risk management, which are based on the chain-of-events model and reliability theory. The discussion covers FTA, ETA, and FMECA.</p>

<p>Shortcomings of failure-based methods</p> <p>Failure-based accident and hazard analysis methods cannot capture failure modes possessed by modern automated industrial systems, nor incorporate human decision-making.</p>
<p>System-based hazard analysis</p> <p>The discussion of traditional approaches for risk analysis is extended to include top-down methods that consider the entire system. The discussion focuses on HAZOP and SHARD.</p>
<p>Changes in technology</p> <p>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.</p>
<p>System engineering</p> <p>Discussion of general framework of system engineering used to analyze accidents in modern complex systems. Provides additional details of the STAMP accident model.</p>
<p>Causal analysis using systems theory (CAST)</p> <p>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.</p>
<p>System theoretic process analysis (STPA)</p> <p>STPA is a hazard analysis method based on the STAMP model of accident causation. It is demonstrated using an example from aviation.</p>
<p>The how-to of CAST and STPA</p> <p>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.</p>
<p>STPA example</p> <p>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.</p>
<p>The role of humans</p> <p>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.</p>

References

- [1] N.G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*, MIT Press, Cambridge, MA, 2011.
- [2] M. Rausand, *Risk Assessment: Theory, Methods, and Applications*, Wiley, 2011.

Both references are 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.

Simulation

System dynamics modeling will be performed as part of the project using Stella programming. For an overview of this simulation environment see:

<https://www.youtube.com/watch?v=IenySRdkRu8&t=1s>

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, Thursdays	5-7 PM
Enroll:	Tuesday, July 14	
Drop:	Friday, July 24	
Duration:	Monday, July 6 – Monday, August 17	

Remote Learning

The course will be conducted online synchronously. All course material will be posted on Quercus, including PowerPoint presentations and related references, and each topic will be discussed in live BB Collaborate sessions.

Instructor

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