ETH zürich

Risk Center Workshop

A Systems Approach to Safety and Security

by Prof. Nancy Leveson, MIT

Wednesday, 3 April to Thursday, 4 April 2019

ETH Zurich, Leonhardstrasse 21, 8006 Zurich, Lecture room LEE E 308 (Wednesday), Lecture room LEE E 101 (Thursday)

Abstract:
STAMP is a new accident causality model based on systems theory and systems thinking described in Nancy Leveson's book "Engineering a Safer World". STAMP extends traditional views of accident causality to include the causal factors in our increasingly complex systems such as software, human-decision making and human factors, new technology, social and organizational design, and safety culture. Two new tools based on STAMP will be covered in depth: STPA is a powerful new hazard/cybersecurity analysis technique while CAST is the equivalent for accident/incident analysis. These tools are now used globally in almost every industry.

There is no required background for the class. It is appropriate for both engineers and social scientists.

Workshop Fee: 300 CHF (including Coffee Breaks and Lunches).
Students are free of charge.

ETH RISK CENTER

A Systems Approach to Safety and Security

by Prof. Nancy Leveson, MIT

Day 1: April 3, 2019 (Lecture room LEE E 308)
9:00 to 17:00 with Lunch Break (12:00 - 13:00)

Part 1: Overview [3/4 day]

Engineered systems are becoming increasingly complex and software-intensive. These changes in engineering are leading to new causes of losses in these systems. At the same time, the traditional approaches to safety engineering, created 50 to 70 years ago, are based on assumptions about system design that are no longer true.

In this half day tutorial, you will learn about a new systems approach to enhancing safety and security that works on today's engineered systems. It starts with a new, expanded model of accident causation called STAMP, which is based on systems theory as a formal foundation. On this foundation, a large number of more powerful engineering and accident/loss analysis tools can be created, including tools for:

- Accident/loss causality analysis
- Hazard analysis and prevention
- Security analysis
- Identification of leading indicators of increasing risk during operations
- Model-based system engineering
- Organizational risk analysis
- Risk assessment
- Occupational/workplace safety
- Design and analysis of safety management systems

These new tools are starting to be used widely in industry, particularly in the automotive and aviation domains, and they are being added to international standards. Parts 2 and 3 of the tutorial will focus on two of these tools.

Part 2: Introduction to CAST (Causal Analysis based on System Theory) [1/2 day]

Accidents and losses are tragic, but not as tragic as not learning as much as possible in order to prevent their reoccurrence. In this tutorial, you will learn an approach to accident causality analysis based on system theory and STAMP. The approach, called CAST, assists in accident understanding through identifying the questions that should be asked during an investigation and by reducing oversimplification of causality and hindsight bias. The result is a more comprehensive and systemic view of the factors involved in the loss. In the tutorial, you will walk through the application of CAST to a real accident.

Day 2: (Lecture room LEE E 101)
08:30 - 15:00 with Lunch Break (11:00 - 12:00)

Part 3: Introduction to System-Theoretic Process Analysis (STPA) [3/4 day]
While learning from adverse events is important in improving safety and security, prevention before these events occur should be our highest goal. STPA is a new, more powerful hazard/vulnerability analysis technique. Hazard analysis has been described as "investigating an accident before it happens." Because STPA is applicable during system concept development, it can be used to drive designs that build in safety and security from the beginning. Like the traditional hazard analysis techniques, it identifies scenarios leading to hazards but it generates more scenarios (what engineers sometimes call the "unknown unknowns') and also derives the system and component requirements necessary to eliminate or mitigate losses. In the tutorial, you will be guided through the STPA analysis of a real system.

About Prof. Nancy Leveson
Nancy Leveson is Professor of Aeronautics and Astronautics and also Professor of Engineering Systems at MIT. She is an elected member of the National Academy of Engineering (NAE). Prof. Leveson conducts research on the topics of system safety, software safety, software and system engineering, and human-computer interaction. She has won many awards, published 300 papers, and is the author of two books: Safeware: System Safety and Computers published in 1995 by Addison-Wesley and Engineering a Safer World published in 2012 by MIT Press. She consults extensively in many industries on the ways to prevent accidents and has served as an expert consultant in many accident investigations including the loss of the Columbia Space Shuttle, Deepwater Horizon, and the Texas City refinery explosion.