Engineering a safer world

April 24 2012, by Jennifer Chu

The cover of Engineering a Safer World: Systems Thinking Applied to Safety (MIT Press). Image: MIT Press

Innovations in software and technology are creating increasingly complex systems: cars that park themselves; medical devices that automatically deliver drugs; and smartphones with the computing power of desktop computers, to name a few. Such complex systems allow us to do things that seemed difficult or impossible just a few years ago.

But Nancy Leveson, professor of aeronautics and astronautics and engineering systems at MIT, says increasing complexity is also making systems more vulnerable to accidents. What's more, she says traditional safety engineering approaches are not very effective in keeping new and fast-evolving systems safe. For example, engineers typically evaluate the

safety of a system by checking the performance of each of its components. Leveson argues that safety — particularly in complex systems — depends on more than a system's individual parts.

For the past decade, Leveson has been championing a new, more holistic approach to safety engineering. In addition to analyzing systems' technical components, her approach — dubbed STAMP, for System-Theoretic Accident Model and Processes — addresses the impacts of human, social, economic and governmental factors on safety.

Last week, Leveson hosted a three-day workshop at which more than 250 safety engineering professionals from around the world gathered to learn about STAMP and to explore the event's theme, "Engineering a Safer World." The event also coincided with the publication of Leveson's new book on the topic, titled Engineering a Safer World: Systems Thinking Applied to Safety.

The workshop drew participants from industries including aviation and automotive engineering, occupational health, missile defense, road tunnel safety, and medicine, some of whom gave presentations during the workshop.

In many cases, safety analyses are performed only after an accident has occurred. Several researchers at the workshop presented cases in which they used Leveson's approach to identify causes of accidents.

Daijiang Suo, a graduate student in computer science at Tsinghua University, reconstructed a 2003 train accident that killed 40 people in southwest China. Engineers originally determined that lightning caused a track circuit to malfunction, causing the train to derail. Using Leveson's approach, however, Suo expanded the parameters of safety to include other factors, ultimately attributing the accident in part to communication issues between operators and in part to pressure to keep

the train on schedule.

Stathis Malakis, an air traffic controller and human factors researcher for the National Technical University of Athens, is analyzing the safety of helicopters that provide emergency medical services in Greece. When these helicopters crash, authorities write up accident reports, although Malakis says many reports are not released until much later.

“It’s interesting that after three decades, we have never revisited accident reports,” Malakis said. “What can we unearth about these accidents to prevent further accidents?”

Malakis is using STAMP to answer this question, looking for patterns among multiple accident reports.

“It’s much better to do this analysis at the beginning rather than right before a system is deployed,” said Grady Lee, president of Safeware Engineering Corporation, a company he started with Leveson. Lee was one of the first to adopt Leveson’s approach for a real-world application, using the technique to evaluate the U.S. Ballistic Missile Defense System. Lee found that while each individual component of the system worked well, together the components experienced problems. Following Leveson’s plan, Lee tested the components under various scenarios, identifying weaknesses in the system.

“Safety is always against the grain,” Lee said. “Everyone is success-oriented, and you want to say, ‘Wait a minute.’ But at the end of the day, if it doesn’t fall apart, you’re happy.”

Qi van Eikema Hommes, a research scientist in MIT’s Engineering Systems Division, is using Leveson’s technique to identify potential hazards of adaptive cruise control systems in cars. Hommes said that technology — particularly software — is evolving at such a rapid pace

that it is no longer feasible to assess a system's safety using conventional approaches.

"What are the implications of automating all these tasks on system safety?" Hommes asked. "We're playing in a dangerous field here."

While most engineers are employing Leveson's technique to evaluate technical systems, Marvin Dainoff, director of the Center for Behavioral Science at the Liberty Mutual Research Institute for Safety, is employing the approach in the occupational safety arena. In 2010, more than 4,500 people died from occupational injuries, "equivalent to two fully loaded 747s crashing each month," Dainoff said.

Overexertion and falls are mostly to blame. Dainoff is studying a slice of the problem, in the food services industry. Specifically, Dainoff is using Leveson's technique to identify the causes of slips and falls in restaurant kitchens.

"There's low-hanging fruit here," Dainoff said. "Can we use this technique? At this point, we're learning."

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology