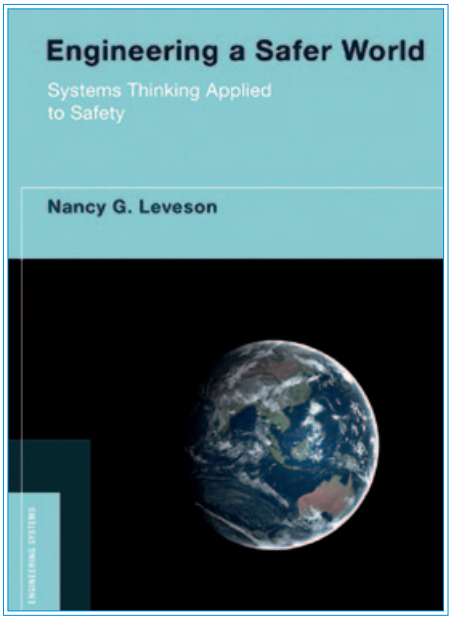
Engineering a Safer World

Systems Thinking Applied to Safety

By Nancy Leveson



The MIT Press (January 13, 2012), Nancy Leveson, MIT.

Engineering is facing every day a set of new challenges, caused by a steady technological revolution and by our increasing reliance on systems of increasing complexity. Yet, the basic engineering techniques applied in safety and reliability engineering, created for a simpler, analog world, have changed very little over the years. In the book "Engineering a Safer World – Thinking Applied to Safety", Nancy Leveson, Professor of Aeronautics and Astronautics and also Professor of Engineering Systems at MIT *and IAASS fellow, describes a new approach to safety and risk management, better suited to today's complex, socio-technical, software-intensive world.*

A Case for STAMP

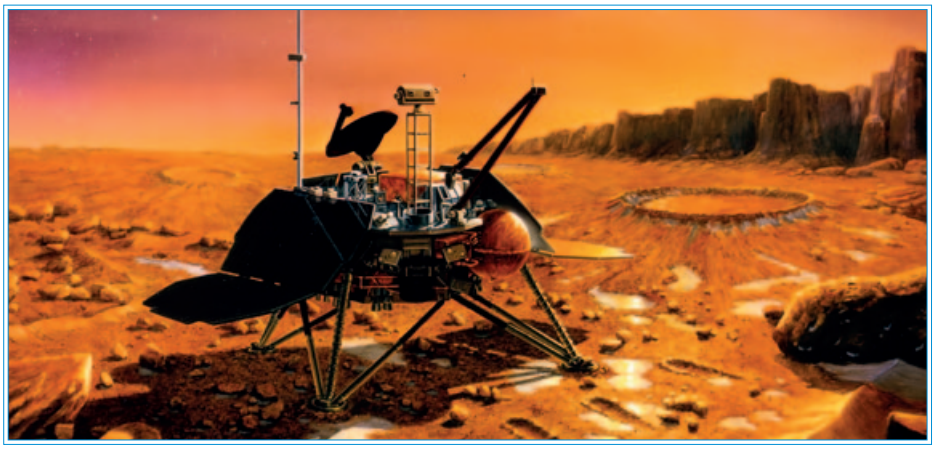
STAMP is a new model of accident causation in complex systems. The traditional model that thinks of accidents as caused by component failures was adequate for the relatively simply electro-mechanical systems for which it was created, but it does not fit the more complex, software-intensive systems we are building today. Accidents, such as the loss of the Mars Polar Lander, are increasingly likely to result from interactions among system components that have not failed, but satisfy their specifications (which were inadequate). The real problems lie in system engineering and flaws in the component requirements specifications and the system design. These problems need to be handled by improved system engineering supported by a top-down hazard analysis technique rather than simply by bottom-up reliability engineering. For Mars Polar Lander, and many other space mishaps, no components failed, in that each satisfied its specification but the understanding by the component developers of the required behavior was incorrect or incomplete. Many of these "component interaction accidents" have been related to software and flawed software requirements.

> "STAMP extends the old failure model of accident causation to include new types of accident causes"

STAMP extends the old failure model of accident causation to include these new types of accident causes. It redefines the safety problem in terms of control engineering rather than reliability engineering. Preventing component failure is still part of the solution, but the overall problem is changed to a control problem, where the design goal becomes the enforcement of behavioral constraints on the system as a whole and on the components.

STPA (System-Theoretic Process Analysis) is the new hazard analysis based on the STAMP model of accident causality. This hazard analysis method uses basic control theory approaches to identify hazard causes and to generate safety requirements for the individual system components.

STPA can be used early in the system design process, including even high-level architectural tradeoff decisions, to build safety into the system rather than waiting until a design is completed to analyze whether it is safe. In later stages of development, the cost of making changes (rework) may be exorbitant and the most effective design features for preventing losses may no longer be possible to incorporate.



Artist's conception of Mars Polar Lander, which crashed into Mars in 1999 due to an interaction problem among otherwise working components. - Credits: NASA/JPL

> "Systems thinking will be needed to increase our probability of success in new missions"

Success Stories

While the actual publication of *Engineering a Safer World* is very recent, drafts have been available for a while. We and others have been trying STPA on a large variety of real systems, including spacecraft, medical devices, autos, railroads, aircraft, nuclear power, and defense systems. In all cases, STPA found the accident scenarios identified by the engineers using traditional Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA), but also found important paths to mishaps that the other traditional techniques did not—and could not—identify. In space, for example, JAXA has been experimenting and using STPA on the HTV, on a new scientific satellite, and on the early architectural tradeoff analysis for their planned crew vehicle. The results have been described in papers presented at IAASS conferences. In defense, the deployment and field testing of the new U.S. ballistic missile system was delayed for six months to fix all the paths to inadvertent launch found during the application of STPA in a non-advocate risk assessment right before the system was to be deployed.

One of the most surprising results we have found is that not only is STPA more powerful than current hazard analysis techniques, it also appears to be easier to use, according to the feedback we are getting, and less costly. Safety engineering activities are often not cost-effective. *Engineering a Safer World* provides some reasons for this problem and presents a more cost-effective way to manage system safety.

In addition to the new hazard analysis technique, the book describes a new structured, more comprehensive mishap analysis technique, called CAST (Causal Analysis based on System Theory), using the STAMP model as a foundation. CAST has been used on dozens of real accidents and identified many more causal factors, including flawed organizational design and management decision making that contributed to the loss than were identified in analyses based on standard practice.

The H-II Transfer Vehicle (HTV) cargo spacecraft that was developed by JAXA using STPA (System-Theoretic Process Analysis). - Credits: NASA

The Human Factor

Accident analysis and hazard analysis often stop with some unsafe operator action or inaction and then assign blame to the human operator. STAMP helps to identify the design and contextual features that contributed to the erroneous actions or flawed decision-making so that similar errors can be prevented in the future. *Engineering a Safer World* contains information about how to better understand human error in accident investigations and also about how to design systems from the beginning to reduce human error.

Operability needs to be considered from the start of the development process and appropriate information documented and passed to the system operators. My new book describes what information needs to be documented and how to use this information to create a safety management operations plan. It also discusses how to design important safety-related operations functions such as managing and controlling changes and creating feedback channels to detect performance changes that may be leading to increased risk during operations.

Safety has to be carefully managed. A chapter is included in the book on how to manage safety in complex system development and in operations. Another chapter describes the very successful nuclear submarine safety program, called SUBSAFE, and the approaches used in this program that have allowed the U.S. to avoid losing a submarine in the last 49 years since the program's inception in 1963 after the Thresher loss.

Final Remarks

To improve the success of our new space ventures, we need to go beyond the techniques and processes created decades ago for much simpler systems. They are not powerful enough for the increased complexity and new technology being incorporated into today's spacecraft. Systems thinking will be needed to increase our probability of success in new missions. The techniques and ideas in *Engineering a Safer World* are a start, but we will need to improve and build on them for the future.

Prof. Nancy Leveson, IAASS Fellow Member, has conducted research on all aspects of system safety including design, operations, management, and social aspects. She has published over 200 research papers and two books. She served on the NASA Aerospace Safety Advisor Panel and was a consultant to the Columbia Accident Investigation Board and an expert advisor to the Presidential Oil Spill Commission.