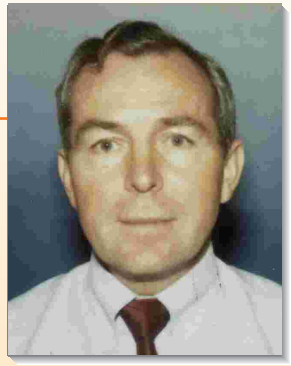
PRESIDENT'S MESSAGE



Against the background of the recent publication of the NASA Columbia Space Shuttle investigation report and the 20th anniversary of Bhopal I have recently been involved in professional development training and auditing. This has led me to think more deeply about system safety, as the failure of the safety management systems is a root cause in these incidents and many other incidents.

The traditional approaches to safety management are necessary but insufficient. For example the classic approach of energy sources and barriers addresses the risk management of energy sources but does not provide insight into broader safety management systems issues. Often incident investigation processes look for fault and frequently blame the victim. Unfortunately these approaches do not address the root causes of many incidents. They do not identify failures of the safety management systems.

In my search for information I came across several interesting sources.

Firstly from the Massachusetts Institute of Technology. MIT is publishing its course materials under the MIT Open Courseware program (http://ocw.mit.edu) to make such materials freely available on the web for all to use. One of these courses is by Professor Nancy Leveson titled "System Safety" (http://ocw.mit.edu/OcwWeb/Aeronautics-and-Astronautics/16-358JSystem-SafetySpring2003/CourseHome/). I found this course very interesting. However the real strength of the course is not in the PowerPoint slides, as these are only memory props for the lecturer. The real strength of the course is that Professor Leveson has the draft of her next book "A New Approach to System Safety Engineering" on the website. I found this excellent reading. So much so I bought her earlier book "Safeware: System Safety and Computers".

In her books Leveson develops the concept of systems safety. In particular she addresses the use of software as it is a poorly managed component in our safety management systems. We can predict failures of plant equipment but we cannot predict software failures. Software uses a generic machine, the computer, to carry out its instructions. Unlike hardware, software does not wear out and fail in predictable ways. Most of our software systems are quite complex and cannot be guaranteed to be free of bugs. There are many examples of incidents related to safety management system failures in her books. They include several incidents from the chemical processing industry. Professor Leveson includes one incident, attributed to Trevor Kletz, where both the operator and the computer followed their instructions correctly, but an incident still happened.

Professor Leveson uses the term systems theory for the analyses and design of the whole as distinct from the parts. She believes that our plant systems are too complex for complete analysis and too disorganised for statistical analysis.

Professor Leveson analyses safety management systems using two ideas. The first is emergence and hierarchy. An emergent property arises when components of the system interact with each other within a larger environment. In the hierarchy, each level of the organisation is more complex than the one below. Some properties characteristic of a level are irreducible. The second idea is communication and control.

In the model of accidents used with systems theory, accidents arise from interactions among humans, machines, and the environment. Accidents are not simply a chain of events or linear causality. Accidents arise from more complex causal connections. Safety is enforced by a set of constraints related to the behavior of the components of the system. When appropriate constraints are lacking, or not managed, incidents will occur.

Many examples of serious computer software failures are available on the internet.

I found Professor Leveson's books very useful. She provides an analysis of our current safety management tools and suggests ways to manage safety, both software and organisational. I think you may also find her ideas useful.