Progress Report: Diagnosis and Design of Complex Systems Software

Goals

(1) This project is a continuation of research which began many years ago.

The intent is to develop study, analyze, design and ultimately improve complex systems software. The study of complex systems failures has taken us far afield over the years, including nuclear power stations (Three Mile Island, (1980), Chernobyl, (1986)), Air disasters (including TWA FL 800, (1996), The Swissair crash over Newfoundland, (1998), Korean Air Flight 801, (1983), the Space Shuttle (1986), Chemical Plants (Bhopal, (1984), and Seveso (1976), Defense accidents (NORAD, (1979-80), Iranian Airbus Flight 655 (1988), Sea disasters (Exxon Valdez, (1989), Estonian Ferry (1994), and Medical Disasters (Therac-25, (1986), The London Ambulance Service (1987 - 1993) to name a few. Arguably, many of these systems failures did not specifically involve software design failures – but we feel that their "epitaphs" are generally helpful towards our understanding complex systems and the important role that software can play in helping to avert disasters.

In October, 2000 Ms. E. Haas started to work for me (5 hours per week) as an undergraduate research assistant; and in November, 2000 Mr. K. Khan started to work (6 hours per week) as a graduate research assistant. Their primary task has been to help me find, organize, and assemble research material related to a number of complex systems accidents, particularly those involving software.

(2) My research assistants and I are exploring a number of software and complex systems modeling tools such as STELLA, UML, and Rational Rose, as well as diagnostic expert systems shells. Such investigations are also helping to enhance my computer science course offerings in Software Methodology and Artificial Intelligence. We have been able to focus our primary area of research to software involving medical information systems.

(3) When we have carried out the relevant background research, documenting the medical software information systems failures to date, and having explored the various modeling and design tools available, we will embark on the deep study of prevalent existing medical information systems. From our study, hopefully in cooperation with a suitable hospital contact, we hope to be able to analyze medical information systems and make definitive suggestions for design improvements. Initial contacts have been made with Mount Sinai hospital and North Shore University Hospital.

Our primary area of research in these past few months have been to document and analyze past cases of complex system failures. The repercussions of these system failures range from minor inconveniences (i.e.- faulty mailing systems), to major catastrophes which could have been prevented with some basic precautions (i.e.- incidents in hospitals, airports, army bases and so on). Each case study that we have reviewed, serves as a motivational factor to better identify and focus our research on this domain. The tracing of software problems in each incident and considerations for how these "bugs", which, in some instances, put so many lives at risk, might be eliminated, is our primary concern.

Tools

STELLA

The STELLA software has been the gold standard for model building and simulation software since its development and introduction in 1985 by High Performance Systems. STELLA provides tools for rendering, simulation, analysis and communication of our mental models. Mental models help us to construct meaning out of what we experience, share that meaning by communicating with others, and decide upon appropriate courses of action. The aim of the STELLA software is to accelerate and enrich these mental models. STELLA uses the following tools when constructing a model.

- Parts of speech (words) stocks, flows, converters
- Sentences flows processes
- Paragraphs feedback loops
- Short stories infrastructures

STELLA has many diverse applications. For example, it has been used to simulate the SELTRAC (monorail) System. The SELTRAC System embodies elements of Artificial Intelligence that allow vehicles (trains) to operate without human supervision.

Methodology

Each incident that we document is to be catalogued into a custom built database which accommodates various data that is crucial to uniquely identifying each incident. The data fields will include obvious information, such as Date, Location, Brief Description, People Involved, Software Used and so on. We are also in the process of developing a rating system where each incident is evaluated according to event- type (category, e.g. Air, Ship, Medical, Business), number of casualties involved, deaths, financial consequences, environmental consequences, etc. Then the data will be analyzed to determine if some meaningful patterns can be identified, particularly as they relate to software, people, and design issues.

We have decided that the primary area that our research will be software in the health field. This is an issue which has affected every single one of us at one point or another in our lives. In November, 1999 a report by the United States Institute of Medicine entitled "To Err is Human: Building a Safer Healthcare System", stated that somewhere between 44,000 and 98,000 people die in hospitals every year as a result of medical errors. **Our research question, in this regard is, how many of these deaths are caused by faulty or poorly designed software? If we can identify any improvement in software design that would save even one life, our mission would be accomplished.**

One such example involved the computerized radiation therapy system called Therac-25. In the span of two years, this medical accelerator, which was used to reduce the size of tumors and other cancerous growths, was involved in a series of deaths caused by massive radiation overdose. The accidents that occurred as a result of Therac-25 have been considered by some to be the most serious computer related catastrophes in the medical field. Medicinal programs used all over the country, SMS and MEDSTAT have come to our attention as well, and will fall under the scrutiny of our evaluations on their safety properties.

Our investigation has also led us to other areas, such as airports, nuclear power plants, army bases and software manufacturers. By studying these cases we hope to determine repeating patterns in these various instances and heighten the awareness of people who put too much trust into technology today.