Computer Science 773

Robotics and Real-time Control

THE THERAC ACCIDENTS

The attached paper describes in some detail a series of accidents (for want of a better word) which came about in the use of a computer-controlled radiation therapy machine, and presents a detailed analysis of the cause of the accidents. I recommend that you read it carefully, and learn from it what you can.

I had originally intended to give you selected excerpts from the paper, but on reading it again decided that there was very little that could be omitted without missing out something significant, so it's all here.

A FEW SELECTED QUOTATIONS :

- "A significant amount of software for life-critical systems comes from small firms ... that fit the profile of those resistant to or uninformed of the principles of either system safety or software engineering."
- "It is still a common belief that any good engineer can build software ..."
- "Most accidents are system accidents; that is, they stem from complex interactions between various components and activities."

REFERENCE.

N.G. Leveson, C.S. Turner : "An investigation of the Therac-25 accidents", *IEEE Computer* **26#7**, 18-41 (July, 1993).

Alan Creak,
April, 1997.