Review report

Review object (topic): Topic02.ppt
Version: Apr.16,2003
Reviewer: D. Bojic
Date: May.17,2003
---

1. General remarks and general impression concerning the
   state of the review object

  - somewhere on slides should be a reference to topic on measuring software quality
    Some good measures of external quality factors are given in
    N.E. Fenton, S.L. Pfleeger, Software Metrics, A Rigorous & Practical Approach

2. Technical errors and misspellings in the slides

   Slide 2 (and general): question mark should be written next to last word? without space

  - In the footer of each slide, there is a copyright (C) sign, but there is no year.

3. Physical errors in the slides

  (e.g. the order of animated parts)

4. Slides with a bad style and suggestions for improvements

  (e.g. too much contents, too textual)

5. Additional suggestions for improvements and and extentions

  - some introductory "motivation" slides maybe should be added:
    e.g. graph showing the rise of the relative cost of correcting an error
         later it is detected in the development process

  - some "horror story" like Therac 25 disaster, a radiation therapy machine that
    massively overdosed 6 people due to software bug (the story is attached at the
    end, I found it in the lecture of Daniel M. Berry "Myths and Realities in Software
    Development", Technion Univ.)

6. Lecture notes for particular slides:

   Slide 14 notes: write "nearly" instead of "neaerly"

--- optional parts (later): ------------------

7. Deviations from the style guides

  (e.g. slide 3: question to students not in a cloud)

8. Experience report from a lecture:

  - conveniences and inconveniences
  - involvement of students (by questions)

9. Experience with the translation into the native language

Therac 25 Disaster
Between June 1985 and January 1987, the computer-controlled radiation therapy machine Therac-25 massively overdosed 6 people, all of whom developed severed radiation sickness and all but 1 of whom has died (as of 1994). It was the worst accident in the history of radiation therapy machines.
A study by Nancy Leveson showed that earlier machines, the Therac-6 and Therac-20, were controlled by computer, but the computer was added after the machines had been available with electromechanical (EM) controls. In particular, the safety controls were still EM even after the addition of the computer.
In the Therac-25, designed from the start with computer control, more of the control, including the maintenance of safety, was given to the computer.
Software checks were substituted for many of the traditional hardware interlocks.
Nominally, this was a good plan; they reused code that appeared to be reliable.
The problem was that the Therac-20 was a reliable system!
The original Therac-20 software had a bug that just never showed up because the independent hardware interlocks prevented overdoses.
When they programmed the new checks into this buggy code, and they happened to never duplicate the error causing situation in the tests, the old bug was never discovered and

reared its ugly head later with fatal results.
After much denial and protestation that the overdose was impossible, the manufacturer was forced to put the independent hardware interlocks back into the machine, just to be sure, even after they had found and fixed the bugs.