System design techniques

- Quality assurance.

Quality assurance

- Quality judged by how well product satisfies its intended function.
  - May be measured in different ways for different kinds of products.
- Quality assurance (QA) makes sure that all stages of the design process help to deliver a quality product.

Therac-25 Medical Imager (Leveson and Turner)

- Six known accidents: radiation overdoses leading to death and serious injury.
- Radiation gun controlled by PDP-11.
- Four major software components:
  - stored data;
  - scheduler;
  - set of tasks;
  - interrupt services.

Therac-25 tasks

- Treatment monitor controlled and monitored setup and delivery of treatment in eight phases.
- Servo task controlled radiation gun.
- Housekeeper task took care of status interlocks and limit checks.

Treatment monitor task

- Treat was main monitor task.
  - Eight subroutines.
  - Treat rescheduled itself after every subroutine.

Software timing race

- Timing-dependent use of mode and energy:
  - if keyboard handler sets completion behavior before operator changes mode/energy data, Datent task will not detect the change, but Hand task will.

Software timing errors

- Changes to parameters made by operator may show on screen but not be sensed by Datent task.
- One accident caused by entering mode/energy, changing mode/energy, returning to command line in 8 seconds.
- Skilled operators typed faster, more likely to exercise bug.

Leveson and Turner observations

- Performed limited safety analysis: guessed at error probabilities, etc.
- Did not use mechanical backups to check machine operation.
- Used overly complex programs written in unreliable styles.

ISO 9000

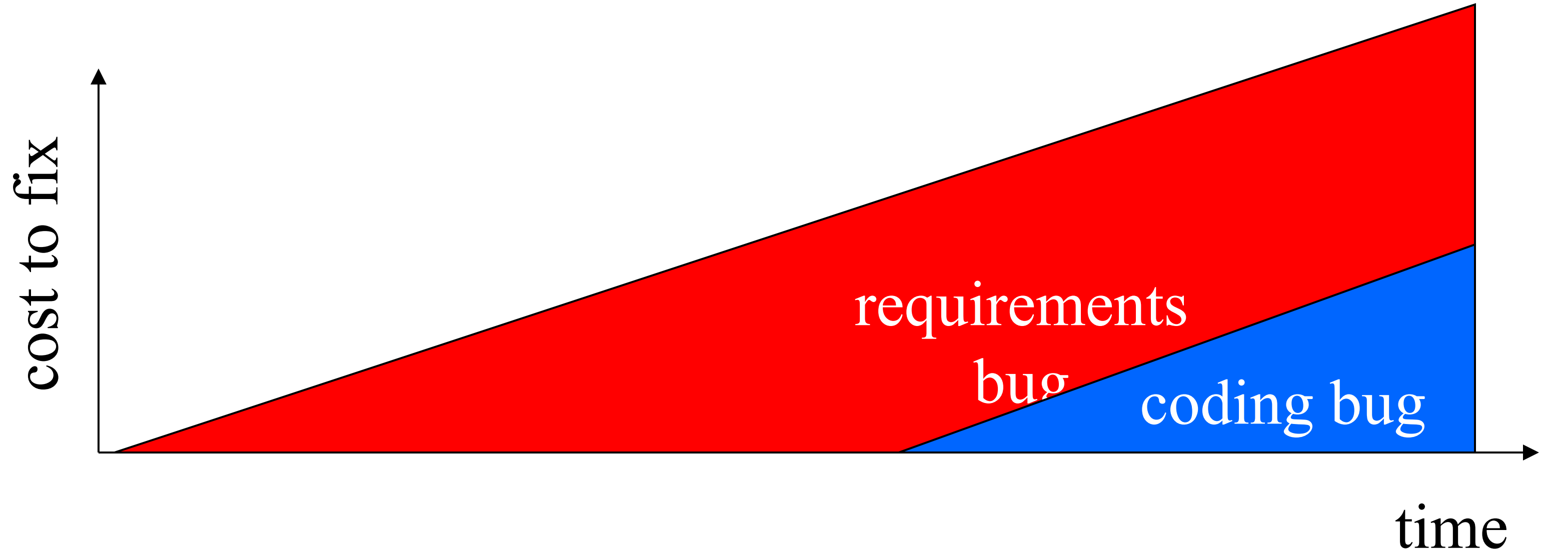
- Developed by International Standards organization.
- Applies to a broad range industries.
- Concentrates on process.
- Validation based on extensive documentation of organization’s process.

CMU Capability Maturity Model

- Five levels of organizational maturity:
  - Initial: poorly organized process, depends on individuals.
  - Repeatable: basic tracking mechanisms.
  - Defined: processes documented and standardized.
  - Managed: makes detailed measurements.
  - Optimizing: measurements used for improvement.

Verification

- Verification and testing are important throughout the design flow.
- Early bugs are more expensive to fix:



Verifying requirements and specification

- Requirements:
  - prototypes;
  - prototyping languages;
  - pre-existing systems.
- Specifications:
  - usage scenarios;
  - formal techniques.

Design review

- Uses meetings to catch design flaws.
  - Simple, low-cost.
  - Proven by experiments to be effective.
- Use other people in the project/company to help spot design problems.

Design review players

- Designers: present design to rest of team, make changes.
- Review leader: coordinates process.
- Review scribe: takes notes of meetings.
- Review audience: looks for bugs.

Before the design review

- Design team prepares documents used to describe the design.
- Leader recruits audience, coordinates meetings, distributes handouts, etc.
- Audience members familiarize themselves with the documents before they go to the meeting.

Design review meeting

- Leader keeps meeting moving; scribe takes notes.
- Designers present the design:
  - use handouts;
  - explain what is going on;
  - go through details.

Design review audience

- Look for any problems:
  - Is the design consistent with the specification?
  - Is the interface correct?
  - How well is the component's internal architecture designed?
  - Did they use good design/coding practices?
  - Is the testing strategy adequate?

Follow-up

- Designers make suggested changes.
  - Document changes.
- Leader checks on results of changes, may distribute to audience for further review or additional reviews.

Measurements

- Measurements help ground our beliefs:
  - Do our practices really work?
  - Do they work where we think they work?
- Types of measurements:
  - bugs found at different stages of design;
  - bugs as a function of time;
  - bugs in different types of components;
  - how bugs are found.