Faculty of ECMS / School of Computer Science

Software Engineering & Project Ethics

adelaide.edu.au

seek LIGHT

Ethics

Lecture 17

Ethics

- What are ethics?
- What is morality?

“The root of all superstition is that men observe when a thing hits -but not when it misses.”
-- Francis Bacon

Ethics

- Ethics – a systematic reflection on what is moral
- Morality – the totality of opinions, decisions, and actions with which people express, individually or collectively, what they think is good or bad.

What do you think?
-An employee knowingly misled a superior, to protect themselves, in the presence of the researcher and the researcher knew the employee was misleading the superior.
-Findings of a research project are too broad, to make a final judgment, although the researcher knew the details reveal weaknesses.

- Common sense? (intoxicated mother drives with child to hospital after a severe condition – saves child – she is fined – morally incorrect?

Software engineering ethics

- Software engineering involves wider responsibilities than simply the application of technical skills.
- Software engineers must behave in an honest and ethically responsible way if they are to be respected as professionals.
- Ethical behaviour is more than simply upholding the law but involves following a set of principles that are morally correct.

Issues of professional responsibility

- Confidentiality
  - Engineers should normally respect the confidentiality of their employers or clients irrespective of whether or not a formal confidentiality agreement has been signed.
- Competence
  - Engineers should not misrepresent their level of competence. They should not knowingly accept work which is outwith their competence.

Issues of professional responsibility

- Intellectual property rights
  - Engineers should be aware of local laws governing the use of intellectual property such as patents, copyright, etc. They should be careful to ensure that the intellectual property of employers and clients is protected.
- Computer misuse
  - Software engineers should not use their technical skills to misuse other people's computers. Computer misuse ranges from relatively trivial (game playing on an employer's machine) to extremely serious (dissemination of viruses).

ACM/IEEE Code of Ethics

- The professional societies in the US have cooperated to produce a code of ethical practice.
- Members of these organisations sign up to the code of practice when they join.
- The Code contains eight Principles related to the behaviour of and decisions made by professional software engineers, including practitioners, educators, managers, supervisors and policy makers, as well as trainees and students of the profession.

Rationale for the code of ethics

- Computers have a central and growing role in commerce, industry, government, medicine, education, entertainment and society at large. Software engineers are those who contribute by direct participation or by teaching, to the analysis, specification, design, development, certification, maintenance and testing of software systems.
- Because of their roles in developing software systems, software engineers have significant opportunities to do good or cause harm, to enable others to do good or cause harm, or to influence others to do good or cause harm. To ensure, as much as possible, that their efforts will be used for good, software engineers must commit themselves to making software engineering a beneficial and respected profession.

The ACM/IEEE Code of Ethics

Software Engineering Code of Ethics and Professional Practice

ACM/IEEE-CS Joint Task Force on Software Engineering Ethics and Professional Practices

PREAMBLE

The short version of the code summarizes aspirations at a high level of the abstraction; the clauses that are included in the full version give examples and details of how these aspirations change the way we act as software engineering professionals. Without the aspirations, the details can become legalistic and tedious; without the details, the aspirations can become high sounding but empty; together, the aspirations and the details form a cohesive code.

Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:

Ethical principles

1. PUBLIC - Software engineers shall act consistently with the public interest.

2. CLIENT AND EMPLOYER - Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.

3. PRODUCT - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.

4. JUDGMENT - Software engineers shall maintain integrity and independence in their professional judgment.

5. MANAGEMENT - Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.

6. PROFESSION - Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.

7. COLLEAGUES - Software engineers shall be fair to and supportive of their colleagues.

8. SELF - Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

Ethical dilemmas

- Disagreement in principle with the policies of senior management.
- Your employer acts in an unethical way and releases a safety-critical system without finishing the testing of the system.
- Participation in the development of military weapons systems or nuclear systems.

Ethical questions

Ethical concerns are not ***descriptive*** but ***prescriptive*** (or ***normative***)

- not a question of what ***does*** happen, but what ***ought to*** happen

- Should censorship be applied to the Internet, and if so, what should be censored?
- Should computers be allowed to take the place of humans in the workforce, and in jobs of what kinds?
- Are people entitled to make whatever use they like of information they gain by means of their own computers, and who should have access to what information?
- Should employers be allowed to read the e-mail of their employees?
- ... and many much greyer areas

Philosophical Basis: Two (basic) views

- An act is “good” if the outcome is good… (?)…
  - (**Teleological ethics**, also consequentialism)
  - Not very simple!
- An act is “good” by itself, with regard to intention, outcome or who is doing it.
  - This is duty-based ethics, or **deontological** ethics.
- We usually adopt a hybrid of these.

Utilitarianism

- …all is “ok”…(good)
- A branch of consequentialism.
- “the maximum good for the maximum number”

- How do we define good?
- How do we compare actions?
- Under this, we could break the rules for the greater good.

Utilitarianism examples

Lockheed Tristar

In 1970s president of Lockheed was accused of paying $12 million bribes to Japanese officials to persuade them to buy Lockheed Tristar

- beneficial to many US constituencies
- social good to stockholders
- benefits to Lockheed's suppliers, employees, communities
- benefit to US economy
- dangers of bribery in a free enterprise system?
- impaired level of trust in society?

Pinto Ford car 1994.. fuel tank re-positioning / cost to company – several million - costs of life 200k -

Utilitarianism consequences

- There are no intrinsically evil acts
  - what matters first and foremost are the consequences
- Even human and moral rights are not absolute
  - a person's or group's rights can be taken away in the interests of maximising utility
- Assumes that various "goods" are commensurable
  - e.g. car manufacturer installing safer rear seat belts
  - save 10 lives per year or save $87 M?
- Can managers and professionals objectively evaluate the greatest good
  - avoid self-serving assumptions and prejudices

Kantian Ethics

- Immanuel Kant, 18th Century philosopher.
- Categorical imperative (deontological):
  "Act only according to that maxim (a subjective rule or policy or action) by which you can also will - that it would become a universal law"
- Goodness depends of taking the right actions.
- Consequences less important because of moral luck - intention is far more important.

Duty-based ethics consequences

- Kant's theory has a certain inflexibility and rigidity
- If it is wrong to tell lies, then it is always wrong to tell lies
  - e.g. it is wrong to lie to a criminal even if that might save the life of an innocent person
- When two laws conflict, it is difficult to avoid an appeal to consequences
  - e.g. lying vs saving innocent lives

Principles of Ethics in Software Engineering

Principle	Description
Public	Software engineers shall act consistently with the public interest.
Client and Employer	Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.
Product	Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
Judgment	Software engineers shall maintain integrity and independence in their professional judgment.
Management	Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
Profession	Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
Colleagues	Software engineers shall be fair to and supportive of their colleagues.
Self	Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

Source: IEEE Computer Society, Software Engineering Code of Ethics and Professional Practice. 2010.

Ethics in Software Engineering

- Ethics in Software Engineering - very similar to other engineering ethics in general
  - Responsibilities
    - In professional activities, take due responsibilities
    - Be fair to and supportive of their colleagues
  - Quality of Life
  - Use of Power
  - Safety
  - Property Rights
  - Privacy
  - Equity and Access
  - Honesty and Deception

  Several special characteristics
  - Data confidentiality (privacy (private data: medical records, bank information))
  - Specific domains such as medical equipment that are related to the treatment and diagnosis of diseases.

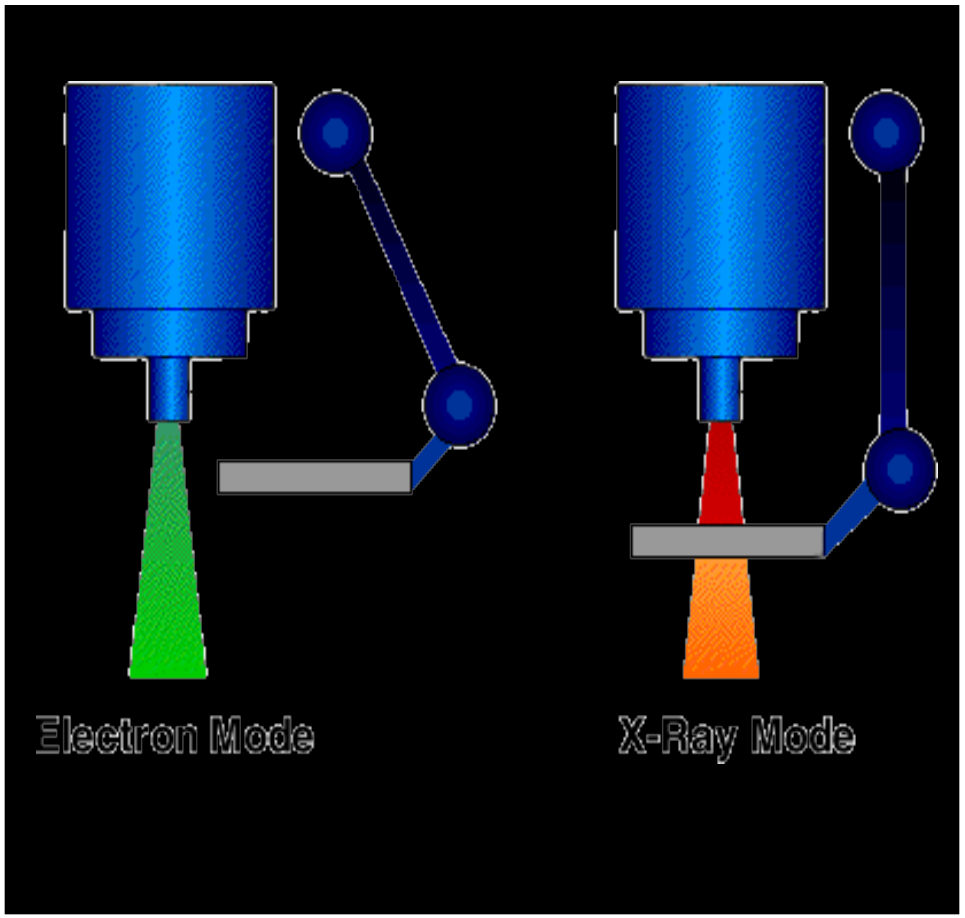
Ethics case-study: Therac-25 (1/4)

- Radiation therapy machine
- Medical linear accelerator for destroying tumours
- Successor to Therac-6 and Therac-20
- 11 Therac-25 machines used in US and Canada

An Investigation of the Therac-25 Accidents
Source: IEEE Computer, Vol. 26, No. 7, July 1993, pp. 18-41.

Therac-25 Design (2/4)

- Dual mode
  - Electrons for shallow tissue
    - Use relatively low energy beam
    - revolving magnets spread the beam to a safe concentration
  - X-rays for deep tissue
    - Higher level energy beam is required
    - An attenuator trims the beam



Mechanical Design (3/4)

- Mode changed by moving turnstile
  - Interlocks should prevent treatment in the incorrect mode
- Intensity of mode controlled
  - Magnets for electron mode
  - Computer control of beam energy of X-ray…software…

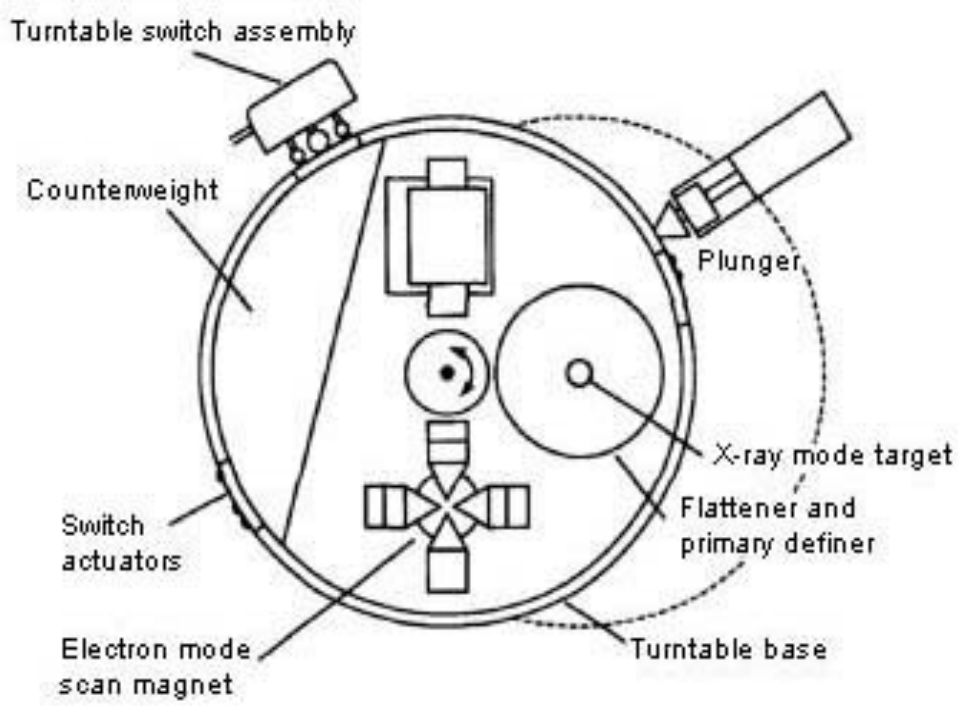


Figure B. Upper turntable assembly

Comparison of the Two Systems (4/4)

- Therac 6 and Therac 20
  - Systems based upon mechanical controls
  - Some computer assistance - But can run with no computer
- Therac 25
  - ❖ Run with only computer control - more software control
    - ➢ Monitors status
    - ➢ Sets up the machine
    - ➢ Turns the beam on and off according to operator commands
    - ➢ Also shuts the beam off if a fault occurs
    - ➢ The operator only needs to enter the data, it is the software that actually operates the machine
- Some software reused from earlier versions - Two different software bugs led to accidents
  - The same bugs were later found in Therac-20
  - But hardware interlocks prevented accidents

GENERAL - Safety in Design

- Manufacturer performed fault tree analysis ??
- Used “chance in a billion” odds for software failure ??
- Analysis only based upon mechanical wear and malfunction ??
- Software coded in Assembler
- One programmer ??
- Programmer tested own code ??

Software Design errors

- Concurrent tasks
  - A clock interrupt service routine
  - A scanning interrupt service routine
  - Traps (for software overflow and computer-hardware generated interrupts)
  - Power up (initialise the system and pass control to the scheduler)
  - Treatment console screen interrupt handler
  - Treatment console keyboard interrupt handler
  - Service printer interrupt handler
  - Service keyboard interrupt handler

Failures in Design

- System had no concurrent access to data
- No concurrency control
- Race conditions
  - (A race condition occurs when two or more threads can access shared data and they try to change it at the same time)

Failures in the Field

- Malfunction: 54 cases
  - Three deaths – due to massive overdosage
  - Three serious injuries – also massive overdosage
  - Lawsuits
    - Manufacturer denies machine could malfunction
      - Also denies any other known incidents

Software Bugs

Race condition

Variable, set by the keyboard handler, indicates presence of edits

- But edited mode or energy only detected every 8 seconds, after magnets have been set
- Operator can quickly change data without it being detected by software

Consequence

- Magnets set up for X-ray (no dilution of beam by magnets)
- Turntable set for electron (no flattening)
- Full strength beam delivered to patient

Failure of software interlock

Variable used to indicate whether machine is set up correctly

❖If non-zero then treatment will not proceed

❖BUT, this variable is incremented during a set-up loop

❖Variable will eventually overflow and become zero

❖Incorrect indication that the machine is correctly set

Consequence

❖Software incorrectly indicated that the turntable had been rotated correctly, however turntable still in field light position

- Patient received approximately 100 times required dose

Incident Reporting

- Machine approved based upon existing systems by Food and Drug Administration (FDA)
- FDA unable to stop machine being used
  - (Machine is still mostly saving lives)
- Manufacturer changes microswitches
  - Declares machine 5 times as safe as before
- Medical physicist able to reproduce fault
  - Remove up arrow key fix!
  - FDA unhappy
- After two years FDA declares machine unfit
  - Asks manufacturer to notify customers

Questions

- Who shall take the responsibilities?
  - Programmer
  - Manufacturer
  - Users
  - Hospital
  - Government agencies

Lessons Learnt (1)

Also applies to in general coding

- Engineering Perspectives:
  - Poor design specifications
  - Safety issues and reliability issues are not addressed adequately
  - One programmer design without having adequately quality control mechanism
    - Code review, design review,
    - Software components are not tested sufficiently
      - No test plan for software components
  - Ridiculously reused code from Therac-6 and 20 without conducting compatibility and hazard analysis
    - Reused code is from Therac-6 and 20 developed by CGR documentation in French.

Lessons Learnt (2)

- Other aspects:
  - Undue trust in software
    - Replaced hardware interlocks by software interlocks
    - Failed to analyse software sufficiently
    - Confusion of reliability and safety
  - Poor management of accidents
    - Failure to accept that Therac-25 was cause of accidents
    - Inadequate follow-up on accident reports
    - Poor reporting of earlier accidents to other parties
  - Lack of defensive design
    - No error detection or error handling features

IEEE – code of ethics

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

•to accept responsibility in making decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;

•to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;

•to be honest and realistic in stating claims or estimates based on available data;

•to reject bribery in all its forms;

•to improve the understanding of technology; its appropriate application, and potential consequences;

•to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;

•to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;

•to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;

•to avoid injuring others, their property, reputation, or employment by false or malicious action;

•to assist colleagues and co-workers in their professional development and to support them in following this code of ethics.

Changes to the IEEE Code of Ethics will be made only after the following conditions are met:

•Proposed changes shall have been published in THE INSTITUTE at least three (3) months in advance of final consideration by the Board of Directors, with a request for comment, and

•All IEEE Major Boards shall have the opportunity to discuss proposed changes prior to final action by the Board of Directors, and

•An affirmative vote of two-thirds of the votes of the members of the Board of Directors present at the time of the vote, provided a quorum is present, shall be required for changes to be made.

•http://www.ieee.org/about/corporate/governance/p7-8.html

•http://repository.cmu.edu/cgi/viewcontent.cgi?article=1192&context=sei

Read – more info

More ethical considerations

- http://phys.org/news/2013-08-world-lab-grown-burger-london.html (Reproducing living cells)

- http://www.tandfonline.com/doi/pdf10.1080/08993408.2012.721073