Software Safety

Safety Engineering & Ethics

Prof. Dr.-Ing. Patrick Mäder, M.Sc. Martin Rabe

Contents

Ethics

What is Ethics?

- Ethics is based on **well-founded standards of right and wrong** that prescribe what humans ought to do, usually in terms of **rights, obligations, benefits to society, fairness, or specific virtues**.

Ethics $\neq$ Feelings

Ethics $\neq$ Laws

Ethics $\neq$ Societal Beliefs

[Manuel Velasquez, Claire Andre, Thomas Shanks, S.J., and Michael J. Meyer: **What is Ethics?**, 2010]

Ethical Theories (1/2)

Divine command

- Moral behaviors are those commanded by the divine (god)
- Criticism: not much philosophy can say

Virtue ethics

- Moral behaviors uphold the person's virtues
- Criticism: increasing evidence that character traits are illusory

Deontology (Duty)

- Moral behaviors are those that satisfy the categorical imperative (e.g. don't lie, don't kill)
- Criticism: unacceptable inflexibility

Utilitarianism

- Moral behaviors are those that bring the most good to the most people
- Criticism: How to measure utility?

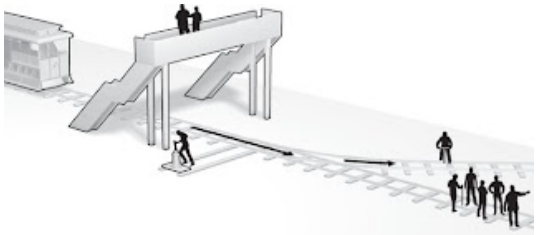
[Kevin Binz: **An Introduction to Ethical Theories**, 2017]

Ethical Theories (2/2)

- Professional philosophers are just about evenly split between theories

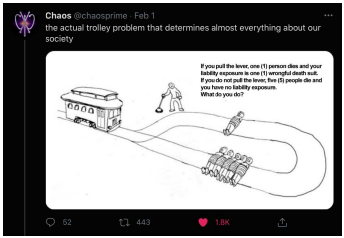
The Trolley Problem

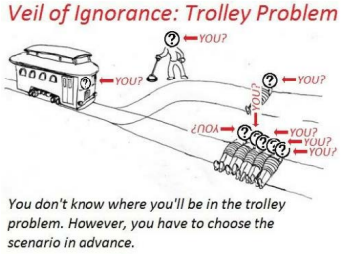
- “A trolley is running out of control down a track. In its path are five people who have been tied to the track by a mad philosopher. Fortunately, you could flip a switch, which will lead the trolley down a different track to safety. Unfortunately, there is a single person tied to that track. Should you flip the switch or do nothing?”



[The Philosophical Muser: **Off Your Trolley: Re-Examining A Famous Ethical Dilemma**. 2013]

Derived Trolley Problems

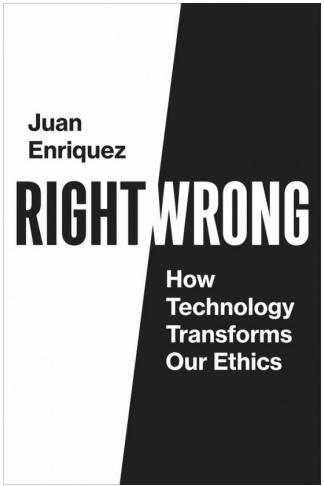




[Twitter: #trollyproblem. 2022]

Ethics of Technology

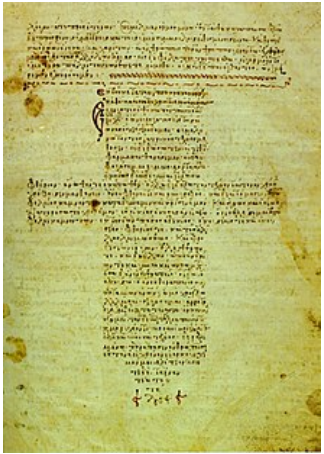
- Ethics change with technological progress
  - e.g., industrial revolution
  - e.g., right to Internet access
  - e.g. birth control, surrogate pregnancy, embryo selection, artificial womb
  - e.g., lab-grown meat



[Juan Enriquez: **Right/Wrong: How Technology Transforms Our Ethics**. MIT Press, 2021]

Professional Code of Ethics (1/2)

- Professional societies typically have a code of ethics
  - [IEEE Code of Ethics]
  - [ACM Code of Ethics]
  - Other examples: medicine: [Hippocratic Oath], armed forces: [Joint Ethics Regulation (JER) DoD 5500.7-R]
- Accreditation agencies (ABET) deem it a critical part of all engineering curricula, including EE and CmpE



[Hippocratic Oath. Wikipedia, 2022]

Professional Code of Ethics (2/2)

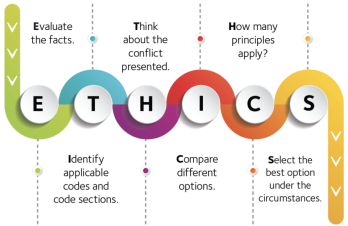
- Highlights from the IEEE Code of Ethics
  - “To accept responsibility in making decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment”
  - “To avoid real or perceived conflicts of interest whenever 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 avoid injuring others, their property, reputation, or employment by false or malicious action”

[IEEE Board of DirectorsIEEE Code of Ethics. IEEE, 2020]

Ethical Conflicts and Consequences

- Ethical conflicts
  - Duty/responsibility vs. malice/indifference
  - Duty vs. self-interest (aka conflict of interest)
    - e.g., bribery, misuse of position, mishandling classified or proprietary material
  - Duty vs. duty
    - maximize profit for employer vs. obligation to society, e.g., confidentiality vs. whistle-blowing

- Potential consequences
  - Injury or loss of human life
  - Damage to a business and reputation
  - Fines, penalties, jail



[Navigating ethical dilemmas as a new dentist. ADA, 2018]

Ethics Case Studies

Ford Pinto: Background

- Ford created the Pinto as a compact competitive car
  - Early 1970s, gas prices were rising in the US
  - Customers became interested in smaller, more efficient cars (competing Japanese cars and VW Beetle)
- Errors were made in fuel tank design due to a rushed design process
  - Ford was aware of the issue from internal studies and had a patent on a safer fuel tank design
  - US regulations only required front-end crash testing at speeds less than 20 MPH at the time

top: [Jonathan Turley: **Has GM pulled a Pinto?**. Los Angeles Times, 2014], bottom: [Bob Unruh: **Vicious train wreck nearly killed 'Harbinger Man'**. WND, 2015]

Ford Pinto: Economic Analysis – Redesign vs. Tolerating Injuries (1/2)

- **Cost of design modification determined to be $11 per car** in 1970 (∼$150 today)
- Ford performed an **economic analysis** using the following assumptions in order to determine whether or not a redesign was necessary:
  - cost of a human life: $200,000 (∼$1.2M today)
  - cost of a severe burn injury: $67,000 (∼$415,000 today)
  - cost to replace destroyed vehicle: $700 ($4,327 today)
  - estimated deaths: 180
  - estimated burn injuries: 180
  - estimated vehicles destroyed: 2,100
  - estimated vehicles sold: 11M
  - estimated light trucks sold: 1.5M

Ford Pinto: Economic Analysis – Redesign vs. Tolerating Injuries (2/2)

- Results of the economic analysis

Category	Cost/incident	# Incidents	Cost
Burn Deaths	$200,000	180	$36M
Burn Injuries	$67,000	180	$12M
Burned Vehicles	$700	2100	$1.5M
Total			**$49.5M**

Category	Cost/unit	# Units	Cost
Cars	$11	11M	$121M
Light trucks	$11	1.5M	$16.5M
Total			**$137.5M**

Ford Pinto: Consequences

- Ford Pinto was **delivered to market**
- Several cases of: burned cars, burn injuries, and deaths resulting from the design problems
- Ford became engaged in a high-profile court case
  - Incriminating evidence: “We’ll never go to a jury again. Not in a fire case. Juries are too sentimental. They see those charred remains and forget the evidence. No sir, we’ll settle.” [quote from a Ford Employee]

→ Ford was **forced to recall** the Pinto at a significant cost

Ford Pinto: Ethical Questions

- Did Ford's actions constitute unethical behavior?
- **What is the monetary value of a human life?**
  - Environmental Protection Agency (EPA) set the value of a human life at $9.1M in 2011
  - Food and Drug Administration (FDA) → $7.9M
  - Department of Transportation (DoT) → $6M
- If you had the option to spent $150 to make a car 1% less likely to fail in a catastrophic manner, e.g., catch on fire, would you do so?

Boeing 737 Max: Aftermath (1/2)

- **FAA delegated much safety certification work to Boeing** for expediency and budget
  - FAA managers pressured safety engineers to delegate more safety analysis to Boeing for faster approval
  - FAA engineers did not even read some of Boeing's documents
  - Managers delegated reviewing Boeing's findings back to Boeing (including the safety of the MCAS)

- Boeing and FAA concluded that a faulty activation of the MCAS under extreme flight conditions would be a **hazardous failure** rather than a **catastrophic failure**
  - → MCAS only used readings from one of the 737 Max 8's angle of attack sensors

Lion Air flight 610

top: [Wikimedia 2018], bottom: [Reuters]

Boeing 737 Max: Aftermath (2/2)

- Boeing designed a **warning light to alert pilots** of significant differing in sensor readings – would have notified a faulty MCAS activation
  - **not installed as a "standard feature"** on the 737 Max 8 – airlines have to pay extra
- Without informing the FAA, Boeing had modified the MCAS movement limit of the rear stabilizer based on flight tests
  - raising the limit from 0.6° to 2.5°
  - FAA only found out about this change after the Lion Air crash

[David Gelles and Natalie Kitroeff: **Boeing Believed a 737 Max Warning Light Was Standard. It Wasn't.**. The New York Times, 2019]

Boeing 737 Max: Ethical Questions

- Did the FAA's delegated safety oversight constitute unethical behavior?
- Did Boeing's apparent failure to test the MCAS system in response to bad angle of attack sensor data constitute unethical behavior?
- Did pressure for market share and profit compromise the thoroughness of safety certification?

Moral Frameworks for Engineering Ethics

Why a Moral Framework?

- Illuminates connections between engineering codes of ethics and everyday morality
- Helps make moral choices, resolve moral dilemmas

[Elizabeth Fernandez: Engineering Ethics Isn't Always Black And White. forbes.com, 2019]

Utilitarianism

- “Produce the most good for the most people, giving equal consideration to everyone affected”
- What is “good”? Consider “acts” or “rules”?
- From codes: “Engineers shall hold paramount the safety, health, and welfare of the public in the performance of their professional duties”? Related?
- “Welfare” is a type of “utility” (so are safety, health)

Utilitarianism vs. Engineering Cost-Benefit Analysis

- Is a cost-benefit analysis the same as utilitarianism? → No.
- Typical cost-benefit analysis identifies good and bad consequences of actions/policies in terms of money
- Why is money the correct utility? How to include costs of lives, injuries?
- Usually, focus on profits to corporation
- Example: cost of safe designs vs. warranty vs. loss of lives/legal issues (e.g., Ford Pinto)

Deontology (Rights Ethics, Duty Ethics)

- **Rights ethics**: Human rights is the moral “bottom-line” (and human dignity and respect are fundamental)
  - liberty rights: rights to exercise one’s liberty that lead to duties of others not to interfere with one’s freedoms
  - welfare rights: rights to benefits needed for decent human life
- **Codes?** “Engineers shall hold paramount the safety, health, and welfare of the public in the performance of their professional duties.” (refers to each individual)
- Public has rights (life/no injuries from bad products, privacy, to get benefits through fair/honest exchange in a free market), what are their duties in these respects?
- **Duty ethics**: right actions are those required by duties to respect the liberty or autonomy of individuals. Codes?

Virtue Ethics

- Virtue ethics **emphasizes character** (virtues, vices) more than rights and rules
- **Virtues**: competence, honesty, courage, fairness, loyalty, and humility (vices opposites)
- **Relevance to codes? IEEE**:
  - "...be honest...in stating claims..."
  - "...improve our technical competence..."
  - "...treat fairly all persons..."

Virtues in Engineering (1/2)

- Public-spirited virtues
  - focus on good of clients (“client-focused”)
  - focus on good of public
  - generosity – going beyond minimum requirements in helping: “engineers who voluntarily give their time, talent, and money to their professional societies and local communities”

Virtues in Engineering (2/2)

- Proficiency virtues
  - mastery/competence
  - diligence (e.g., software engineering case study example)
  - creativity (to keep up with technology)
- Teamwork virtues
  - working together effectively (not a loner)
  - collegiality, cooperation, loyalty, respect for authority

Summary

Summary

- Making decisions according to ethical standards is an important but no trivial desire
- Moral frameworks for engineering ethics provide a guideline

Questions?