24
Society & Ethics

Distributed Embedded Systems

Philip Koopman

November 30, 2015

Carnegie
Mellon

How Much Risk Is OK?

- **Few or no products are entirely risk free**
  - Is it OK to simply inform people of the risks?
    - What if they have no practical alternative?
  - Is it OK to let people self-pay to be safe?
    - Are poor people more expendable?

  - How do we decide how safe is safe enough?
  - How do we know we built it safe enough?
    - Follow the recipe: IEC 61508, ISO 26262, UL 1998, …. Etc.

- **Should the “many” be protected at the cost of the “few”?**
  - Passenger side air bags probably help save males who wear seat belts
    - Can injure people not wearing seat belts
    - Until recent changes, it looks like they increased child and female death rates
  - If something is risky, should it be illegal?
    - Is it OK to modify your car’s software for performance at expense of safety?

What Forces Product Safety?

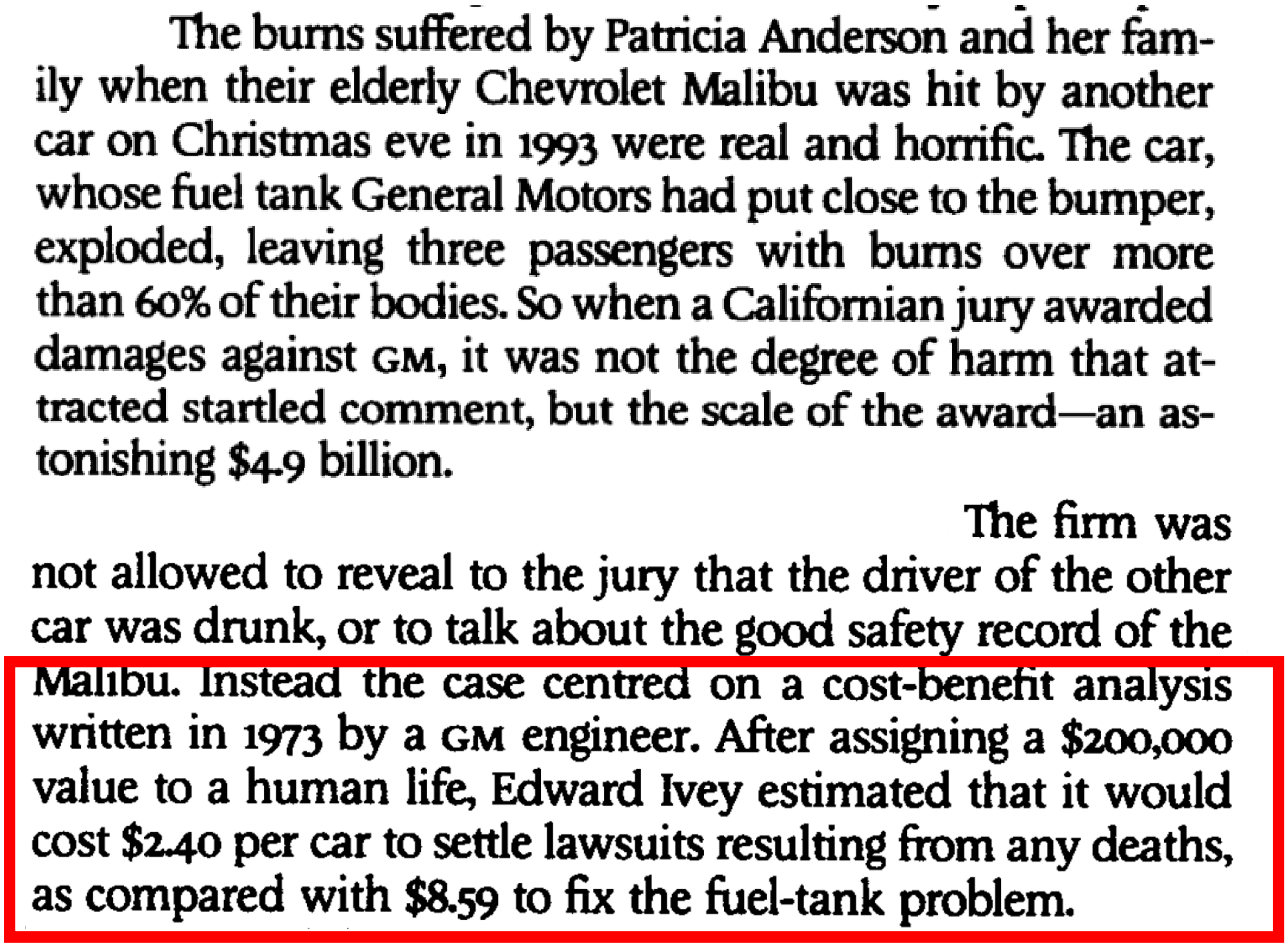
- **Making laws**
  - Legislative action, especially consumer protection laws
  - Litigation results (case law)

- **Industry making improvements for other reasons**
  - Safety to improve public image
  - “Self-regulation” in hopes of avoiding legislative action
  - Improvements made at request (or upon demand) by insurance companies

- **Sometimes good technical products can’t/shouldn’t be sold**
  - If you can’t figure out who is liable if it fails, it might not be viable.
  - If you can’t figure out risks to set insurance rates, can you sell it?
  - If society wants it anyway, maybe legislate that it is OK for it to fail

Putting A $$$ Amount On Human Life Is Risky

- “GM and the Law,” *The Economist*, July 17, 1999

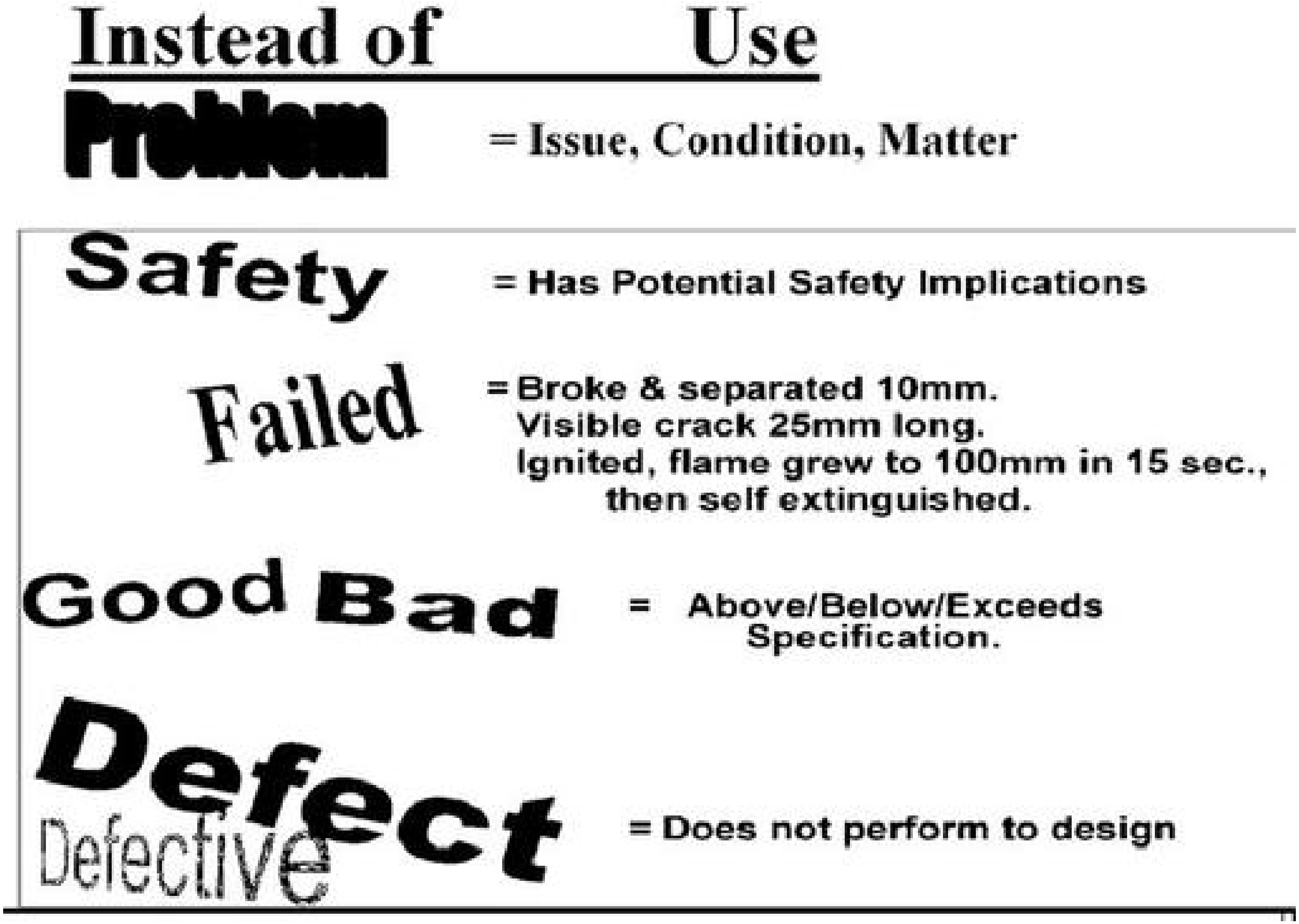


The burns suffered by Patricia Anderson and her family when their elderly Chevrolet Malibu was hit by another car on Christmas eve in 1993 were real and horrific. The car, whose fuel tank General Motors had put close to the bumper, exploded, leaving three passengers with burns over more than 60% of their bodies. So when a Californian jury awarded damages against GM, it was not the degree of harm that attracted startled comment, but the scale of the award—an astonishing $4.9 billion.

The firm was not allowed to reveal to the jury that the driver of the other car was drunk, or to talk about the good safety record of the Malibu. Instead the case centred on a cost-benefit analysis written in 1973 by a GM engineer. After assigning a $200,000 value to a human life, Edward Ivey estimated that it would cost $2.40 per car to settle lawsuits resulting from any deaths, as compared with $8.59 to fix the fuel-tank problem.

- Remember this discussion?

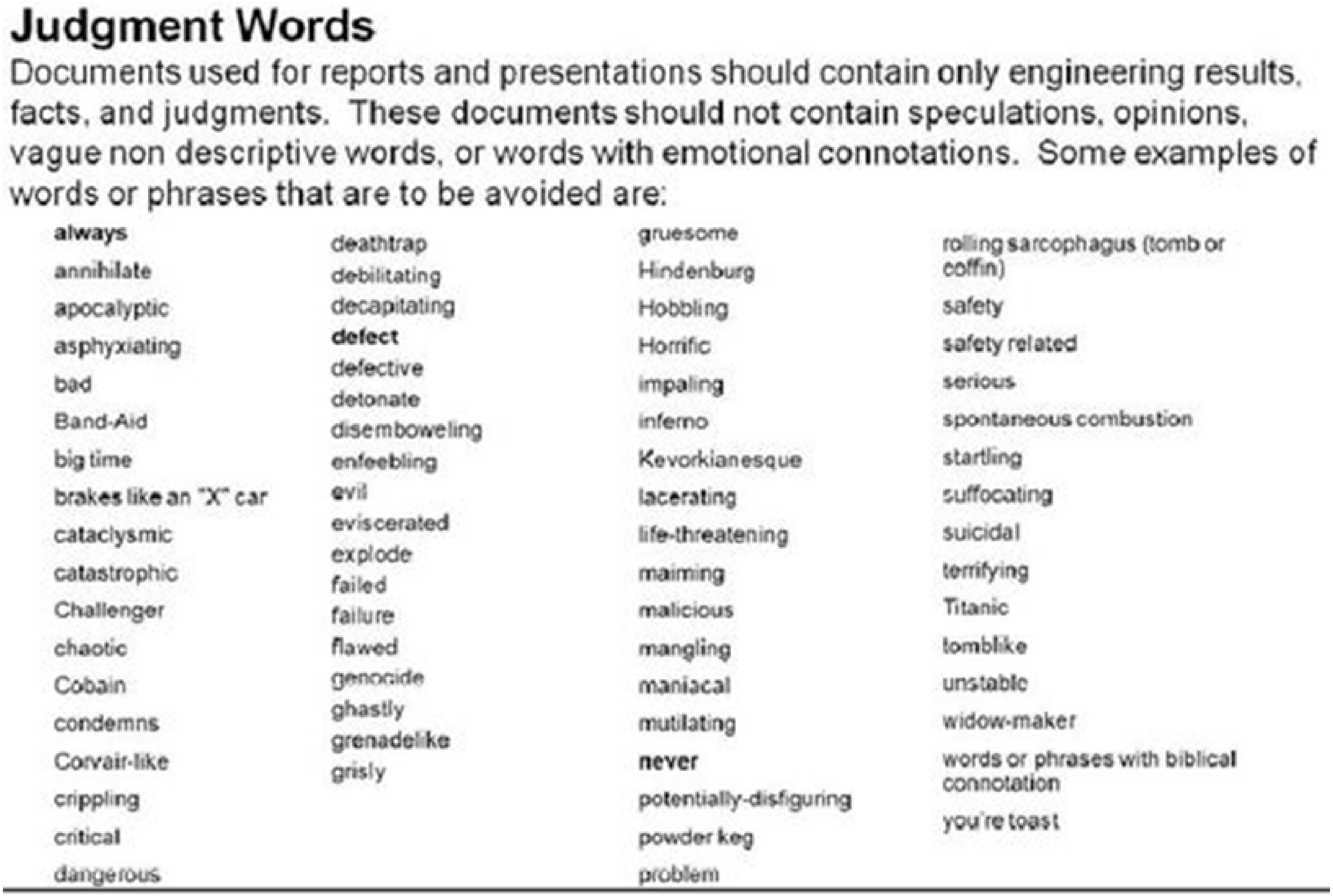
Automotive Guide To Correct Wording



Instead of	Use
Problem	= Issue, Condition, Matter
Safety	= Has Potential Safety Implications
Failed	= Broke & separated 10mm. Visible crack 25mm long. Ignited, flame grew to 100mm in 15 sec., then self extinguished.
Good Bad	= Above/Below/Exceeds Specification.
Defect Defective	= Does not perform to design

http://blogs.wsj.com/corporate-intelligence/2014/05/16/the-69-words-you-cant-use-at-gm/

Automotive Guide To Correct Wording



Judgment Words

Documents used for reports and presentations should contain only engineering results, facts, and judgments. These documents should not contain speculations, opinions, vague non descriptive words, or words with emotional connotations. Some examples of words or phrases that are to be avoided are:

- **always**
- annihilate
- apocalyptic
- asphyxiating
- bad
- Band-Aid
- big time
- brakes like an "X" car
- cataclysmic
- catastrophic
- Challenger
- chaotic
- Cobain
- condemns
- Corvair-like
- crippling
- critical
- dangerous
- deathtrap
- debilitating
- decapitating
- **defect**
- defective
- detonate
- disemboweling
- enfeebling
- evil
- eviscerated
- explode
- failed
- failure
- flawed
- genocide
- ghastly
- grenadelike
- grisly
- gruesome
- Hindenburg
- Hobbling
- Horrific
- impaling
- inferno
- Kevorkianesque
- lacerating
- life-threatening
- maiming
- malicious
- mangling
- maniacal
- mutilating
- **never**
- potentially-disfiguring
- powder keg
- problem
- rolling sarcophagus (tomb or coffin)
- safety
- safety related
- serious
- spontaneous combustion
- startling
- suffocating
- suicidal
- terrifying
- Titanic
- tomblike
- unstable
- widow-maker
- words or phrases with biblical connotation
- you're toast

http://blogs.wsj.com/corporate-intelligence/2014/05/16/the-69-words-you-cant-use-at-gm/

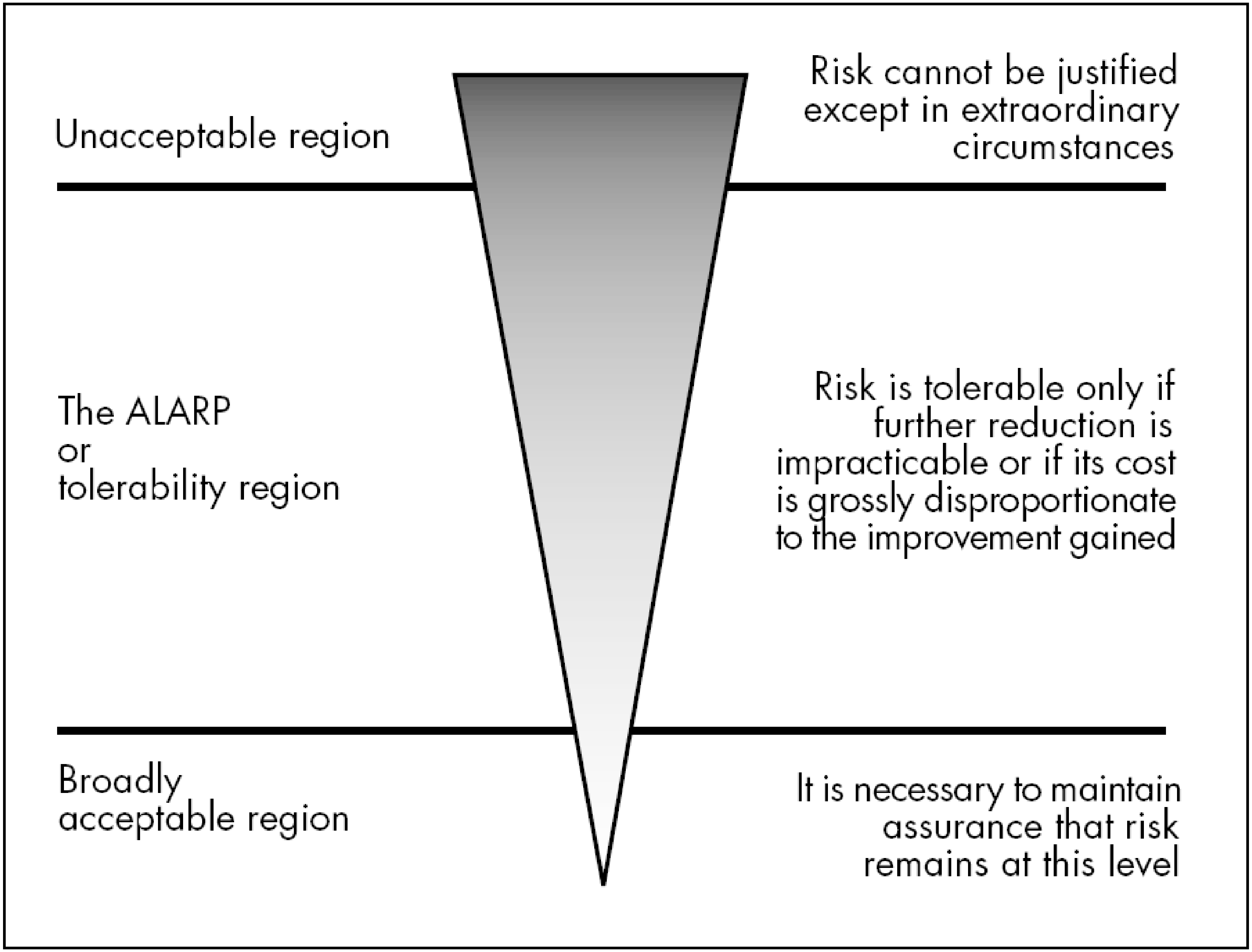

Unacceptable region
Risk cannot be justified except in extraordinary circumstances
The ALARP or tolerability region
Risk is tolerable only if further reduction is impracticable or if its cost is grossly disproportionate to the improvement gained
Broadly acceptable region
It is necessary to maintain assurance that risk remains at this level

Figure 6 The Health and Safety Executive's ALARP model [AN9025-3]

ALARP Principle (IEC 61508)

- **Nothing is completely safe!**

- **ALARP = As Low As Reasonably Practicable –Guideline for IEC 61508**
  - Idea is to associate risk with cost (British safety principle)
  - Set cutoff at "it's not worth it to spend more on this risk"
  - Means you need to know a tolerable risk; often based on existing risks
  - Automotive application:
    "X-by-Wire should be at least as safe, overall, as current vehicles"
    - Current, non-X-by-Wire fatality rate is about 7 * 10^{-7}/hr
    - Total accident rate, including fender benders and drunk driving, is about 7 * 10^{-4}/hr

- **Alternate principle (not discussed in 61508, but possible to use):**
  - German MEM (Minimum Endogenous Mortality)
  - General idea – technology-caused death rate should not be significantly affected
  - CENELEC pre-standard prEN 50126: 2 * 10^{-4} fatalities / year baseline
    - Less than 10^{-5} fatalities/year for a new system over entire population (5% of reference value)
    - For vehicles, this works out to 4 * 10^{-8} fatalities/hr

- **Good discussion at:**
  http://www.ewics.org/uploads/attachments/_risk-analysis-subgroup-working-papers/A_discussion_of_risk_tolerance_principles.html

US Criminal Investigation of Toyota UA

- **"Toyota Is Fined $1.2 Billion for Concealing Safety Defects" – March 19, 2014**
  - Four-year investigation by US Attorney General
  - Related to floor mats & sticky throttle pedals only

- **"TOYOTA misled U.S. consumers by concealing and making deceptive statements about two safety-related issues affecting its vehicles, each of which caused a type of unintended acceleration."** [DoJ Statement of Facts]
  - Deferred prosecution for three years in exchange for fine and continuing independent review of its safety processes.
  - Toyota said in a statement that it had made fundamental changes in its corporate structure and internal safety controls since the government started its investigation four years ago.

http://www.nytimes.com/2014/03/20/business/toyota-reaches-1-2-billion-settlement-in-criminal-inquiry.html

Professional Licensing for Engineers

- Bridge builders are licenses Professional Engineers
  - They use genuine math to ensure structural safety
- Should software developers be licensed?

Ethics

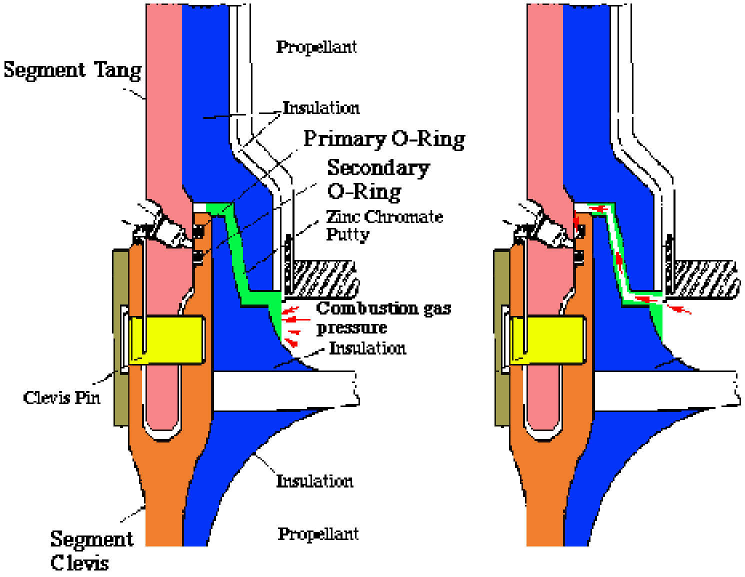
- **Ethics is all about doing the right thing**
  - What is the “right” thing?
  - Ethics is always interesting in the gray areas, usually not simple answers
  - There are always the obvious rights and wrongs

- **Definition: Ethics are a personal code of behavior.**
  - They represent an ideal we strive toward because we presume that to achieve ethical behavior is appropriate, honorable, and desirable --- both on a personal level and within the groups we belong to. [Dakin]

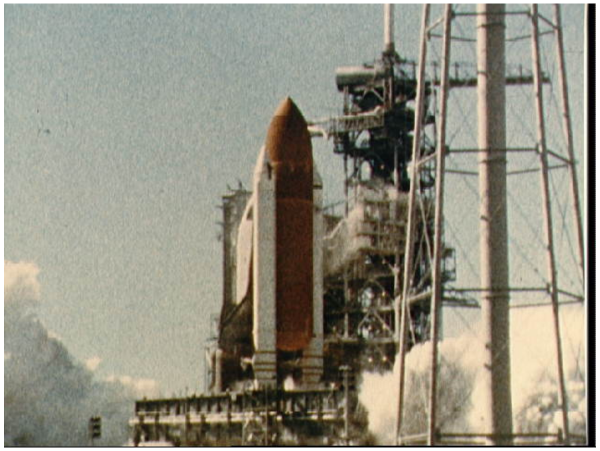
Process Is Not Sufficient For Ethical Behavior

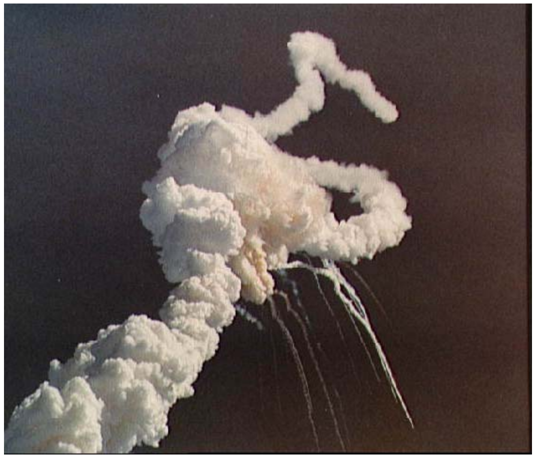
- **How to destroy a Space Shuttle (and lose 7 astronauts); January 1986**
  - Complex process and mechanisms in place to ensure safe shuttle launch
  - O-rings had been known to fail at low temperatures
    - Single O-ring seal failure at 53 degree observed in a previous launch
    - For Challenger launch, temperature was 29 to 36 degrees – double O-ring seal failure resulted

http://onlineethics.org/moral/boisjoly/rocket.html



Presidential Commission Report, p. 57





Some Say Graphs Played A Role

- **Thiokol engineering graph 1/27/86**

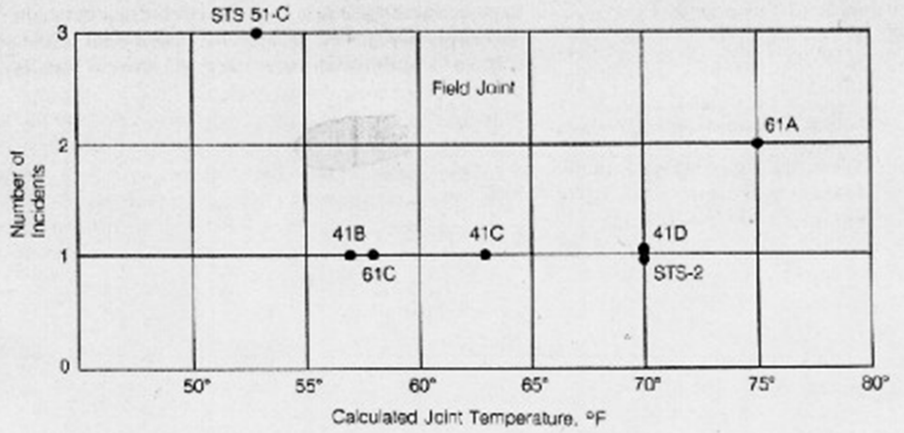


Figure 6
Plot of flights with incidents of O-ring thermal distress as function of temperature

- **Rogers Commission Graph**

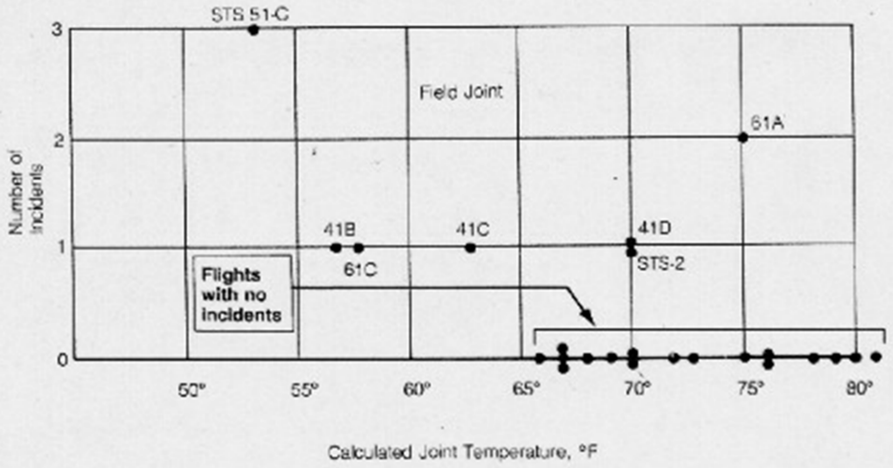
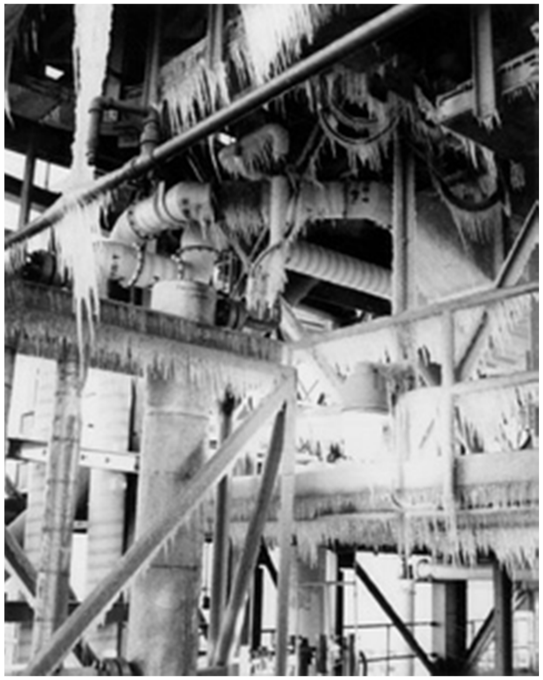


Figure 7
Plot of flights with and without incidents of O-ring thermal distress

http://www.footnote.tv/mwchallenger.html



http://www.firstscience.com/SITE/ARTICLES/challenger.asp

Challenger Cultural Failure

- **Morton-Thiokol initially said "don't launch; it's too cold"**
  - NASA responded "please reconsider"
  - Engineers had to prove to management shuttle is safe to launch
  - Management decided to tell NASA "OK to launch" over engineer protests
- **How did Challenger happen then?**
  - Role reversal – engineers proving to managers that shuttle shouldn't launch!
- **Ethics is about personal responsibility**
  - Just because the customer says you'll lose your job if you don't do something doesn't make it right

Morals vs. Ethics

- **By the dictionary, they are nearly identical, but:**
  - Morals: principles of right and wrong conduct. (religious connotations)
  - Ethics: system/structure of morally correct conduct. (professional/social connotations)

Professional Codes of Ethics

- **IEEE code of ethics short to the point**
  - Mostly broad points; No in-depth discussion
  - Sometimes IEEE has had trouble standing behind its members on these points
    - But they will be happy to hang you out to dry if you violate them
- **ACM code of ethics is longer**
- **Software Engineering code of ethics is fairly reasonable**
  - Has real recommendations
  - Very practical
  - Not contradictory
  - Reads like a specification
- **Most codes have rules/recommendations that are "common sense"**
  - Emphasize responsibility to public good

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:

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

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

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

4 to reject bribery in all its forms;

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

6 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;

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

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

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

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

Approved by the IEEE Board of Directors, August 1990

Seven Ethics Guidance Points

If faced with an ethical dilemma, ask:

1. Is the action Legal?

2. Is it wrong?

3. If the problem is gray: “How would this look in the newspaper? Will it appear insensitive or reckless, or be seen as taking more risk than we should have?”
   - The Washington Post test – how does it look as an unsympathetic headline?

4. Does the action violate the company’s stated values (i.e. written policy?)

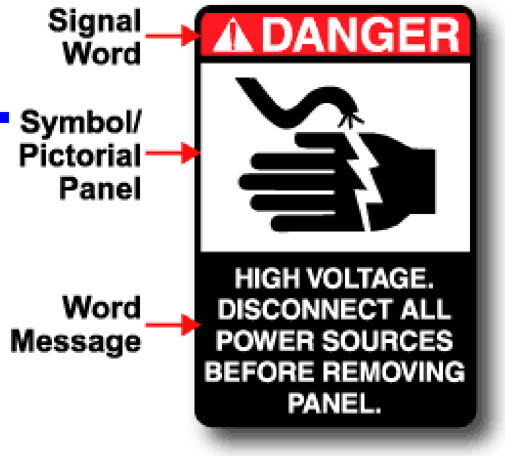
5. Will you feel bad if you take this action?

6. Ask someone you trust for guidance (a friend; the corporate ethics officer)

7. Keep asking until you have an answer

[Costlow, IEEE Spectrum, Dec. 2002, pg. 57]

Legal Questions To Ask


Signal Word
Symbol/ Pictorial Panel
Word Message
DANGER
HIGH VOLTAGE. DISCONNECT ALL POWER SOURCES BEFORE REMOVING PANEL.

- **If it breaks, who gets sued? (Who goes to jail?)**
- **What about things that are beyond your control?**
  - Unintended use
  - Failure in “extreme” conditions (what is reasonable to anticipate?)
  - Moron users
- **How much diligence is “enough”**
  - If there is a standard for similar products, that helps a lot (e.g., UL)
  - If there is a generic standard, that may help (e.g., IEEE)
  - Warning labels even help some, no matter how silly they may seem
- **Important US Judicial system lessons:**
  - Financial liability is not linearly correlated with culpability
  - Nobody wants bad news in writing
  - Money talks (it doesn’t buy results, but without it you are at a disadvantage)

Ethical Issues Specific To Embedded Systems

- **How much is a human life worth?**
  - Is it OK to avoid documenting the number when making a decision?
- **If we don’t know how to get software perfect, when do we ship it?**
  - Is it enough that potential good outweighs potential bad?
  - Is it enough that we’ll get fired (or our startup will fail) if we don’t ship?
  - If bad process statistically predicts producing bad products, is it OK to work for a company with a “broken” software process?
  - Is it OK to produce critical systems without being able to measure their safety directly (i.e., by arguing that best-known practices ensure sufficient safety)?
- **Is it OK to tell the consumer he/she is responsible for things we don’t know how to get right? (security, safety, exceptional situations)**
  - Is it OK to evade consumer protection laws by redesigning an embedded product to be a “computer” instead of “goods”?
- **Is it OK to create products that will inevitably compromise privacy?**
  - Location-aware mobile cell phone trackers/databases
  - Personal authentication systems