ECE 3080

Ethics in Electrical and Computer Engineering

Lectures #6-#8: Case Studies for the Design Process

Prof. K.M. Passino
The Ohio State University
Department of Electrical and Computer Engineering

Connecting design to professionalism...

- It takes significant competence, experience, and a broad perspective to incorporate safety and environmental impact into design...

"On the other hand, my responsibility to society makes me want to stop right here."

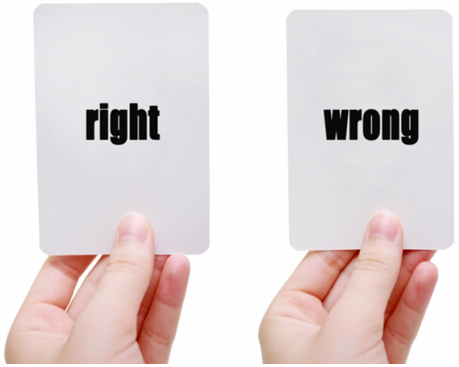
THE OHIO STATE UNIVERSITY

In companies, the trade-offs become clearer?

Consider some specific case studies...

Resolving Moral Dilemmas

1. Moral clarity
   - Need to know something is wrong! *Do not ignore problems!*
   - Loyalty to employer, responsibilities to public and environment (and complex relations between these)
2. Know the facts
   - Get hard, documented facts, discuss with others
   - Competence matters in gathering technical facts



3. Consider options
   - Diversity of actions to take? Evaluate/discuss.
   - Long-term, short-term perspectives, repercussions?
4. Make a reasonable decision
   - Weigh all factors, recognize "gray areas"/compromises
   - An engineering design problem?

The cost of safety…

Student: "I worked at a Power Company. Power distribution was my section. Guy wires (wires that provide mechanical support of utility pole to earth) are often not within clearance of energized conducts. New standards observe this clearance requirement, but many unsafe constructions are in the public. It is just too expensive to redesign and reconstruct utility poles…"

Student: "I worked at the power company and saw instances where potentially dangerous transformers were asked to be kept in service for money reasons." Engineer responsibilities? Diligence?

Student: "I worked for a power supply manufacturer. The units typically used 480 Volts up to 30 KVA. Shielding is obviously a very important safety issue. But we could not seal up the units, so many warning labels had to be used to keep hands out." Innovative solutions?

Uncertainty in assessing safety…

Student: "I was involved in the manufacturing of a polymer. The polymer was made in continuous processes that involved a solvent, dimethyl acidamide (DMAC). The company had set maximum levels for the concentration of DMAC in the work environment, but no one was completely sure about the long term effects of exposure to the solvent. The monitoring done by the company involved routine medical examinations of employees, but no guarantees were offered to employees for their personal safety. In compensation for their increased risk they were paid at levels above average."

What to do? Research safety? Balance professionalism with being a pest?

Diligence with implementation of safety procedures…

Student: "I was working for a company that manufactures TV tubes using PLC control. The engineer responsible for programming and safety was not very concerned about implementing enough safety measures. One day a worker stopped the machine to check the pipe that poured the glass, and he was right underneath it. At the same time, another one who did not know about this turned the machine on. The worker got burned and had to be hospitalized for three months. I didn't say anything about it!" Engineer responsibilities? Demand compliance? Know facts? Apply pressure?

Student: "While working at my internship I heard of units coming into the shop that contained asbestos-based insulation. The sales engineer had difficulty relaying that information to the people in the shop who were to "strip" the units. Because of this lack of communication the people who stripped the units did not wear the proper safety equipment and were exposed to the asbestos. This may not have occurred if more emphasis was put on internal communications and safety." Be alert to organizational issues and impact on safety.

Competence/diligence…

Student: "When I co-oped at Company Y my supervisor asked me to do significant corrections on a programmable logic controller (PLC) program that controls the robots on a conveyor. At that time I did not have a lot of experience with PLCs. I made some changes, but was not sure whether I did things correctly. So I asked the supervisor to check it for me, but he did not have time. So he said "it is fine, I trust you". Later on they found that I had disabled the main safety subroutine. Nothing happened but it was possible that people would have been injured from the mistake and some very expensive equipment (worth millions) could have been damaged."

How fast can you teach yourself? Does all this make you uneasy?

Press the boss? Hurt the engineer's career? What is more important, advancement or safety?

THE OHIO STATE UNIVERSITY

Automotive Components, Safety Testing (Harris, Pritchard, and Rabins)

Charlie Long is an electrical engineer working for a major automobile company in the year 2001. He works in the automatic sensors department, and his job is to design and test electronic sensors for use in different parts of cars.

The latest version of the Lightning-Z100 was recently launched into the national market, equipped with an electronic sensor crucial to an innovative safety feature of the vehicle. This sensor was designed and…

tested by Charlie's department. The Lightning-Z100's major competitor equipped its comparable model (the Bolt-Z100) with a somewhat similar sensor two years before, and it apparently was effective in reducing the number of fatalities in head-on collisions.

Convinced that they could quickly come up with a design for an electronic sensor to match the Bolt-Z100's, Charlie's department committed to preparing one in time for the 2001 Lightning-Z100 model. Unfortunately, the design challenge proved to be more formidable than they expected, and they fell behind schedule. At the same time, they were under pressure to have something ready for the 2001 model. This, they were told by management and marketing strategists, could be the key to competing successfully with the Bolt-Z100.

So, time was short, and Charlie's department could delay its recommendation no longer. Although the prototype was not subjected to as rigorous testing as usual,

Charlie's department recommended a go-ahead. Charlie was uncomfortable with this decision. He objected that more testing was needed on sensors that served an important safety function. But he was overruled, and he pressed the issue no further.

Several months after the Lightning-Z100 was on the road, a disturbing set of data emerged. A very high percentage of head-on collisions resulted in the death of passengers in the Lightning-Z100, much higher than similar collisions involving the Bolt-Z100.

As Charlie thought about this, he realized that the problem could lie in the new electronic sensor. The National Highway Traffic Safety Administration (NHTSA) decided to do a detailed study of the Lightning-Z100. Although it could not determine the precise nature of the problem, NHTSA found that, for some reason, the new electronic sensor was not functioning according to the design. All the new Lightning-Z100's would have to be recalled

as soon as possible in order to avoid any more deaths from malfunctioning sensors.

Charlie reexamined the design. Suddenly he realized that there was a very specific design flaw. He was not sure why this realization had come to him--it would not be obvious, even to experienced electrical engineers. But there it was, staring him in the face. Further testing might have revealed this earlier, but there had not been time for that.

Meanwhile, many expensive lawsuits were being pressed against Charlie's company. Called in to testify in court, Charlie had a tough problem. Should he reveal everything (his belief that the testing was inadequate and his recent discovery) and cost the company a great deal of money? Or should he testify that he had been convinced that the testing was adequate? Should he keep it to himself that he now knew that there was something wrong with the design?

THE OHIO STATE UNIVERSITY

Case: Honesty in Specifications/Bidding (Martin and Schinzinger)

- Arthur is chief engineer in a components house. As such, he sits in meetings concerning bidding on contracts. At one such meeting between top company executives, who are interested in getting a major contract, and the National Aeronautics and Space Administration, NASA presents specifications for components that are to be several orders of magnitude more reliable than the current state of the art. The components are not part of a life-support system, yet are critical for the success of several planned experiments. Arthur does not believe such reliability can be achieved by his company or any other, and he knows the executives feel the same.

THE OHIO STATE UNIVERSITY

Nevertheless, the executives indicate an interest to bid on the contract without questioning the specifications. Arthur discusses the issue privately with the executives and recommends that they review the seemingly technical impossibility with NASA and try to amend the contract. The executives say that they intend, if they win the contract, to argue mid-stream for a change. They remind Arthur that if they don't win the contract, several engineers in Arthur's division will have to be laid off. Arthur is well-liked by his employees and fear the lay-offs would affect some close friendships. What should Arthur do?

THE OHIO STATE UNIVERSITY

Attendance Question

Please: Put your name on the sheet of paper and turn it in...

THE OHIO STATE UNIVERSITY

Challenger Disaster

- Challenger was a delta-wing craft with a huge payload bay
- Three main engines fueled by several million pounds of liquid hydrogen
- Fuel carried by an immense external divided fuel tank
- During liftoff main engines fire for 8.5 min., thrust for first two minutes provided by two booster rockets

THE OHIO STATE UNIVERSITY

- Booster rockets fueled by solid fuel
- Casing of each booster rocket about 150 ft long and 12 ft in diameter
- NASA+companies: Rockwell Int. (orbiter and main rocket), Morton-Thiokol (booster rockets)
- After embarrassing delays, flight set for Tues. morning Jan 28, 1986

THE OHIO STATE UNIVERSITY

- A.J. McDonald of Morton-Thiokol worried about predicted freezing temperatures since he knew of problems with field joints on a previous cold-weather launch
- He arranged a telecon
- A. Thompson and R. Boisjoly, seal experts at Morton-Thiokol, explained how booster rocket walls bulge and combustion gases can blow past one or both of the O-rings that make up the field joints

THE OHIO STATE UNIVERSITY

- O-rings char and erode as seen on many previous flights
- In cold weather problem is aggravated because rings and putty packing a less pliable
- Past flights showed that below 65 deg launches always resulted in failure incidents with O-rings

- Engineering managers B. Lund and J. Kilminster agreed there was a problem with safety
- During a recess in telecon, Senior VP Jerry Mason turned to B. Lund and told him “to take off your engineering hat and put on your management hat.”
- Tone: You have to prove to us that there will be a problem if we launch

THE OHIO STATE UNIVERSITY

- Countdown ended at 11:38am
- Temperature was 36 deg.
- Smoke came from field joint on take-off
- Soon turned into a flame
- Hydrogen in tank caught fire, tank broke loose and smashed into Challenger's wing
- By 76 sec. into flight at 50,000 ft totally engulfed in fire ball

THE OHIO STATE UNIVERSITY

- Died: F. Scobee, M. Smith, G. Jarvis, R. McNair, E. Onizuka, J. Resnick, and Christa MacAuliffe ("teacher in a space")
- What could have been done differently?
  - Clearer presentation of the problem (temp influence on O-ring failure)? Could have made for more forcible arguments?
  - Watch for growing problems!
  - Don't take off your engineer's hat!

THE OHIO STATE UNIVERSITY

- Aerospace engineer: “The arrogance that prompts higher-level decision makers to pretend that factors other than engineering judgement should influence flight safety decisions and, more important, the arrogance that rationalizes overruling the engineering judgement of engineers close to the problem by those whose expertise is naïve and superficial by comparison”

THE OHIO STATE UNIVERSITY

The Flaw in the Intel Pentium Chip (case study by C. Fleddermann)

- In late 1994 media started reporting flaw in Intel's pentium microprocessor
- It was the chip used in 80% of all personal computers in the world
- Flaws in the integrated circuits of microprocessors are not uncommon (most of these cannot be detected by the user and do not affect operation)
- The 1994 flaw was different. It caused incorrect answers when performing double-precision arithmetic (common operation, easily detectable)

THE OHIO STATE UNIVERSITY

- Intel response:
  - Acknowledged error but said that defect was insignificant and the vast majority of users would never even notice it
  - Chip would be replaced for free only for users who could demonstrate that they needed an unflawed version
- Users found this unsatisfactory
- IBM, a major pentium user, cancelled the sales of all computers using the chip

THE OHIO STATE UNIVERSITY

- After much negative press, and an outcry from Pentium users, Intel agreed to replace the faulty microprocessor with an unflawed version for any customer who asked to have it replaced
- Note: Long before news of the flaw surfaced, Intel was aware of the problem and corrected it on subsequent versions
- But, they continued to sell the flawed chip
- New Intel policy: Flawed chips should be replaced on request, regardless of how insignificant the flaw is

THE OHIO STATE UNIVERSITY

- Public relations problem, with ethical issues
- Questions (Fleddermann):
  - Should flaws always be revealed to customers?
  - Is it an ethics problem only if safety is involved?
  - What if they added a label “This product may contain unexpected flaws and might not operate correctly under all conditions”. Does this solve the ethical problems for the company?

THE OHIO STATE UNIVERSITY

- How can an engineer be sure that there are no defects in a product? Testing! Before/after product release
- If it is impossible to eliminate all defects in a product, what level of defects is acceptable?
- Does this depend on the type of product?

NSPE BER Case No. 09-2

- Engineer A, an electrical engineer, worked for Dicers a company that purchased wafers for microprocessor chips from another company and then reprocessed, packaged, and resold them. Engineer A was assigned the task of testing the wafers. After a while, Engineer A was instructed by his supervisor to alter the testing process, to which both parties had contractually agreed. The testing process was altered, over Engineer A's objections in such a manner that the quality of the purchased wafers was made to seem lower, when in reality there is not reduction in the quality. This lowered the price paid by Dicers to the other company. Engineer A objected to this practice and refused to go along, and as a consequence was discharged.

NSPE BER Case No. 08-2

- Engineer A is an electrical engineer working in quality control at a computer chip plant. Engineer A's staff generally identifies defects in manufactured chips at a rate of 1 in 150. The general industry practice is for defective chips to be repaired or destroyed. Engineer B, Engineer A's supervisor, recently announced that defective chips are to be destroyed, because it is more expensive to repair a defective chip than it is to make a new chip. Engineer A proceeds on the basis of Engineer B's instructions. A few months later, Engineer B informs Engineer A that Engineer A's quality control staff is rejecting too many chips, which is having an effect on overall plant output…

THE OHIO STATE UNIVERSITY

- and ultimately company profitability. Engineer B advises Engineer A's staff to allow a higher percentage of chips to pass through quality control. Engineer B notes that in the end, these issues can be best handled under the company's warranty policy under which the company agrees to replace defective chips based upon customer complaints. Engineer A has concerns as to whether this approach is in the best interest of the company or its clients.

- Question: What are Engineer A's ethical obligations under the circumstances?

THE OHIO STATE UNIVERSITY

Attendance Question

Please: Put your name on the sheet of paper and turn it in...

NSPE BER Case No. 01-10

- Engineer A is a graduating senior with excellent credentials from State University. Engineer A has had a series of job interviews with engineering companies from around the US. Following interviews with several industrial companies, Engineer A decides to accept an offer with ABC Incorporated located in his hometown of Townville, and plans to notify ABC the following week. In the interim period, Engineer A receives a call from Engineer B, an executive with XYZ Incorporated, a potential employer with whom Engineer A had interviewed. On behalf of XYZ, Engineer B offers Engineer A a position with XYZ and invites Engineer A,…

- at XYZ's expense, to visit XYZ's headquarters in Mountainville, a city located near a resort area, following Engineer A's graduation. Engineer A had earlier decided that he would not accept a position at XYZ if offered a position by ABC because Engineer A wanted to be close to family and friends in Townville, and also because ABC provided better long-term professional opportunities. However, after receiving the call from XYZ, Engineer A decides to accept the invitation to visit XYZ's headquarters and combine the trip with a post-graduation vacation, believing that the visit to XYZ will broaden Engineer A's knowledge of the employment market as well as future…

- professional opportunities with XYZ. A week after the trip, Engineer A calls ABC to inform the company that he will accept the position with ABC.

- Question: Was it ethical for Engineer A to accept the invitation to visit XYZ headquarters?

Confidentiality/Conflict of Interest: Whose Property? (Harris, Pritchard, and Rabins)

Derek Evans used to work for a small computer firm that specializes in developing software for management tasks. Derek was a primary contributor in designing an innovative software system for customer services. This software system is essentially the "lifeblood" of the firm. The small computer firm never asked Derek to sign an agreement that software designed during his employment there becomes the property of the company. However, his new employer did.

Derek is now working for a much larger computer firm. His job is in the customer service area, and he spends most of his time on the telephone talking with customers having systems problems. This requires him to cross-reference large amounts of information. It now occurs to him that by making a few minor alterations in the

innovative software system he helped design at the small computer firm, cross-referencing can be greatly simplified.

On Friday Derek decides he will come in early next Monday morning to make the adaptation. However, on Saturday evening he attends a party with two of his old friends, you and Horace Jones. Not having seen each other for some time, you talk about what you have been doing recently. Derek mentions his plan to adapt the software system on Monday. Horace asks, "Isn't that unethical? That system is really the property of your previous employer." "But," Derek replies, "I'm just trying to make my work more efficient. I'm not selling the system to anyone, or anything like that. It's just for my use--and, after all, I did help design it. Besides, it's not exactly the same system--I've made a few changes."

This leads to a discussion among the three of you. What is your contribution?

Derek installs the software on Monday morning. Soon everyone is impressed with his efficiency; they ask about the "secret" of his success. Derek begins to realize that the software system might well have company-wide adaptability. This does not go unnoticed by his superiors either, so he is offered an opportunity to introduce the system in other parts of the company.

Now Derek recalls the conversation at the party, and he begins to wonder if Horace was right after all. He suggests that his previous employer be contacted and that the more extended use of the software system be negotiated with the small firm. His superiors firmly resist this suggestion. They insist that the software system is now the property of the larger firm. Derek balks at the idea of going ahead without talking with the smaller firm. If Derek does not want the new job, his superiors reply, someone else can be invited to do it; in any case, the adaptation will be made.

THE OHIO STATE UNIVERSITY

What should Derek do now?

Does Horace have any responsibility to alert the smaller firm about Derek's plans?

Do you?

What if Horace is friends with people who work at the smaller firm?

What if you are?

THE OHIO STATE UNIVERSITY

Reverse Engineering (J. Wallberg, MIT)

- While working at a large information technology company over the past two summers, I have been involved with the hard disk drive group of the semiconductor division. One of the products that this group designs is the read channel chip. This chip communicates between the computer and the disk. This is a very competitive area in the semiconductor business, because the demand for computer performance has increased (and continues to increase) exponentially over the past decade. One common practice that I have heard discussed more than once is to use reverse engineering to see what the competitors are doing. …

THE OHIO STATE UNIVERSITY

- This involves taking a microscopic picture of the chip as it is laid out in silicon, and try to work backwards to the transistor and system levels. The accuracy and amount of information that can be deduced varies, but it is certainly possible to obtain system level designs

- Question: Is such reverse engineering of competitor's products ethical?

NSPE BER Case No. 10-2

- Engineer A works as an employee for QRS Engineering on a full time basis. Engineer A also has his own separate engineering practice in which he performs services that are also performed by QRS Engineering. Engineer A's work, including all client contacts is done completely on his own time (evenings and weekends) using his own equipment and materials. Engineer A does not attempt to lure existing QRS Engineering clients to his engineering practice. The QRS Engineering Employee Handbook has no specific policy that addresses performing outside work and Engineer A does not advise the firm of his outside practice.

NSPE BER Case 09-1

- Engineer A, a young professional engineer with expertise in software engineering works for a hospital information technology department. He is assigned to work with the people in the intensive care unit (ICU). A computer user group, headed by the lead physician in the ICU, is forced to facilitate interface between a piece of commercial data processing software and various units in the ICU, including real-time patient monitoring devices. From the manager on down, the computer user group is not technically up to the mark in experience or in education. The computer user group was falling significantly behind schedule. Engineer A learns that the group is seriously…

THE OHIO STATE UNIVERSITY

- considering cutting back on testing in order to close the schedule gap. Appalled at this idea, Engineer A argues strongly against it with the computer user group. In this case, Engineer A's arguments has some effect, but Engineer A is nevertheless given the clear impression that his long-term employment prospects with this organization are now significantly impaired. Apparently, part of the problem had to do with a reluctance on the part of hospital administration to clash with the physician who heads the computer user group. Engineer A feels that the basic problem is incompetence of the computer user group and he does not see how he could be effective on his own in combating it.

NSPE BER Case No. 09-4

- Engineer A worked for the US Government in a defense agency for many years as an engineer, rising to a fairly high managerial position in the government. Upon retirement, Engineer A accepts an executive position with SuperCom, a company producing electronic equipment for the military. Shortly after coming on board with SuperCom, Engineer A is informed by a manager in another SuperCom division that, under an existing contract with the Department of Defense, a key test on an important product was not being performed in the manner specified by the contract. According to the employee, this practice had been going on for several years and the subordinate…

- felt very uncomfortable about it. Engineer A, who had considerable expertise with the testing technology involved, looked into the matter carefully. Engineer A found that the shorter and significantly less costly test had indeed been substituted by the company for one under the contract. But after some review and study, Engineer A concludes that SuperCom's test was actually as effective as the specified test. Nevertheless, Engineer A takes his findings to SuperCom's upper executive management team and recommends that the company apply to the contracting agency for a contract change authorizing the simpler test. Following a meeting, SuperCom executives decide to …

- continue with its current course of action. Since there were no safety or quality issues involved, and wanting to start out on the right foot with SuperCom, Engineer A decided not to pursue the matter further.

- Question: Was it ethical for Engineer A not to pursue the matter further?

NSPE BER Case No. 08-3

- Engineer A, a software engineer, serves as a consultant to CreditData a credit records clearinghouse and is asked to evaluate a software problem with their five million individual credit files. The original software was designed by another software company, which is no longer under contract with CreditData. The problem, an apparent software design flaw, relates to the fact that the database software sometimes misidentifies individuals located in the credit files. Recently, several situations were uncovered involving home purchasers with a high credit score who were in the process of seeking a home loan. However, a credit check through CreditData indicated that the applicant was a poor credit risk and the loan was denied….

THE OHIO STATE UNIVERSITY

- The problem is later corrected and the proper applicant credit information is forwarded to the lender, but in many cases, the purchasers lost the opportunity to purchase a home. In other cases, applicants with low credit scores were misidentified as individuals with high credit scores and as a result, loans and in some cases low interest loans were offered which later resulted in loan defaults. Up to this point no information has been released to the public or to governmental regulators. Engineer A is asked to make a recommendation concerning the CreditData software problem.
- Question: What are Engineer A's ethical responsibilities, if any, concerning this matter?

NSPE BER Case No. 08-11

- Engineer A is a software systems engineer hired by NewSoft, a start-up company, to help in the development of a new software product. Engineer A soon learns that the plans for the proposed new product will be based upon proprietary software for which NewSoft does not have a license. Engineer A assumes that this is some sort of mistake and speaks to the company president about the matter. Engineer A is assured by the company president that the situation will be rectified. But several months pass and no licenses have been secured for the proprietary software. Repeated efforts by Engineer A to get the NewSoft leadership to address this issue have failed. Engineer A is uncertain as to what steps she should take next.

NSPE BER Case No. 00-1

- Engineer A, a CEO of a small engineering corporation, teams up with another small engineering firm in the development and delivery of highway/rail intersection database management systems for various public and private enterprises. Engineer A is the coauthor and the program is patented/copyrighted. Engineer B in a private firm from State X calls Engineer A and informs Engineer A that State X's Department of Transportation (XDOT) is interested in the highway/rail system and has asked Engineer B to evaluate the system. Engineer B requests, and Engineer A agrees to visit with Engineer B in State X. Prior to the visit, Engineer B requests that Engineer A…

THE OHIO STATE UNIVERSITY

- prepare a project proposal which Engineer A submits. Later, at Engineer B's request, Engineer A visits Engineer B's offices and demonstrates the systems. Project managers, as well as programmers from Engineer B's firm are present at the meeting. Engineer A describes in great detail the technical aspects of the system. Following the meeting, Engineer B requests that Engineer A prepare a new proposal with a detailed breakdown of all costs. Following the passage of time, Engineer A receives a phone call from a subordinate of Engineer B advising that Engineer B will not need Engineer A's firm's services because Engineer B's firm now has the capability to design their own system.

NSPE BER Case No. 95-10

- ENGCO, an engineering firm, distributes a brochure that, along with the usual information, contains a listing of key personnel. Some are licensed professional engineers; others are not. In some instances, key personnel who do not hold an engineering degree and who may in fact be high school graduates only, are given such titles in the brochure as "Engineer", "Design Engineer", etc. This practice has arisen from federal agency engineering contracts that refer to inspection personnel as "Engineers". ENGCO is concerned that the company brochure may be conveying a misrepresentation, implying that there are more engineers on its staff than is the true situation.
- Question: Is it ethical for ENGCO to refer to its non-degreed personnel as engineers?

NSPE BER Case No. 02-11

- Engineer A observes what he believes is a serious violation of the state board's rules of professional conduct by Engineer B. Engineer A is not a competitor of Engineer B and does not know Engineer B personally. Thereafter, Engineer A submits an anonymous complaint to the state engineering licensure board identifying Engineer B and the circumstances surrounding the alleged violations of the state board's rules of professional conduct.

- Question: Was it ethical for Engineer A to submit an anonymous letter to the state engineering licensure board?

NSPE BER Case No. 10-6

- Engineer A, a licensed professional engineer in private practice, designs low-voltage electrical systems for commercial buildings and other facilities. Recently, Engineer A started his own consulting engineering firm. Engineer A would like to include on his firm's web site several projects that Engineer A designed over the years, including some work that Engineer A designed while employed with other consulting firms. All web content would be original and the content would be non-confidential. The content would include a picture of the project building and a short generic narrative of the work performed. Work performed by Engineer A while…

- under employment with the other firms would be described accordingly. Engineer A would claim credit for the design work only and would not state or imply that clients of other consulting firms are a client of Engineer A. None of the subject projects are covered by any employment agreements with any of Engineer A's previous employers.

- Question: Is it ethical for Engineer A to reference previous projects he has worked on for other employers on his web site in the manner indicated?

NSPE BER Case No. 10-1

- Engineer A reads a public on-line newspaper blog relating to a local construction project. Engineer A strenuously disagrees with the view of the author of the blog and so writes a lengthy response to the on-line blog which also includes coarse, abusive, and obscene language. Engineer A includes his name along with his PE designation.

- Question: Was it ethical for Engineer A to include his PE designation in the blog posting?

THE OHIO STATE UNIVERSITY

Therac-25 Accidents (N. Leveson, C. Turner, P. Sarin)

- The Therac-25, a computerized radiation therapy machine, massively overdosed patients at least six times between June 1985 and January 1987. Each overdose was several times the normal therapeutic dose and resulted in the patient's severe injury or even death. Overdoses, although they sometimes involved operator error, occurred primarily because of errors in the Therac-25's software and because the manufacturer did not follow proper software engineering practices.

THE OHIO STATE UNIVERSITY

- Overconfidence in the ability of software to ensure the safety of the Therac-25 was an important factor which led to the accidents. The Therac-20, a predecessor of the Therac-25, employed independent protective circuits and mechanical interlocks to protect against overdose. The Therac-25 relied more heavily on software. Moreoever, when the manufacturer started receiving accident reports, it, unable to reproduce the accidents, assumed hardware faults, implemented minor fixes, and then declared that the machine's safety had improved by several orders of magnitude.

THE OHIO STATE UNIVERSITY

- The design of the software was itself unsafe. The Therac-25 supported a multitasking environment, and the software allowed concurrent access to shared data. This precarious implementation caused program failure under certain conditions. Risk assessments were, from the start, unrealistic. A risk assessment performed by the manufacturer seems to consider only hardware failures as it lists the possibilities of the computer selecting the wrong energy or mode as 1e-11 and 4e-9 respectively. Justification never appears for these numbers, but, more surprisingly, the company accepted this low risk assessment easily.

THE OHIO STATE UNIVERSITY

- Follow-through on accident reports was unacceptable. After one accident, the manufacturer tried to reproduce the condition which occurred at the treatment. When it could not, it concluded that a hardware error caused the accident, and implemented a solution based on that assumption. It declared that the system was several orders of magnitude safer, but accidents did not cease.

THE OHIO STATE UNIVERSITY

- The Therac-25 incidents demonstrate that several misconceptions in the manufacturer's attitude led to the accidents. Poor software design, overconfidence in the software's abilities, unreasonably low risk assessments, and poor manufacturer response to complaints all contributed to the overdoses.
- Companies must understand that for safety-critical software design rigorous testing and failure analyses are essential and that trained software engineers, not simply any reasonably experienced engineers, should implement the software design.

Attendance Question

- **For those who have had a job in engineering industry, rate on a scale of 1 to 10 (10 the highest) the *overall* level of professionalism at your workplace (combine persons with environment).**

Please: Put your name on the sheet of paper and turn it in...