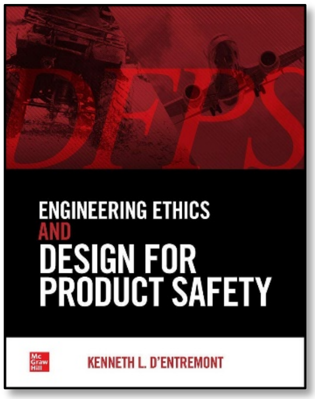
Study Guide: Key Concepts and Discussion Topics and Questions

for the book

Engineering Ethics and Design for Product Safety
by Kenneth L. d'Entremont
McGraw-Hill, New York, NY, 2021

www.DesignForProductSafety.com

(Revised: 06/24/21)



Chapter 0: Notice

N/A

Chapter 1: Introduction

N/A

Chapter 2: Product Safety

Key Concepts

- Safety
- Product safety
- Safety versus health
- Safety may *not* mean reliable, dependable, available, secure, compliant, high-quality, or legal
- Corporate Social Responsibility (CSR)
- Supply-chain integrity
- "Safe enough"
- Engineers must make ethical, values-driven conclusions on acceptable levels of product safety
- New technologies often bring new benefits and new risks to consumers
- Many new or innovative products *must* be designed without guidance from standards and regulations
- Product-safety management is not the same as PSEg
- Products for "at risk" populations must be designed with extra care
- PSEg and product safety are ultimately dependent upon value systems when determining sufficient safety levels of products

- Compliance with standards and regulations is a *necessary* condition not a *sufficient* condition for the safety of products
- Engineers should work to *design-in* positive safety characteristics to their product from the very beginning of the PDP
- There are few—if any—safety *facts*
- A country's or region's customs and laws often reflect the collective values of that population
- Mathematical and scientific principles are insufficient to fully assess acceptable risk from a product
- Exactly what is considered by society to be "safe" changes over time
- Product *liability* is not the same as product *safety*
    - The study of product liability does not reward reason and logic
    - The same (product-liability) *inputs* often produce different *outputs* in a litigation, or trial, setting

Discussion Topics and Questions

- How are health and safety similar to one another?
- How are health and safety different from one another?
- Does compliance with laws, regulations, and practices *always* lead to better safety?
    - Can you provide any counterexamples?
- What does the term "product safety" mean:
    - To you?
    - To engineers?
    - To government regulators?
    - To consumer advocates?
    - To the public?
- Do you consider multi-use straws to be superior to single-use straws?
    - Why?
    - Can you reach this conclusion without making presumptions or assumptions?
        - If not, what are these presumptions or assumptions?
            - Are they values based and not completely supportable by science or technology?
- Find some examples of an organization—commercial, non-profit, or governmental—and their Corporate Social Responsibility (CSR) efforts
    - Are their CSR efforts in line with their proclaimed values?
        - Why or why not?
- List ways in which a compromised supply chain could affect product safety for consumers.
- When is a product "safe enough?"
    - Who should be the final authority?
    - How should disputes about "safe enough" be handled?
- Identify examples where a safe product may *not* be:

  - Healthy
  - Reliable
  - Compliant
  - (High in) Quality
  - Legal
- What new risks are posed by consumer products connected through the Internet of Things (IoT)?
  - What engineering-design countermeasures are being, or could be, deployed against these new risks?
- Where have you seen the automation of a product improve consumer safety?
- Where have you seen the automation of a product compromise consumer safety?
- How must a design engineer proceed in designing a completely new type of product for which no standards exist?
  - Select a fictional product and list specific ways that standards (for other products) or prior product experience could guide the design engineers
- Find examples of where *designed-in* levels of product safety did not align with consumer expectations
- Select a product designed and marketed for an "at risk" population
  - Describe in detail and with examples of how this population is "at risk"
  - List what accommodations the design engineers have made for this group and its abilities or vulnerabilities
- What does PSEg mean to you?
- Why might two people differ on whether or not a product is sufficiently safe?
- Can you name any safety *facts*?
- In what ways are a country's values evident to visitors from other nations?
- In what ways may mathematics and science fail the PSEr?
- Identify and list some examples of how society's view of "safe" has evolved over time
- What new technologies do you see as able to improve product safety in the near future?
- In what ways do product liability and product safety differ from one another?
  - In what ways might an engineer's understanding of product liability:
    - Help in product design
    - Harm in product design

Chapter 3: Engineering Ethics

Key Concepts

- *Priorities* versus *Values*
- Business needs may make a pressing, but temporary, priority appear to be a value
- The true values of an organization become apparent over time
- Ethics
- Classical Western ethics

- Unethical behavior may have consequences
    - Provide examples of possible short-term consequences
    - Provide examples of possible long-term consequences
- The isolation of some engineers from the results of their work
- An engineer's ethics should never be compromised by those of an employer
- An engineering code of ethics
    - Engineering codes of ethics are silent on some important aspects of engineering practice
- Engineering Ethics
    - Model of engineering ethics
- Applied Engineering Ethics
- Rules of Applied Engineering Ethics (by the author)
    - Work hard
    - Do the right thing
        - Be able to sleep at night
        - Be able to look yourself in the mirror
    - Make managers and executives earn their salaries
    - Do NOT go to jail!
- Whistleblowing
    - It may become necessary for an engineer to protest or even "blow the whistle" at some point in a career
    - A price will be paid by a whistleblowing engineer
    - Only the whistleblowing engineer may ever know if it was the right thing to do and worth the consequences
- Engineers are, by necessity, practical and paid to deliver results, not theories
- Classical intellectuals differ from technical intellectuals
- Scientists differ from engineers
- The "two cultures" in society (C.P. Snow)
- Engineering ethics is tightly coupled with product-safety engineering
- Simply becoming an engineer should not change the actions of an ethical person
- There are *three* entities in the typical engineer-business relationship
    - The engineer
    - The employer
    - Society
    - And each of these has responsibility "arrows" to the others
- Engineering is a *career*—not a *profession*—to many practicing engineers
- The engineer has a simple *business* relationship with the employer
- Relatively few practicing engineers belong to professional-engineering societies
- Accredited undergraduate engineering curricula and the need for engineering-ethics education
- Many undergraduate-engineering students receive little instruction on ethics

- Some higher-education classes have been, or are being offered, to help educate engineering students on ethics
- Engineers must always act ethically for the good of the public
- Engineers cannot forget their responsibilities to *themselves*
- Engineers *alone* are not responsible for ethical behavior and decisions; management (especially the executive) *also* bears responsibility for creating and nurturing an unethical environment and its resulting decisions and actions.
- Executive corporate management must *establish* and *support* an engineering work environment that encourages ethical behavior and decisions

Discussion Topics and Questions

- Is winning always right and losing always wrong—and why or why not?
    - If so, in what ways does such a perspective affect society?
    - How can it affect a business and the safety of its products?
- Are there any current negative press stories—or even scandals—in the headlines regarding corporate ethics or product safety?
    - Is there truth to any of the allegations?
        - How do you know this? (Is it knowledge or speculation?)
    - Were these problems avoidable and, if so, how?
    - How were/are the problems being addressed by the companies involved?
- At what point, if ever, do corporate actions become criminal?
- Are there differences between *management* and *leadership*?
    - If so, what are they?
- Does corporate "sloganeering" produce results and why or why not?
- Are engineers too isolated from the results and consequences of their work?
    - If so, why?
    - If so, how can this be improved and what would the results possibly be?
- Do you agree that executive management must establish and support an environment *encouraging* and *rewarding* ethical conduct and decisions?
    - Why or why not?
    - Provide examples of how management might do this?
    - What might the rewards be?
- Compare and contrast the ethical requirements of the engineer with those of:
    - A physician
    - An attorney
    - A professional of your choice
- Are present engineering codes of ethics sufficient today?
    - Why or why not?
    - How might engineering ethics be improved—either through the codes or otherwise?
- Does public notoriety (e.g., fame and publicity) affect the objectivity of a scientist, engineer, or physician?

  - Are its effects positive or negative—and provide examples?
  - Provide any examples of this?
- Do you regard engineering as a *career* or as a *profession*?
  - Why or why not?
- To whom does an engineer owe allegiance—and why?
  - Provide examples of this/these allegiance(s)?
- In what ways do the ethics of engineers and scientists differ?
  - Why might there be differences?
- In the wake of the COVID-19 pandemic, what ethical or professional responsibilities do public-health and public-policy officials have to the public whom they serve?
  - Provide examples—good and bad—of how official positions and "science" used by those involved in public health during the 2020-2021 period.
  - Is science a *process*, an *institution*, or *something else*?
    - Support your conclusion
- Can science and technology alone make decisions?
  - If not, what else is needed in the decision-making process?
    - Support your conclusion
- In what way is engineering ethics connected to product-safety engineering?
- Do you agree with the "Rules of Applied Engineering Ethics?"
  - What would you subtract from, or add to, these rules?
- In what ways to *morals* and *ethics* differ from one another?
- What does the term "ethical engineer" mean to you?
- What does—or did—becoming or being an engineer mean to you?
- What has been your "engineering experience?"
  - How might your experience differ from another person's experience?
    - How could this potentially affect your actions as an engineer?
- Do you plan on becoming a registered Professional Engineer (P.E.)?
  - Why or why not?
- Is whistleblowing ever an option?
  - Under what conditions?
  - Find examples of whistleblowers in technical fields
    - What led to these events?
    - What were the results of whistleblowing?
    - Do you agree with their decisions to blow the whistle?
    - Were these situations avoidable?
    - How were these whistleblowers treated?
    - Would they do it all again?
- Do you believe that ethics requirements for accredited engineering curricula are sufficient?
  - Why or why not?
  - If not, how could it be improved? (Provide concrete examples)
    - What, if any, are the challenges to doing so?

- What responsibilities do working engineers have, regardless of professional registration?
    - In what order do these responsibilities rank?
- Did you receive sufficient exposure to engineering ethics in your undergraduate curriculum?
    - How could this be/have been improved?
        - Provide concrete examples

Chapter 4: Product-Safety Concepts

Key Concepts

- Safety hierarchies
    - From two to five steps each
    - The *consensus* safety hierarchy—often called "The Safety Hierarchy"
- Guard versus Safeguard
- Haddon energy-damage countermeasures
- Inherently safe design measures
- Industrial hierarchy of controls (NIOSH)
    - Engineering controls—"hard" controls
    - Administrative controls—"soft" controls
- Classification of safeguard devices
    - Types I–VII
    - There are ethical considerations for some types of safeguard devices
- *Probability* versus *Possibility*
    - Despite standards sometimes calling for it, one cannot reduce the "possibility" of an event
- Engineering judgement—the "common sense" of engineering
- Classification of safeguard systems
    - Zero order
    - First order
    - Second order
    - *n*th order
    - Series and parallel functioning
- Dependency
    - Misuse as a *control system*
    - Misuse in *kind*
    - Misuse in *magnitude*
- Uniformity
- Decreased vigilance
- Compatibility
    - Closed-loop behavior
    - Open-loop behavior
- User activity and product risk

    - Some user-active products cannot produce the same (lower) levels of risks that user-inactive products produce
- User task load
    - NASA Task Load Index (TLX)
    - Consider the product and use environment effects and demands on user/operator
- User qualification and at-risk populations
    - Physical-ability limits and vulnerabilities
    - Cognitive-ability limits
- Haddon Matrix and product-system countermeasures
    - Three phases
        - Pre-accident
        - Accident
        - Post-accident
    - Four factors
        - Product
        - User
        - Physical environment
        - Socio-economic environment
- Structure of NHTSA's FMVSS—100, 200, and 300 series

Discussion Topics and Questions

- Why is there not one unique "Safety Hierarchy?"
    - Is the consensus safety hierarchy sufficient?
        - State why or why not
- List some advantages and disadvantages to using the consensus safety hierarchy within the PDP
- Guards and Safeguards:
    - List three examples of each
    - What are some differences between the two concepts?
- In what ways is Haddon's list of countermeasures to energy release similar to—and different from—the consensus safety hierarchy?
- In what ways are the consensus safety hierarchy and NIOSH's industrial hierarchy of controls *similar* to each other—and *different* from one another?
- Find real-world examples for each of the seven types of safeguarding devices?
- How can focusing on event *possibilities*—rather than *probabilities*—delay or even mislead a product-safety engineering effort?
- Describe what the term "engineering judgement" means to you?
- How, when, and where should engineering judgement be used in the engineering-design process?
- Are safety considerations the *only* pivotal decisions within the PDP—or is safety the only important goal within the PDP?
    - Why or why not?
    - Provide some examples to support your position?

- Determine your own set of zero-, first-, and second-order safeguarding systems for a product/system of your choice
- How foreseeable is user dependence upon a safeguarding system and provide some examples in support of your conclusion?
- Find some examples of “similarly perceived dangers” being treated both uniformly and non-uniformly
- With what type of behavior—"open-loop” or “closed-loop”—do citizens respond when taxes are raised on them and, also, when a product is banned?
  - Justify your answers to the two examples above
  - Can you provide your own examples of open-loop and closed-loop behaviors?
- Create your own User Activity versus Safety Risk plot using your own two example products (or activities)?
  - From your above plot, take two products at extreme sides of the user-activity and safety-risk axes and compare and contrast product-safety engineering measures taken (or, perhaps, should be taken) to protect their respective users or participants
- Conduct your own NASA TLX experiment for two or more products or activities of your choosing
  - Do your results confirm or contradict your suspicions prior to the experiment?
- What are some of the benefits that experienced users of products have over inexperienced users?
  - How can this experience “gap” be bridged by a design engineer?
- Take several products of your choosing and construct a set of user qualifications—even if their designers/manufacturers did not state them explicitly
  - What user populations could potentially be “at-risk” from their use?
- Construct a Haddon matrix for an activity of your choice and discuss where, within the matrix, a participant is well protected and where that participant is vulnerable
  - How might participants be better protected than they currently are?

Chapter 5: Hazards, Risks, Accidents, and Outcomes

Key Concepts

- Hazard
- Risk
- Accident
- Outcome
- Safety
- System(s) engineering
- System(s) safety
- MIL-STD-882E
- Possibility versus probability
- Health versus safety
- Human injury versus property damage

- Severity and probability
- Incident
- Blame
- Hazard identification/hazard recognition
- Product design element
- Emergent property
- Acceptable risk
- Direct effects of severity and probability on risk
- Severity ranking
- Probability ranking
- Notation: $H_{M,N}$ and $R_{M,N}$
- S', P'; S'', P''; S''', P'''; S_0, P_0; and S^*, P^*
- The appropriate role of PPE
- Design intent
- (Final) Outcome
- Risk estimation
- Risk analysis
- Risk assessment
- Risk evaluation
- Risk reduction/risk mitigation
- Risk management
- Risk level
- Inherently safe design

Discussion Topics and Questions

- What is *safety*?
- Is it possible to be *safe*—and why or why not?
- Why did many breakthroughs in system safety take place within the military and the aerospace industries?
    - Provide some examples
- Regarding the *Apollo 1* accident:
    - What led to the accident?
    - Was it preventable and how?
    - Was the accident necessary to force improvements in system safety?
        - If so, why do you believe so?
- Is it productive to consider all *possibilities* when looking at risk?
    - Why or why not?
- What constitutes a *hazard*?
- What constitutes a *risk*?
    - Of what elements is a risk composed?
- Explain how a *hazard* differs from a *risk*
- Explain how a *hazard* and a *risk* are related
- Take a product of your choice and list some of its *hazards* and *risks*

    - Relate the hazards and risks to one another
- Explain how an *accident* differs from an *outcome*
- Take a product or an activity of your choice and list possible outcomes from various accident events
- What other risks (beyond those in the book) can you find from:
    - A lawn-mower's blade?
    - A lawn-mower's gasoline supply?
    - Estimate these risks using Tables 5.2, 5.3, and 5.4
        - Do you agree with your estimated risk found from Table 5.4?
            - If not, how and why do you disagree?
    - Is this risk estimate authoritative?
        - How might someone either support or discredit a result using these tables?
- How would you rate the utility and effectiveness of the U.S. CPSC mandatory warning label for portable electric generators?
    - How could it be improved?
        - How might you verify improvements resulting from your suggested changes?
- Is *assigning blame* a useful exercise?
    - If not, why is it still frequently done?
- Why is what something is called sometimes important?
- What is an *emergent* property?
    - Provide your own examples of emergent properties in products
        - From what do these properties emerge—what product components and attributes affect that emergent property?
- Identify some emergent properties of a:
    - Snow blower
    - Child's car seat
    - Portable electric deep fryer
    - Coffee maker
    - Electric scooter
    - A product of your choosing
- What would a risk plot—as a function of severity and probability such as shown in Figures 5.6–5.8—look like for an arbitrary product such as the one chosen above?
    - Construct its severity-probability "space" to estimate risk
- Why is it difficult to agree upon an "acceptable risk" for a product?
- What is meant by risk being *directly* affected by severity and probability?
- Do you agree with the book's Severity, Probability, and Risk-Estimate rankings in Tables 5.2, 5.3, and 5.4?
    - Are they the result of consensus or research?
    - How could they be improved for classroom use?
    - Are they suitable for real-world applications?
        - Why or why not?
- Can you explain the notation used in $H_{M,N}$ and $R_{M,N}\ (S,P)$?
- Are *only* the most-grave risks for each hazard of interest to a product-safety engineer?
    - Why or why not?

  - Does protecting a user from the most-serious injury risk also necessarily protect the user from less-severe injuries?
- In what ways do the value systems of different people affect risk estimates?
  - Provide some examples to support your conclusion
- In what ways does the operation and maintenance of a large-scale, complex system differ from that of a typical consumer product?
  - Make a list and comment on how each difference may affect user safety
- Is it ethical to make/recommend that users wear PPE when using your product?
  - Why or why not?
    - If so, in what cases is recommending PPE use ethical?
- How might the desire to be "first to market" with an exciting new product affect its safety performance?
- Are NASA-scale system-safety efforts *always* necessary for consumer products?
  - Why or why not?
  - Are such measures necessarily sufficient to assure a safe product?
    - Why or why not?
- In what ways might a product's design *intent* stray away from the product that is ultimately *delivered* to a consumer?
  - Through what mechanisms could this happen?
  - What countermeasures can be put in place to prevent this?
- Do all environmental and user influences affect product safety equally within a given phase—pre-accident, accident, and post-accident—of an accident/outcome situation?
- How can the user-activity level of a given product either increase—or decrease—that product's risk to a user?
  - How, if at all, could this effect of high user activity be attenuated?
- Would the addition of a component such as the fusible extinguishing bulb,[1] shown in Figures 5.12, result in a manufacturing cost increase or a cost decrease to PCB?
  - Would an established supplier competing on the basis of reputation and quality product or a "bargain-basement" supplier competing purely on the basis of *cost* be more sensitive to a marginal increase in PCB manufacturing cost due to adding a component such as the extinguishing bulb? (Remember that the PCBs will be produced by the thousands)
  - Consequently, what is the likelihood that the PCB *most in need of* a countermeasure *will* feature this extinguishing component and why?
  - If something would need to change in order to promote the use of such a component—or a similar device or tactic—how, and by whom, could the necessary change(s) be affected?
  - Why would a manufacturer or supplier *voluntarily* add to the cost of its product?
- Explain the differences between an *accident* and an *outcome*
  - Why are these differences significant to a product-safety engineer?
- Is it fair to criticize a risk-estimation *method* for not delivering an *expected* result?
- Why might someone within a design-and-manufacturing company to expect, want, or demand that a product be given a certain risk level rating by a team of risk evaluators?

[1] Now known as an AMFE—automatic miniature fire extinguisher

    - Is it ethical to insist upon a higher safety rating than warranted (without any appropriate product re-designs) when it comes to public safety?
    - Why or why not?
- How might the "user" of a product, system, or service vary from one industry to another?
    - In what ways could this change in "user" affect product risk?
- Within the risk-management process, what might be the roles of:
    - Technology, science, and mathematics?
    - Prejudice?
    - Opinion?
    - Critical thinking?
    - Engineering ethics?
- What are the components of risk assessment?
- Why is it important to document product-safety decisions and their rationales?
- What is the role of the consensus safety hierarchy within the risk-management process?

Chapter 6: A Product-Design Process

Key Concepts

- Product-Design Process (PDP)
    - Idea/Ideation
    - Concept Selection
    - Engineering Design
    - Manufacturing & Logistics
    - Use (including Repair & Maintenance)
    - Disposal / Recycle
- The product-safety engineering function
- The detailed design
    - The preliminary design
    - An intermediate design
    - The final design
- Engineering, Design, Development, and Testing Phase (EDDTP)
    - Synthesis
    - Analysis
    - Prototyping
    - Testing
        - Laboratory
        - Field
    - Iteration (and Re-Iteration)
- Technology development
- Manufacturing engineering
- Original-equipment manufacturers (OEM)
- Suppliers and sub-suppliers
    - Tier 1, Tier 2, Tier 3, …

- Purchasing Department
    - Quality Control (QC) and Quality Assurance (QA)
    - Production-Part Approval Process (PPAP)
- Stage-and-Gate Process (for example)
- Gate Reviews
- Integrated and systematic product-design process

Discussion Topics and Questions

- Is there a *unique* good PDP?
    - Why or why not?
    - Upon what specifics might a suitable PDP depend—product, industry, world region, …?
- In what ways does mass production of a product potentially affect the safety of the public?
- What are the six phases to a PDP?
- In what ways do, or can, each of these PDP phases affect product safety?
    - Can you identify any product-safety—not *health*—issues that may arise during the disposal of a consumer product?
- List some of the potential problems with depending upon a new technology to be ready, on-schedule, for a new product's production schedule
    - Can you identify any examples on your own of when such problems have arisen with real-world products?
        - What have been the effects of this?
- Why is it often vital to create a product prototype?
- Why is product testing important?
- Will laboratory- and field-testing programs produce identical results?
    - Why or why not?
    - Provide examples
- In what ways can manufacturing engineers help design engineers?
- In what ways do a design-and-manufacturing company's Purchasing and Quality departments assist in the PDP and its product-safety efforts?
- What useful purposes do Gate Reviews serve in the PDP?
- State why the following are particularly important within a PDP:
    - Gate Review II?
    - Gate Review III?
- For what reasons should an integrated and systematic process be used for product design?
    - What could be the results of a non-systematic approach to design new consumer products?
    - Will a product be unsafe if such a systematic product-development process be used?

Chapter 7: Product-Safety Engineering

Key Concepts

- Product-safety engineering versus "compliance engineering"
- Product Risk and the Product-User-Environment (PUE) Model
- Analysis work within the EDDTP
- Testing work within the EDDTP
- Continuous Improvement
- "Safe enough"
- The product-safety engineer/manager (PSMr/PSEr) must be a competent engineer to help identify and *solve* real-world engineering problems
    - The PSEr should be a part of the solution to product-safety problems
- The Product-Safety Engineering (PSEg) function
- Product-safety *management* versus product-safety *engineering*
- Compliance ≠ Safety
- Product *Safety* versus Product(s) *Liability*
- MIL-STD-882E
- Executive management's role in product-safety engineering
- The product-safety engineer and product-safety manager are (often) *not* part of what is generally called Product-Safety Management (PSMt) which is often only *compliance* based
- Prevention of misuse versus fitness for intended use
- Safety reviews
- Any product-safety problems should be discussed *before* a safety review to any avoid public surprises
    - Work out either a solution or a plan of attack "off-line" beforehand
    - Be sure that the "solution" is follow up on and proves effective
- Understand the strengths and weaknesses of any concepts and methods used within the safety-review process
- Management's words, actions, and rewards—they should be consistent
- Speaking truth must be encouraged and rewarded—and never punished
- Test engineering and VVT
    - Verification testing
    - Validation testing
- The importance—and underappreciation—of test engineering
- Analysis (tearing apart) versus Synthesis (putting together)
- Analysis versus Testing
- Capstone-design projects at engineering programs at universities and colleges
- The importance of a thorough test-engineering program in identifying and solving product-safety problems—before production
- Accelerated testing
- Forensic engineering
    - Accident reconstruction

    - Occupant kinematics
    - Biomechanics and injury mechanisms
- Corporate Product-Safety Policy
- A company's true product-safety policy
- The value of a human life
    - Cost-Benefit analysis—why this is *not* covered
- Companies must quickly admit to design mistakes—and then rapidly fix them

Discussion Topics and Questions

- The term "product safety:"
    - What might it mean to a design-and-manufacturing company and its:
        - Assembly-line workers?
        - Managers and Directors?
        - Executives?
    - What does it mean to you as a design or product-safety engineer?
    - What does it mean to your family, your friends, and the public?
- For what reasons do many critical decisions in engineering design become more than applying a simple mathematical formula?
    - How then might/must such questions be answered?
- Why are many product-safety engineering decisions not simple black-or-white choices?
- Is there such a thing as "safe enough" with:
    - *All* consumer products? Explain and provide examples
    - *Any* particular consumer product? Explain and provide examples
- Can a designer/manufacturer, after an injury accident, point to unwise or warned-against product use or user behavior without resorting to "victim blaming?"
    - Explain your answer
- To what extent can a retailer or distributor that is isolated from the design and manufacture of the products it merely sells positively affect the product-safety characteristics of those goods?
    - Will this be an easy or a difficult task to accomplish?
    - What can stand in the way of accomplishing this?
- Regarding executive management:
    - In what specific ways can they assist with product-safety engineering?
    - What are their ethical obligations, if any, to do so:
        - For the company?
        - For its employees?
        - For the company's shareholders?
        - For society?
- What balance should executive management maintain between profitability and product safety?
    - Is profit more important than product safety?
        - Why or why not?
        - Is there evidence of this?
- How might a highly litigious and regulated environment affect the product-safety levels of consumer products?

    - Would this *always* be beneficial to consumers and why?
- Why are safety reviews important in the PDP and EDDTP?
- Can a design engineer be blamed for blindly following the product-safety guidance—both explicit and implicit—given by management?
    - Why or why not?
- When and why might a product-safety or design engineer fear openly discussing a product-safety problem?
    - How could this situation be resolved:
        - By the company?
        - By the engineer?
- Compare and contrast *verification* testing and *validation* testing
- Why is test engineering not a better-known and more-studied aspect of engineering?
- In what critical ways do Analysis and Testing differ?
    - What are the effects of these?
    - Should these two efforts be seen as competitive or as complementary to one another?
- Test one or test many, which is better?
    - Why?
    - Under all circumstances?
- Can a problem be solved if it is not *fully* understood?
    - Can an important problem *ever* be resolved if *complete* knowledge cannot be obtained?
        - How?
- Identify other instances where a competent accident-reconstruction effort could help a design engineer better understand and, thereby, better design a product
- Are all third-party accident-reconstruction results useful to a product's designer and manufacturer?
    - Why or why not?
- What product-use and accident information can be useful to a design-and-manufacturing company and why?
- Placing a value on human life:
    - Can you find any examples of doing this?
    - Do you agree on the methodology/ies used?
    - Are there situations where placing a monetary value on human life unavoidable?
        - If so, provide examples
- Can you identify examples of when a company did *not* admit to an engineering-design flaw in their product?
    - Discuss if and how their consumers, public opinion, or the media responded
    - Was the matter ever resolved and what was the result?

Chapter 8: Engineering-Design Guidance

Key Concepts

- Sources of engineering-design guidance
  - Rules, procedures, and standards
  - Voluntary Consensus Standards (VCSs)
  - Governmental and Industry Standards (GISs)
  - Codes
  - Regulations
  - Agreements
    - With regulators
    - With other members of an industry
  - Other design guidance
    - External
    - Internal
- *Necessary* conditions versus *Sufficient* conditions for product safety
- Consensus versus Majority versus Unanimity
- Do new standards always have a large impact on product safety?
  - Why or why not?
  - Can you provide any examples of your position?
- The Internet of Things (IoT)
- Design standard versus Performance standard—*how* versus *what*
- Standards development
  - Necessity
  - Utility
  - Competence
  - Motivation
- The financial welfare of the public
- ISO Standards
  - Type A
  - Type B (B1 and B2)
  - Type C
- Harmonized Standards
  - EC Directives
- CE Marking and the European Commission
  - Notified Body
  - Authorized Representative
  - Technical file
  - "Manufacturer" of the product
- Product-Designer Matrix
  - Products: New and Established
  - Designers: New and Established
  - Guidance versus No Guidance
  - Proven Ability versus Unproven Ability

    - Potential risks arising therefrom

Discussion Topics and Questions

- If you have gone through or are going through your Capstone-design course, how did you establish performance criteria—especially sufficient safety levels?
    - Would you establish safety levels in the same manner now?
        - Why or why not?
- See if you can identify a new and innovative product being produced today
    - What makes this product new and innovative?
    - How might this affect the product-design process with respect to product safety?
- What does the word "consensus" mean to you?
- How does the requirement for consensus affect the development of standards?
    - Are its effects always either good or bad?
- Why might it be a good idea for a company to have internal design standards and practices?
- What design challenges will design and product-safety engineers face with the burgeoning Internet of Things (IoT) and connected products?
    - What connected products can you find?
    - How have, or how should, product-safety be *designed-into* in these products?
- Design standards and Performance standards:
    - How do they differ?
    - Generally, which kind of standard is better?
        - Why?
- Are standards always necessary, good, useful, and developed by the competent with pure motivations?
    - Why or why not?
    - What could be some of the consequences of your conclusion?
- Read FMVSS 500 (49 CFR 571) for the low-speed vehicle (LSV) and list what you find sufficient and what you find lacking in it
    - https://www.ecfr.gov/cgi-bin/text-idx?SID=7d443eb75ceba033fed91e90f816b574&node=se49.6.571_1500&rgn=div8
- How could the *motivations* of a committee working to develop a standard affect that standard?
- Why are the possible industry activities prohibited by the Clayton Act pertinent to the standards-development process?
- Whose interests do, or should, a standards-development committee member represent?
    - Why is this important?
- For the product of your choice:
    - Find and list standards of Types A, B, and C
    - List the product attributes that each Type of standard addresses
- Why can product standards never keep up with the development of new, innovative product?
    - What effects does this situation possibly have?
- What do the Product-Designer Matrix example's conclusions mean for product users?

- Do design-and-manufacturing companies and regulators always act in an adversarial manner?
    - To what effect for the consumers?
- How might an entrepreneurial mindset affect the amount of pre-sale engineering-design work put into a product?
    - How might an entrepreneurial mindset affect the post-sale surveillance and remediation of products once sold?
    - How could this business perspective affect product safety for consumers?
- List sources of internal design guidance available to a design engineer
- Why might there not be one, single, standalone required PDP?
    - Would such a *process* be desirable—or just its *results*?

Chapter 9: Product-Safety Facilitators

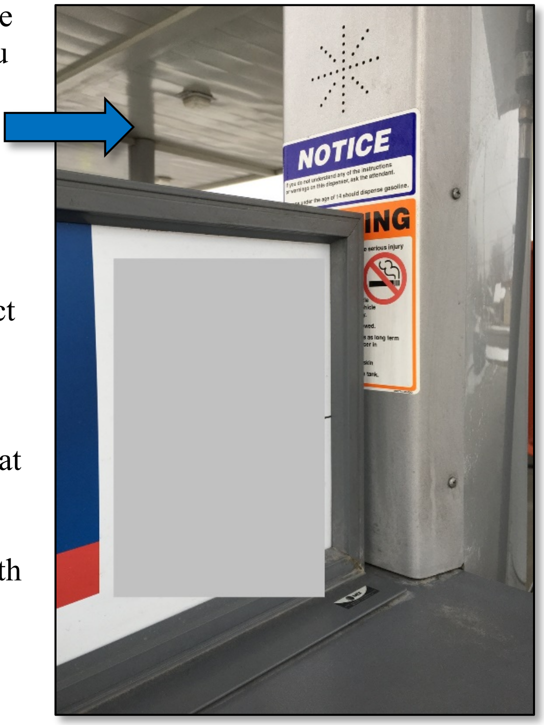
Key Concepts

- Facilitators
- Residual risk
- ANSI Z535.4 for on-product warning signs
- ANSI Z535.6 for product manuals
- Innovative or unique products may require equally innovative and unique product-safety facilitators and approaches in order to effectively convey the information necessary for their safe use to consumers
- The *design* of these materials should be part of an integrated and comprehensive approach to engineering design—not merely an *afterthought* once all design personnel are tired of working on—and even looking at—the project
- These facilitators are *not* to serve as risk-reduction measures *substituting* for additional practical, feasible engineering-design work which could further reduce the risks posed by the hazards of that product
- Proper engineering design should always be considered the *front line* of product-safety engineering
- Facilitators should only be considered in a back-up role to risk reduction after feasible and practical engineering-design work
- Non-traditional approaches to educating and warning product users should be considered and implemented if deemed appropriate
- The goal is the *effective*—not *standardized*—communication of hazards and risks to consumers
- No one will ever construct a set of facilitators with which everyone will agree are sufficient
- What is most important is whether detractors' suggestions would make a significant difference to product-safety levels for consumers when all factors—product, user, and environment—are considered
- Mere compliance with standards *may* be a *necessary* condition, but it may not be a *sufficient* condition for providing the necessary levels of product safety to consumer

- It is more important to effectively communicate hazards to consumers than it is to merely produce materials compliant with standards

Discussion Topics and Questions

- Consider an arbitrary product and determine how heavily its safe use depends upon facilitators
    - Are the facilitators necessary for safe product use?
    - Under all conditions or just some conditions?
- Do warning signs and manuals *ever* work?
    - If so, under all or what conditions?
        - How can they be made better?
    - If not, is there a way to get them to work?
- If warning signs *never* work, then is it ethical to *ever* deliver products with *any* latent (non-obvious) hazards and risks?
    - Under what conditions?
    - *Must* warning signs, therefore, *necessarily* work to some degree?
        - Why or why not?
- Look at—and even photograph—the warning signs on some of the products and facilities (e.g., gasoline pumps) that you encounter in daily life
    - Critique those that you find including this example
        - Are they as good as they could be?
        - Are warnings obstructed by advertisements?
        - How might they be improved?
        - Construct your own preferred warning signs
    - Are there either too many or too few for safe product use?


NOTICE
If you do not understand any of the instructions or warnings on this dispenser, ask the attendant.
under the age of 14 should dispense gasoline.
ING
serious injury
hicle
wed.
s as long term
skin
tank.

- As many readers already know, airlines generally have a passenger-safety information booklet in the seat backs of their planes. These booklets contain details on the use of seat belts, oxygen masks, emergency exits, evacuation slides, life-vests, and more. Instead of using black-and-white images in these booklets, many booklets contain figures with multiple colors to show grass, water, sky, smoke, and pertinent safety devices. However, the same images also include colors for aircraft-cabin interiors and passenger clothing and skin tones
    - Does the excessive use of color *add to*—or *subtract from*—the overall efficacy of such a safety booklet through “color pollution?”
- Select an owner’s manual of your choice and then examine it in light of topics and issues discussed in this chapter
    - Does it appear sufficient?
    - Does the manual go far enough in:
        - Describing operation
        - Describing hazards and risks?
            - Are risks readily known or knowable?

            - Should additional effort be made to explicitly show the consequences from not avoiding the risk(s)?
        - Listing and showing countermeasures to these hazards and risks?
    - Does the manual go too far by showing unnecessary details in photographs or drawings that obstruct the safety message through "detail pollution?"
        - What changes would you suggest to improve it?
- Without actually looking at the warning sign(s) for an existing hazardous product of your choice, mentally identify its hazards and then construct your own warning sign for its most-hazardous aspect.
  Then, compare and contrast this warning sign to the warning sign(s) found on such products in a brick-and-mortar or virtual store.
  For example:
    - Construct a warning sign for a walk-behind lawn mower to caution users about the rotating-blade hazard and risk of amputated toes and fingers. Then, go to a store and look at the warning signs and their placements on several lawn mowers.
        - How similar were your warning signs?
    - To what extent are hazards open?
    - To what extent are hazards obvious?
- Consider the manual style such as that used in Case Study 9.3 on page 255. Could this method be applied to other activities?
    - List some of them
    - What could be areas of application within each activity?
        - What prescriptive and advisory statements might be included?
        - What consultative questions might be asked of participants?

Chapter 10: Product-Safety Engineering Methods

Key Concepts

- Hand-powered winch (Appendix B)
- Preliminary Hazard List (PHL)
- Preliminary Hazard Analysis (PHA)
- Product-Safety Matrix (PSMx)
    - *Safety* PSMx
        - Design a *system* of engineering countermeasures
        - Role of product-safety facilitators
        - Competitive benchmarking
    - *Compliance* PSMx
        - Compliance measures
        - Roles of standards, regulations, agreements, …
- Failure-Averse & Fault-Tolerant Design Approaches
    - Active versus passive
    - Reliability
    - Preventive maintenance (PM)
            - Risks from not following the PM schedule
    - "Fail-safe" design *approach*

        - *Designs* versus *failure modes*
    - Manifest danger
        - Direct cues
        - Fault indicators
- Failure Modes and Effect Analysis (FMEA)
- Failure Modes, Effects, and Criticality Analysis (FMECA)
    - Inductive
    - Bottom-up approach
    - Single failures
    - Design FMECA (DFMECA)
    - Interface between OEMs and suppliers
- Fault-tree analysis (FTA)
    - Deductive
    - Top-down approach
    - Top-level event (TLE)
    - Events and basic events
    - AND gates and OR gates
    - Single-point failure (SPF)

Discussion Topics and Questions

- Think of some "people things" that people continue to do despite knowing that it may not be in their best interests to do so
    - Why do they keep behaving in these manners?
- What do you believe is the "extent practical" when it comes to product-risk reduction?
- List some of the capabilities and limitations of the PSMx within the PDP and EDDTP
- In what ways do the product-safety *design-engineering* and *compliance* exercises differ from one another when completing a PSMx?
- How might benchmarking a competitor's products help a company's product-safety engineering efforts?
- What is the role of product-safety facilitators in the EDDTP?
- Why is it important for design engineers to know the limitations of product-safety facilitators?
    - List some examples of how not knowing facilitator limitations could compromise product safety for a user
    - Can you find examples of products where there is, or may be, an overreliance upon facilitator capabilities?
- Why is the flexibility of (ability to customize) the PSMx important to a design-engineering effort?
- Take a sample of products with which you interact daily and consider the types of failure approaches implemented in parts or aspects of each product
    - Are they failure-averse or failure-tolerant in its nature?
    - Do they employ reliability, PM, fail-safe design, or manifest danger?

- Many USAF Generals have preferred twin-engine fighter planes over single-engine planes. They have stated that their reasoning is "reliability."
    - Does this argument stand up to scrutiny?
        - What must be assumed to make this reasoning correct?
            - Aircraft reliability values?
                - Individual vs. Combined *engine* reliabilities
            - Aircraft performance while operating on one of two engines?
                - Can the mission be completed on a single engine?
                    - If not, is an aircraft with a single engine more or less likely to complete one particular mission than an aircraft with two of the same engines?
- Automobile TPMS (Tire-Pressure Management System)—When was the last time you checked the air pressures in your automobiles tires?
    - Has it been a long time and, if so, why?
        - Consider the following when responding:
            - Dependency
            - Type of misuse
            - Manifest danger
- Under what circumstances might a PM design approach to failure degenerate into a manifest-danger approach?
    - Provide some examples
- What do you believe that the author means by "safe product use may become the *practical* responsibility of the user" (p. 307)?
    - What are your thoughts on this?
- What are some strengths and weaknesses, with respect to product-safety engineering, to the:
    - FMEA/FMECA
    - FTA
- How can there be an accident with a product *without* a failure?
- What are the practical differences between a *bottom-up* and a *top-down* analysis technique?
    - What are the effects on product designs resulting from the two different analysis approaches?
    - Consider situations where one might be a superior product-safety engineering method over the other:
        - Bottom-up better than top-down?
        - Top-down better than bottom-up?

Chapter 11: Product-Safety Defects and Recalls

Key Concepts

- Defects
- Product-Safety defects
- Product safety and function

- Product-safety recall criteria
  - U.S. CPSC
  - U.S. DOT/NHTSA
- Unreasonable risk
- Substantial risk
- Types of safety defects
  - Manufacturing defect
  - Design defect
  - Marketing defect
- Avoidable product-safety recalls
- The role of the Purchasing Department in corporate product-safety efforts
- The role of the supply chain in corporate product-safety efforts
- *Fault* versus *Failure*
- Creating innovative product may lead to product-safety recalls
- The continuous change in an established product's design
- Post-Sale data:
  - Sources
  - Aggregation and storage/retrieval in an electronic database
  - Review and monitoring
  - Investigation
- Product-Safety recall process model
  - Nulla Data Collection and Mining
  - I. Initial Analysis
  - II. Intermediate Analysis
  - III. Advanced Analysis
  - IV. Final Analysis
  - V. Product-Safety Recall
    - Affected product units (to identify which products are defective)
    - Proposed solution as an EDDTP effort
- Short-term and long-term perspectives on product-safety recalls
- "Off-Ramps"
- Legal versus ethical product-safety recall obligations
- Whistleblowing
- The decision to execute a product-safety recall
- The *Groupthink* phenomenon
- "Would I let my loved ones use this product?"
  - The answer
  - The time taken to answer
- *Heuristics*
- Small sample sizes in post-sale product-safety data
- Cognitive Bias
  - Survivorship Bias

Discussion Topics and Questions

- How can varying levels of ego, interests, leadership, and bias affect the product-safety recall process?
    - Consider ways in which these factors can either facilitate and harm a product-safety recall group investigation and/or decision
- Why are objectivity and critical thinking helpful when considering a potential product-safety recall?
- Are accident victim and eyewitness testimony alone sufficient when considering the performance of a product which injured someone?
    - Why or why not?
- Are product-safety recall criteria sufficiently precise?
    - If not, what recommendations do you suggest?
    - Thus, how should such decisions be made?
- Identify and discuss the similarities and differences between manufacturing defects and design defects
    - Are product recalls for these two types of product-safety defects different because of any differences between defect types?
        - If so, how do they differ?
    - What, if any steps, can be taken by a company before a recall to facilitate a rapid, thorough, and effective recall of its product(s)?
- Is it proper to include facilitators as part of a product *design-engineering* effort rather than as part of a *marketing* effort?
    - Why or why not?
- Research recent product-safety recalls at www.cpsc.gov to identify what you would consider an “avoidable recall
    - Why do you believe it to have been avoidable?
    - How could similar safety recalls be avoided in the future?
- Can you identify a recent recall which:
    - Should have been obvious to its designer?
        - If so, why and how should it have been readily evident?
    - Required some amount of analysis and testing before identifying the problem and then devising an effective solution?
- In what ways can a design-and-manufacturing company’s supply chain impact its product-safety efforts?
    - How can these effects be mitigated?
- Do you agree that designing and producing innovative products may lead to a greater number of recalls than doing the same with standard, non-innovative products?
    - Why or why not?
    - Can you find and provide your own examples?
- Identify a product which has been produced for years without significant change and use your “engineering judgement” to identify changes that might have taken place within that product due to factors such as cost cutting and supply-chain changes
- Can you identify a historic product whose design had not undergone regular changes and whose designer/manufacturer might have gone out of business as a result?
- Identify a product whose use—and subsequent accident data—would exhibit seasonality

  - How does the seasonality of some data affect a potential product-safety recall investigation effort?
    - Can this effect, if any, be mitigated—and, if so, how?
- Consider the evaluation of post-sale product-safety data for a product of your choice and identify why its evaluation could be a complex process
- Why is it wise to consider the accessories offered for a product by its designer and manufacturer?
  - State some examples as well as their potential effects
- Should the effects of accessories sold by *other companies* be considered by a particular designer and manufacturer?
  - Why or why not?
  - Could such consideration prove overwhelming?
  - At what point, if ever, do the designers, manufacturers, and retailers of these *other accessories* become responsible for the safety of a new, combined product system?
- As an engineer working for a design-and-manufacturing company, why might it take courage to recommend the recall of a product for safety reasons?
  - In what ways do or might a product-safety recall affect a company?
- How should engineers respond when their company concludes that a product-safety recall for an issue is not legally required, but when engineers still conclude that a recall is necessary?
  - If your answer requires engineer action, construct a list of possible actions that might be undertaken and go into detail about how an engineer might proceed
- Are any accidents/outcomes *solely* the fault of the product user?
  - In what cases do you believe this to be true?
  - How, if at all, might the design-and-manufacturing company still reduce the risks of their product to consumers?
- What is the *consumer's* role in affecting an effective product-safety recall?
- Identify one product for which its post-sale data might be:
  - Relatively straightforward to evaluate
  - Potentially difficult to evaluate
- Do you believe that *groupthink* takes place?
  - Have you witnessed examples of this taking place at work, at school, or in life?
  - Discuss its effects if you have experiences with it taking place
- Discuss and make observations about the survivorship bias example from this chapter
  - Have you witnessed this phenomenon or other cognitive biases in work, school, or life?
- Identify and evaluate the potential effects of other cognitive biases on engineering design and user product safety
- Why are objectivity and critical thinking helpful when discussing the need to recall a product that could pose an unreasonable safety risk to its users?

Chapter 12: Conclusions

N/A

Backmatter

N/A