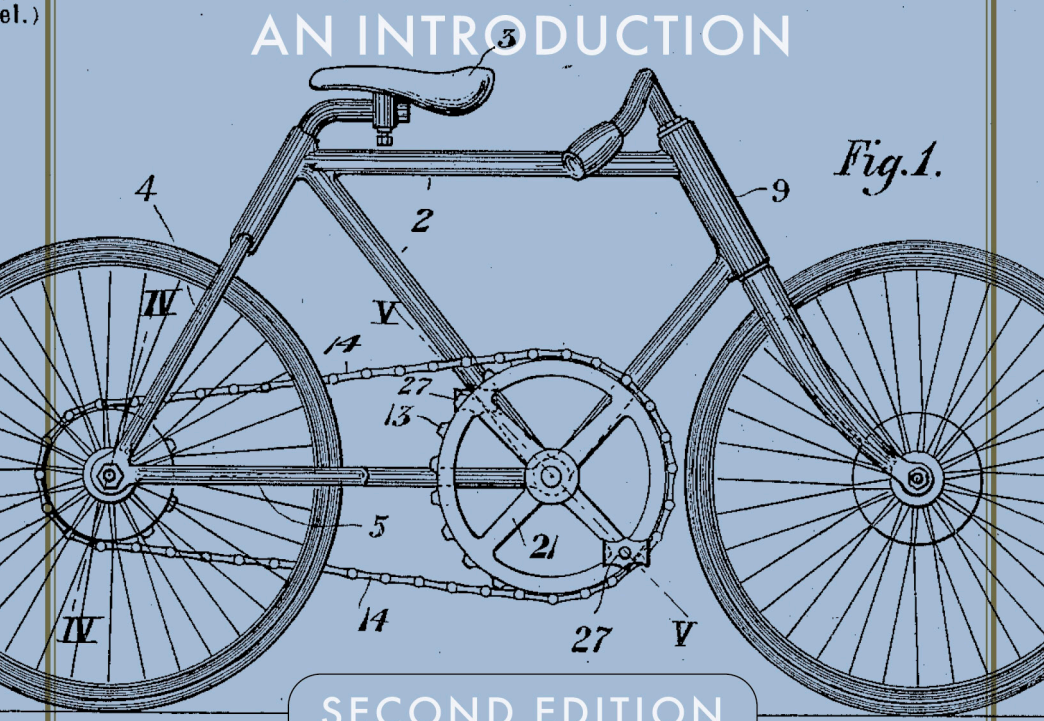
WADE L. ROBISON

ETHICS WITHIN ENGINEERING

AN INTRODUCTION



SECOND EDITION

BLOOMSBURY

Ethics Within Engineering

Also available from Bloomsbury:

Practical and Professional Ethics, Wade L. Robison
Introduction to Applied Ethics, by Robert L. Holmes
Environmental Ethics, by Marion Hourdequin
Ethics: The Key Thinkers, edited by Tom Angier

Ethics Within Engineering

An Introduction

2nd Edition

Wade L. Robison

BLOOMSBURY ACADEMIC
LONDON • NEW YORK • OXFORD • NEW DELHI • SYDNEY

BLOOMSBURY ACADEMIC
Bloomsbury Publishing Plc
50 Bedford Square, London, WC1B 3DP, UK
1385 Broadway, New York, NY 10018, USA
29 Earlsfort Terrace, Dublin 2, Ireland

BLOOMSBURY, BLOOMSBURY ACADEMIC and the Diana logo are trademarks of Bloomsbury Publishing Plc

First published in Great Britain 2016

This edition published 2024

Cover design: Ben Anslow
Cover image: Patent drawing for velocipede filed Sept. 7, 1898 by Wesley Johnson of Pennsylvania. Patent granted June 20, 1899. (© National Archives)

A catalogue record for this book is available from the British Library.

A catalog record for this book is available from the Library of Congress.

ISBN: HB: 978-1-3503-4044-2
PB: 978-1-3503-4043-5
ePDF: 978-1-3503-4046-6
eBook: 978-1-3503-4045-9

Typeset by Deanta Global Publishing Services, Chennai, India

To find out more about our authors and books visit www.bloomsbury.com and sign up for our newsletters.

To Christina

Contents

List of Figures viii
Preface ix
Preface to the Second Edition xv
Acknowledgments xvii

1 Introduction 1
2 Analyzing Accidents 21
3 Error-Provocative Designs 31
4 Airliner Crashes 57
5 Moral Responsibility: Intent Is Not Necessary 79
6 Permitting, Encouraging, and Provoking Errors 89
7 Harms and Design Solutions 107
8 Role Morality 135
9 Forms of Life 157
10 Working with and for Others 177
11 Engineering and Ethics 199

Notes 211
Bibliography 225
Index 233

Figures

1	Japanese toothpick	5
2	Japanese toothpick, used	5
3	Toothpick for the tongue	8
4	Stovetop with burners in a row	32
5	Stovetop with burners and knobs lined up	38
6	A different stovetop configuration	42
7	How the stovetop in Figure 6 really works	43
8	My parents' stovetop, how it really worked	45
9	Stalling angle of attack	65
10	Notice of Microsoft Exchange Server error	114
11	Clearview font	130
12	Shuttle booster rocket joint	147

Preface

An interest in engineering ethics has generated an enormous amount of scholarship over the past few decades. So anyone who writes on how ethical considerations enter into engineering owes much to many. But though I have learned much from those who have written on the subject, I will cite few because I will be concentrating on a way in which ethics enters engineering practice that has been downplayed, if not downright ignored, in the vast literature we now have.

I will concentrate on how ethical considerations enter into the intellectual core of engineering, the solution to design problems. Engineering begins with a design problem—how to make occupants of vehicles safer, settling on the interface for operating an X-ray machine, designing more legible road signs, and so on. Any design problem leaves much room for creativity and innovation, and so the range of possible solutions to any particular design problem is broad. We can see how broad by looking at the various kinds of cars, or toasters, or coffee makers, or computers: each artifact marks one design choice over another.

In choosing any particular solution, engineers must make value choices, and, obviously, as we again know from looking at engineering artifacts like cars, not all design choices are equal. Each reflects a particular configuration of values with a particular set of effects, the effects ranging from those produced by obtaining the material from which the artifact is to be manufactured, to those produced in the manufacture, to those produced in moving the artifact to market and storing it until it is sold, to those produced by those who use the artifact, and to those produced in disposing of or recycling or remanufacturing the artifact once its useful life is completed.

The easiest way to understand how ethical considerations enter into engineering is to focus on design solutions, which cause problems for those who use the artifact embodying the design, and the clearest

examples of those are solutions, which provoke even the most intelligent, well-trained, and most highly motivated into making mistakes and sometimes causing great harm—for example, by designing an X-ray machine that can easily over-radiate patients or a car or truck with a high risk of exploding if hit.

Everyone is subject to the minimal ethical principle: do no unnecessary harm! Engineers have special obligations to take care not to cause unnecessary harms because they can cause a great deal of harm by virtue of being engineers and are best positioned to choose design solutions that minimize harm.

The intellectual core of engineering, the source of the intellectual joy that animates it, is the working through of various possible design solutions and settling on a particular design that solves the original problem and perhaps pushes the envelope of design. At its core this is an ethical enterprise since the particular configuration of effects of each design solution will cause more or less harm and so will be, all else being equal, more or less ethical.

These ethical issues are internal to the discipline of engineering. An internal ethical issue is one that arises within a discipline. No one can be an engineer without solving design problems, and so no one can be an engineer without making the ethical decisions we must make in solving those problems. We should presume that every discipline has its internal ethical problems. A physician, for instance, cannot practice without treating patients in one way or another—with respect as a person, or as a piece of machinery to be fixed, say—and those are radically different ethical views to take of a patient.

Such internal problems are distinct from what I call external ethical problems—an engineer who, as a buyer for a company, faces requests from a supplier to let through somewhat questionable parts; an engineer who is upset to find himself working under a younger female boss when he thought he was going to be promoted; an engineer who, as a manager, is ordered by someone farther up the chain to get a product done by a certain time when the testing will not have been completed. These are problems that arise because the engineer is not working just

as an engineer, but as a buyer, employee, or manager—positions any professional could hold and problems any professional may face.

Internal ethical issues are those that only someone within a discipline will face, and they are, to my mind, the most important ethical issues engineers will face. Yet, as I say, they tend to be ignored. This book is the antidote to that. I will generally ignore external ethical issues to concentrate upon internal ones.

That is not to say that external ethical issues are unimportant. It is to say that we need to pay at least as much attention to internal ethical issues as the current literature on ethics in engineering tends to pay to external ethical issues.

I came to see the value of thinking of design solutions as embodying ethical choices when I took the senior design class at my university. I worked with a number of engineering seniors from various departments in the college, and we had a contract with two internists from the Strong Memorial Hospital in Rochester, New York, to develop a self-propelled colonoscope.

The standard way of inspecting for cancer in a person's colon is to insert a stainless steel articulated endoscope with a lens, a hook for grabbing suspect tissue, and a small hose for cleaning off tissue that needs detailed inspection. The endoscope has to traverse the colon and make two sharp turns where the colon attaches to the rib cage on either side, and the risk of harm is high because cancer makes the lining of the colon friable and easily penetrated—especially by a steel endoscope with the circumference of a small pencil. It takes great skill to maneuver the endoscope, and the internists were looking for a device that would significantly decrease the need for a specialist taking extreme care. An endoscope that would propel itself through the colon and do so without touching the colon walls was the goal of our engineering group.

What I noticed was that the engineering students and I were looking at the problem in different ways and so focused on different aspects of our project. The engineering students were intently concerned with getting something that would work. "How do we get it to move through the colon?" I found myself thinking about how the endoscope would

be used and so focused on what could go wrong. Since not touching the colon walls was part of the design problem, the students considered that but failed to consider what would stop this motorized endoscope if it took off up the colon. When that concern was raised, a student said, "Ah, good point," and the group proceeded to ensure that the endoscope could not take off. Their focus put to the periphery of their vision, unnoticed except when drawn to their attention, concerns about the harms to be avoided.

If we focus not just on whether the solution solves the original problem but also on whether it solves the problem without causing any unnecessary harms, we make explicit what is implicit in any choice of a design solution: we are making an ethical choice no matter what we choose. Once realized in an artifact, each choice carries with it a set of harms, and except choices with only minor differences, those sets are going to differ from each other. We do not need to provide a formula for weighing those harms against each other or against the benefits that may also be realized to see that, whatever the results, we would be putting on the scales what has moral weight.

Engineers distinguish between what they call the hard and soft, or professional, skills.[1] The distinction is questionable, to say the least. It makes it sound as though there are difficult rules to learn, the hard ones, and easy ones, the soft ones. But it can surely be as hard to communicate clearly as it can be to calculate stresses. It takes a master to engineer a sentence that says exactly what needs to be said and no more. Even a master of communication can fail the test of clear and perspicuous communication because, as it turns out, it is not easy to make things clear.

The distinction also does not do the work engineers apparently think it does. It does not divide the skills engineers must learn from those historians or poets, say, must learn. The distinction is meant to separate off the skills students learn from STEM courses from the "extra" stuff like an ability to communicate effectively. There is a movement afoot to add these so-called soft skills to the engineering curriculum.[2]

But they are already there, embedded in engineering practice. Consider the "soft skill" of making ethical judgments. Engineers cannot help but make use of that so-called soft skill in solving design problems. They cannot help but make an ethical choice in choosing one solution over another, I shall argue. Moral considerations are already embedded in the intellectual core of engineering, the solution to design problems.

I shall make this point as vividly as I can by focusing on what I call error-provocative designs to illustrate that ethical considerations enter into design solutions. These are design solutions that provoke errors in even the most intelligent, well-trained, and highly motivated operators in the most pristine circumstances. The design provokes us into making a mistake, and the fault then lies with the design—and the designer—not with us or the circumstances.

Using error-provocative design solutions to illustrate how ethical considerations enter into design solutions may mislead readers into thinking I am writing a book to warn engineers not to pick such terrible design solutions. But I am not looking at what goes wrong, the disasters to be avoided, in order to tell engineers to avoid them—but to illustrate most clearly how any design solution embodies ethical choices and how engineers need to make explicit what they are already doing implicitly in solving any design problem.

The aim of this book, in short, is to show that ethical considerations enter into all design solutions and thus are integral to the intellectual core of engineering. They cannot be avoided. The aim is to make explicit how those ethical considerations enter.

The ultimate goal is to change the way in which ethics is taught in engineering. It is now either an add-on to existing courses, generally discussions of cases, or a separate course called engineering ethics. Both alternatives send the message to students and faculty alike that ethical considerations are not integral to engineering practice. I shall argue in what follows that they are.

I obviously do not expect this book to change a long-standing practice but do hope that once the idea is given a hearing, it will win adherents and ultimately change the practice. That change will require pushing

back against the quantification of the criteria of the Accreditation Board for Engineering and Technology (ABET), but also, in the meantime, providing a numerical weighing, however artificially determined, for the various harms that may occur with various measures of risk for each of them. Engineers are certainly more competent to do that in the detail required for any particular design choice than anyone outside the discipline.

Preface to the Second Edition

The main thesis remains central: ethical considerations enter into the core of engineering, the solution to design problems. They enter into every design solution, from the failures to the marvelous successes that have given us a complex technological world that would have been unimaginable not all that long ago. Who would have thought fifty years ago that we could talk with and see someone on the other side of the world in real time?

But rather than applaud engineering successes, I have concentrated upon the harms that can result from design solutions. One reason is that I can then piggyback on what engineers already do and do very well, making sure that their design solutions do not cause unnecessary harms. That is why I say that I am not proposing that engineers introduce ethics into engineering, but pointing out that they already do. It would take another, very different book to show how the rich technological world we live in illustrates engineering's ethical commitment to the public good.

Readers should not be misled, therefore, by my concentration on harmful design solutions. I am not providing here a complete picture of how ethical considerations enter engineering. What is missing from the first edition besides an examination of how ethical considerations enter into engineering successes is a survey of the ethical problems engineers can face when working with and for others.

These problems are no different in kind than those faced by anyone on a team, for instance, and no different in kind than those faced by any professional working for someone or some company. They are not internal to engineering, that is, not essentially related to solving design problems.

I was moved to add a chapter on these external ethical issues after adding a section on what went wrong with the Boeing 737 MAX, concentrating upon the software engineering that was supposed to

make it fly like its predecessor and upon Boeing's insistence that there was no need to inform airlines or pilots of the changes created by the software. I found myself unable to explain what went wrong at Boeing without referring to the management's failures and to the failures of the participants to communicate with one another.

Engineers generally work in teams, and, as we all know from our experiences in working with others, a team can fail to gel in a variety of ways for a variety of reasons. When that failure results in avoidable harms, as with the Boeing 737 MAX, we have ethical problems. Engineers need to be aware of such problems and at least make arrangements to minimize them.

Engineers also generally work on contract or for companies. Being an engineer and an employee can create all sorts of ethical issues as the demands of one role conflict with the demands of the other, and a company's structure and decisions can create ethical problems as well. Something is clearly wrong when test pilots fail to inform engineers about problems they had with software fixes and when engineers fail to inform pilots about changes they have made that will affect how the plane flies.

I have compensated somewhat for the additional text of the section on the 737 MAX and the chapter on external ethical issues by removing what I now see was redundant or failed to further the narrative. That seems minor, but removing excess verbiage has, I hope, made the sections more concise and easier to comprehend.

I should not end without thanking the anonymous reviewers who suggested changes in the first edition. I have no doubt failed to resolve all the difficulties they raised, but hope it is a better book because of their constructive suggestions.

Acknowledgments

When I came to the Rochester Institute of Technology as the Ezra A. Hale Professor in Applied Ethics, the Provost suggested I visit the Dean of the College of Business to see if I could help with business ethics. The Dean said, in dismissing me, "We're all ethical here." I was amused but went next door to the College of Engineering. The Dean there, Paul Petersen, welcomed me, but told me that if I was going to have any street cred among engineers, I needed to take their senior design course, the capstone of the five-year program. So I did, and I learned an immense amount working with a group of students designing and making a self-propelled colonoscope. I learned more about the workings of the colon than I ever wanted to know.

I then started teaching with Jasper Shealy in the Department of Industrial Engineering, an association that continued for four years or so and afterward lectured on ethics in engineering to the students in the capstone course, telling them something I thought, and think, they needed their first year.

I cannot thank Paul and Jasper enough for their kindness in letting a philosopher into their midst and to Jasper in particular for letting me teach with him. I found him a wonderful teacher, and I learned far more about engineering than I did about colons. I lifted from him the example in Chapter 9 about how those who ski with helmets simply ski faster and so do not diminish their risk of injuries. Jasper and Paul both have my thanks. They would probably think I did not learn enough, but I certainly cannot hold them blameworthy for what follows. They did their best with the material they had, with me, that is.

I also want to thank all my students through the years and especially those to whom I have explained the idea of an error-provocative design. The idea itself seems to provoke example after example, and much of what I have been given by them has found its way into this book. Two students deserve special mention. Ryan Sidel provided the Mazda

example in Chapter 7 where, because of his big feet, he found himself unable to push in the clutch, a thoroughly unexpected consequence of a design choice. Zak Kulage provided the problem with the Cadillac trunk in Chapter 7, a problem confirmed by my father-in-law, Bob Lopez, who jumped out of the car to prevent me from breaking the trunk motor and lock. I am particularly indebted to my colleague, David Suits, both for the surfeit of examples he has provided and for his having read through the manuscript and made many a helpful comment.

I am also indebted to Adam Potthast at Park University and Mark Vopat at Youngstown State University. They each used drafts of the book in classes, and I have learned much from their responses and their assessments of where students had problems understanding the text. Just as engineers need to test their design solutions, so writers need to test their creations. Some may decide the book needed more testing, but I alone am responsible for the errors that remain.

My wife, Christina, has been a godsend, helping me talk through problems I ran into as I tried to put my thoughts into words uncluttered by philosophical jargon. For the first edition of this book, I also owed a special thanks to our companions—to my beloved Scout, the wonder pup, now gone after our affectionate fifteen years; to our beloved and much missed pups Mangia and Gus and Tess, the fierce kitty, who came with Christina; to Raven, our live-in crippled bantam rooster, also now gone, for the companionship he gave us all as well as the insights into just how bright a little rooster can be; and to our new kitty, Peaches, and the pups, Laddie, Gage, and Sunny. We have now lost those three pups, and so for this second edition, I need to thank Charlie, Joey, and Ollie, our new pups, and especially Pepper, the wonderful kitty who came to our door cold and emaciated, asking for help.

1

Introduction

§1. Our Moral World

Engineering artifacts permeate our lives—from cars and iPhones to bridges and planes. Our lives are safer and healthier, richer and fuller, for all that engineers have done. It would be almost as difficult for us now to imagine a world without cell phones as it would have been for our great-grandparents to imagine a world in which they could pick up a little rectangular object and speak with someone on the other side of the world.

There are clunkers, of course. We are all familiar with things so badly designed they cause us to make mistakes: doors that look as if they open one way when they open the other; control knobs that look as if they are to be turned to operate but must be pushed in or pulled out instead; "DO NOT ENTER" signs on entrance ramps so placed that they seem to tell us not to enter where we must. It is unfortunately all too easy to find such designs.

We can always find news of them in the headlines. The crash of the Virgin Galactic SpaceShipTwo killed the copilot, who caused the crash when he "prematurely unlocked a section of the space plane's tail used in braking."[1] The company that did the hazard analysis failed to consider "pilot-induced" errors.[2] It concentrated on the plane and failed to consider how hazards could be introduced through how it would be flown.

We do not know if the copilot's error was induced by the plane's design, but it is easy enough to find designs that provoke errors. The worst are those that provoke mistakes for even the most intelligent,

well-trained, and highly motivated operator, in the most pristine of circumstances. We can find such designs in even the most mundane artifacts. We need look no further than our toasters.

One comes packaged with a slip of paper saying, "WARNING! To interrupt toasting, turn toast color control to off/cancel. Do not push the toast lever manually. Internal mechanism will be irreparably damaged." As someone asked, "What kind of toaster is 'irreparably damaged' by using the LEVER to remove the toast?" We use the lever to push the toast down, and levers generally work in both directions: what goes down goes up. The toaster mechanism will be irreparably damaged by many users who failed to see the warning or having seen it pulled the lever up out of habit while hurriedly trying to save the toast from burning.[3]

That toaster is an accident waiting to happen, an unfortunate solution to part of a complex design problem: How can we toast bread and yet interrupt the toasting? Perhaps the solution was driven by considerations of cost or a change in the internals of the toaster, but to the extent that engineers designed the toaster and signed off on the final design, they are responsible for the results—for the predictable harm of customers breaking the toaster, for one thing.

A toaster that can be irreparably damaged by lifting the lever up is an artifact whose production was a waste and whose quick end is waste that we must put somewhere. We have in that artifact a set of unnecessary harms—those that come from getting the materials to make it, those that come from squandering the energy required to make it, those required to package it, ship it, store it, and use it until it burns our toast and we break it, and those required to rid ourselves of the trash it has become. These are harms because they set back interests we have such as not wasting our money on something that will quickly break and not polluting our air and groundwater any more than necessary. For engineers to choose that particular toaster design from all the possible designs is to make a moral choice, one that will produce more harms, and worse harms, when realized in an artifact than other choices they

could have made. We live in a contingent world that reflects moral choices we have made.

We each no doubt have our own favorite examples. They seem to be object lessons in the frustrations of life, things we have to live with. But there is no necessity that toasters be designed that way or that "DO NOT ENTER" signs be so placed as to mislead drivers into thinking they are on the wrong ramp or that doors look as though they open one way when they open the other. These examples come about because of choices people made. They are artifacts, designed by and created by us.

If it seems puzzling that ethical considerations enter our lives even in the artifacts with which we have populated them, think of how ethical considerations enter our lives even in what we might consider the most mundane of circumstances because of choices we make. If we choose to pick up and answer our cell phone while driving, we have chosen to increase the risk of our having an accident as well as the risk to others. Increasing the risk of harm is itself a harm, and so, in choosing to answer the cell phone, we have chosen an option that is more harmful than the other option, immediately available to us, of not answering the phone.

We have few better examples of how our lives are shaped by such decisions. Not many drivers have escaped having to shape their driving by another driver's failure to signal because preoccupied with a cell phone or by a driver's slowing down and speeding up as the conversation or text becomes more and less animated. The list of how we must accommodate ourselves to the choices of others is long, but the point is short: the way we move down the highway is no different than the way we move through the world. We move in a world created and shaped by moral decisions.

So we should not be puzzled that morality permeates our lives through the artifacts of our lives. That toaster? Those misplaced "DO NOT ENTER" signs? The driver wandering on the highway while talking or texting on a cell phone? Toasters do not need to be designed

so they break so easily. Signs do not need to be misplaced. Drivers do not need to use cell phones. These are all results of choices, and those choices have ethical implications.

The test in these cases is whether the choices cause unnecessary harms. Everyone is subject to the minimal ethical principle: do not cause any unnecessary harm. As soon as the possibility of harm enters, ethics enters, and the possibility of harm enters everywhere in engineering practice, from choosing a design problem to its solution to its realization in an artifact to the artifact's end life.

Engineering practice is complex, but its intellectual core is the solution to design problems, and that is where we will begin. If a convincing case can be made that ethical considerations are integral to solving design problems, engineers should have no problem seeing how they enter other aspects of their practice—working in teams where one is dependent on how others behave to having managers insist on changes to maximize profits or having contractors decide, midstream, as it were, to change the initial specifications, making the previous work useless.

Although one claim often made about engineering is that it is a purely quantitative discipline, it is not. Ethical considerations are at the core of engineering. They are essential to engineering practice. Remove them, and we cannot have engineering.

§2. Design Problems

A condition of our doing something moral is that we could have done otherwise. That is why we comfort toddlers who trip and fall but chastise bullies. Engineers can make a moral choice in picking a design solution because there is no single way to solve any design problem. However detailed, a statement of a design problem does not necessitate any one solution. An engineer could always have done otherwise.

We need only consider toasters and the myriad forms they can take or what might seem simpler, toothpicks. The initial statement

can be sparse: design a pick to get food and other such things out of your teeth. "Ah, a toothpick! What could be easier?" We may well wonder how there can be much room for creativity with such a design problem. How many possible different kinds of toothpicks can there be? And how could any value choices influence the answer, especially moral values?

We can see an answer to that question in this toothpick (Figure 1).

Figure 1 Japanese toothpick. © Wade L. Robison.

This is a Japanese variation of a toothpick, pointed at one end with "a series of grooves encircling the toothpick" at the other end. Once you use the toothpick, you are to break off the end at one of the grooves. You then place the end, like a Japanese pillow, on the table, with the rest of the toothpick resting on it, pointed end up. That way others can see that the toothpick has been used—a health benefit—and with the used end up so that "what had been in the diner's mouth does not touch the common table" (Figure 2).[4]

Figure 2 Japanese toothpick, used. © Wade L. Robison.

This Japanese variation solves a problem not in the design problem with which we began: What are we to do with the toothpick after it is used so that others will not use it? An easy way to transfer disease from person to person is to use a common toothpick. So ensuring that a toothpick is used but once is of some importance.

The design does waste wood, however. It will take two of them to provide two pointed ends for picking. But the value of not spreading disease was judged of more value than making full use of a piece of wood for picking. That is a moral judgment since the aim is to mitigate the harms that come from spreading germs through using someone else's toothpick. The design expresses values.

The design is also an example of another feature of design problems. As it turns out, initial statements of design problems inevitably go through a transformation as engineers work out what might and might not work. In *The Toothpick: Technology and Culture*, Henry Petroski details a variety of transformations of the design problem. That initial sparse description for a toothpick can end up looking something like this:

> These areas between adjacent contacting teeth, i.e., the interdental spaces and the interproximal tunnels, are actually like a passageway with a somewhat triangular cross-sectional shape. The base of the triangle is the gum or gingival tissue; the sides of the triangle are the proximal surfaces or side walls of the contacting teeth; and the apex of the triangle is the incisal or occusal contact area of the two adjacent teeth.
>
> Quite often the openings to these tunnels and spaces are blocked by slightly swollen or edematous gum tissue. Therefore, in order to enter the spaces or tunnels, the cleaning instrument must be sufficiently resistant to bending perpendicular to its longitudinal axis to enable it to depress or displace the gum tissue blocking the entrance or exit to the tunnels or spaces. Furthermore, the posterior interproximal tunnels are often quite tortuous, i.e., the path of the passageway is circuitous. Therefore, the instrument must be sufficiently bendable

> to follow this tortuous tunnel as it contacts the hard surfaces of the teeth and firm healthy gingival tissues. It must also have sufficient strength to dislodge food debris and loosely adherent calcular material from the walls of the tunnel or space. It must also intimately conform to the walls of the sides of the tunnels and spaces and must have sufficient abrasiveness to remove the dental plaque without injuring the tooth or gum tissues. Additionally, it must be able to fit into the usually narrow space between the anterior teeth.[5]

Who would have thought that designing a simple toothpick would require such a detailing of the work a pick would have to do? And this description does not even cover concerns about what can be readily manufactured, what can be manufactured cheaply enough to make it commercially viable, the availability of material, the cost of packing the product, and other such matters an engineer needs to consider before settling on a particular solution.

The intellectual core of engineering, and the source of the joy of success, is the working through of various possibilities and settling on a particular design that both solves the original problem and, where possible, pushes the envelope of design.

So we end up with flat toothpicks and round ones, with toothpicks pointed at on one end and toothpicks pointed at both, and even a toothpick that fits on the end of one's tongue as in Figure 3 on p. 8.

Who would have thought? Human ingenuity knows few bounds.

Design problems are subject to extension and modification, that is, as various possible solutions are considered, their strengths and weaknesses assessed, and new possible features are considered and incorporated into the original design problem. Our inability to reach certain "interdental spaces and the interproximal tunnels" easily was presumably a consideration for the odd tongue toothpick.

Its inability to reach the front of our teeth readily, and a serious concern about accidentally swallowing it as we probe and pick and push, would certainly be considerations in deciding whether to use it in place of more familiar solutions to the design problem.

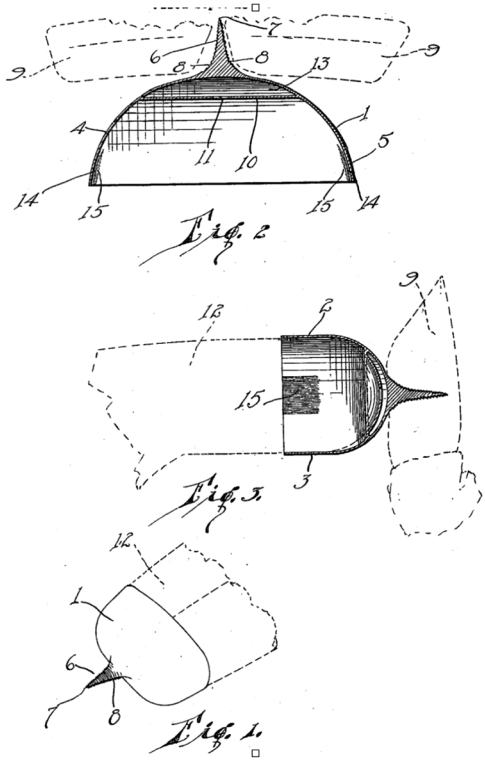


Figure 3 Toothpick for the tongue. Public Domain (Petroski, *The Toothpick*, 262. The patent was issued on August 23, 1923, to Russell Edward Lunday as Patent No. 1,465,522. Available online at https://ppubs.uspto.gov/pubwebapp/static/pages/ppubsbasic.html [accessed February 18, 2023].).

§3. Conceptual Space for Creative Solutions

What is most important for our concerns here is that though a design problem constrains potential solutions, it leaves open enormous space for creativity. Engineers are in no different position than, say, poets in this regard. A poet is constrained by prior choices, both the poet's and those of others. A poet writing "to be or not to be" had best be writing in homage of Shakespeare. The resonance of that phrase is as much a constraint on a poet as the meter chosen, the rhymes and rhythms

of various words used, the subject matter, and the point, of the poem. These are not quantitative constraints, of course—though the meter may be—but they constrain the creative genius of a poet just as much as, and no more than, a design statement and quantitative considerations constrain an engineer's choice of a design solution.

In both cases conceptual space exists for creative solutions, and engineers who think themselves immune from considerations of value because they are in a realm of crystalline quantitative clarity misdescribe the intellectual core of their discipline. It is as though they are taking the quantitative constraints on a design problem not as constraints on the problem, but as the only matter of concern. But the intellectual core of engineering—the intellectually exciting part of the discipline—is the solution to a design problem, and those solutions are not determined wholly by quantitative considerations. Design solutions do not bear the same relation to design problems that mathematical conclusions bear to their premises.

However detailed, nothing in a design statement determines any particular solution. Even a more extended statement is not going to determine a conclusion. We are not working with a mathematical problem where the premises determine the conclusion as in, to use the simplest of examples, 2 + 2 determines the conclusion, 4. Any solution will be constrained by quantitative considerations, of course. Not any object can serve as a toothpick, for instance. A dandelion stalk is straight, but too flimsy to do any picking; a titanium shaft dusted with industrial diamonds will certainly do a lot of picking, but endanger our gums and enamel. Presumably we could quantify the range of stiffness permitted, a range that would exclude the dandelion stalk as not stiff enough and the titanium shaft as too stiff. Aristotle says that "a master of any art avoids excess and deficiency,"[6] and an engineer thus has to take such matters into consideration. Yet one feature of such a design statement as that for a toothpick is how much conceptual space it leaves open for solutions. Even the simplest of objects, that is, can have many different variations, and that means that no design statement determines its solution.

What determines the solution is a creative engineer. The relation between a design problem and a solution is mediated not by deductive inferences, that is, but by a creative mind capable of imagining different ways of solving the problem and equally capable of choosing between those different solutions, weighing the advantages and disadvantages of each possible solution and making a wise choice.[7]

§4. Ethics in Engineering

As the toothpick examples illustrate, a design choice can reflect value considerations. The Japanese toothpick design ranks the healthy disposal of a toothpick above the convenience of having two pointed ends with which to work. Its obvious benefit is the assurance, if it is properly used and disposed of, that no one will pass infectious agents onto another. The design ensures that at the cost, however, of more trees cut down and of a more complex manufacturing process, taking more time and energy. Those costs are harms. They set back the interest of the manufacturers in maximizing profits by minimizing costs and the interest of those concerned with minimizing damage to the environment.

As we can see from the tongue-mounted toothpick, some design solutions are more likely to cause or risk harm than others. We should rank a tongue-mounted toothpick fairly far down the list of viable solutions. After all, swallowing a pointed implement large enough to fit on the end of your tongue and sharp enough to pick your teeth is not a trivial matter. It would be a matter of even more concern if the engineer failed to craft the details of the tongue-mounted toothpick so that it would fit tightly on a tongue and not slip off easily, and that problem is not simple either since there are, no doubt, differently sized tongues, longer and shorter, thicker and thinner, requiring smaller and larger toothpicks of varying widths. There may also be differently shaped tongues, some unable to hold onto, as it were, the variant pictured in the patent application. So choosing the tongue-mounted

toothpick as a design solution is to choose a design with many possible unnecessary harms. We are lucky other design solutions are possible.

So not all design choices are equal, obviously. Each reflects a particular configuration of values with a particular set of effects, the effects ranging from those produced by obtaining the material from which the artifact is to be manufactured, to those produced in its manufacture, to those produced in moving the artifact to market and storing it until it is sold, to those produced in disposing of or recycling or remanufacturing the artifact once its useful life is completed. Not all artifacts are susceptible to all these effects, obviously. We do not remanufacture toothpicks, for instance. But laying out the possible range of effects allows us to see that in picking any one design solution, we are not only picking out one array of values over others, and one set of effects over others, but one set of harms over others.

Ethical considerations enter into design solutions, that is, in two different ways, through what I call the argument from design and the argument from effects.

The argument from design: Whatever choice we make, we are choosing one configuration of values and effects. Design solutions *always* have ethical values. It is not possible, that is, to solve design problems without having ethical considerations enter. An engineer may not consciously decide to solve a design problem with ethical considerations in mind, but whether intentional or not, all design solutions will have ethical values because they embody some configuration of values. The Japanese toothpick illustrates that point.

The argument from effects: Ethical considerations also enter once design solutions are realized in artifacts. Those artifacts have effects. They are introduced into the causal stream of the world and are going to affect that stream just as a boulder dropped in a real stream will create new eddies and change how sediment settles. There will be effects upstream and downstream.

Downstream from an artifact's entry will be effects of all kinds. One example will make the point. Many 1990s cars used mercury in the light switches in the trunks. Mercury is a poison that can cause all sorts of

medical problems, some quite severe, and as of 2002, the Environmental Protection Agency indicated that as many as 630,000 infants had unsafe amounts of mercury in their blood. They imbibed mercury through its being disposed of improperly. When a car is crushed and smelted to make recycled steel, for instance, the mercury escapes, and if it is not to escape, the switch has to be removed, dismantled enough to get the mercury out, and then do something with it, all the time risking exposure through touch and inhalation.[8] Then there is the expense of getting rid of a toxic substance.

Problems also exist upstream since the mercury must be acquired. Someone must get the mercury, store it safely, figure out how to put it safely in the switches, all the while making sure, if possible, not to touch it, inhale it, or let any get loose in the environment.

I am making two different but interrelated points here I need to emphasize:

1. Ethical considerations enter into every solution to design problems: They enter through the design solution and through its effects, once realized in an artifact. At issue is whether engineers, in choosing a design solution, are making an ethical decision. That there is conceptual space for more than one solution means that they could have done otherwise. That is a necessary condition for an ethical decision. But, to repeat, what makes the choice ethical is that engineers are choosing one configuration of values over another and that, once realized in an artifact, any choice will have effects, some beneficial, some harmful. Engineers are choosing one among a number of configurations, and that choice is ethical because some of those choices are ethically better than others. If a choice embodies an unnecessary harm, for instance, it is unethical to choose it and ethical not to choose it. If a choice has more harms than benefits, it is unethical to choose it and ethical not to choose it.

2. We identify ethical issues by tracking harms and resolve them by eliminating or minimizing them: The easiest way to recognize that we have an ethical issue is to look to the harms. A harm raises a red flag: Is it necessary? If not, it would be unethical not to remove it. Are there

more harms than benefits with a solution? If so, it would be unethical not to toss that solution aside.

We found red flags when we assessed that toaster, the toothpicks and the light switches with mercury. We have no need for ethical theories to find and resolve ethical issues. We can simply piggyback on what engineers already do as they work through design solutions and weed out those with unnecessary harms and try to maximize the benefits for any harms that remain. It is enough to appeal to the ethical principle we all accept that we should not cause unnecessary harm.

§5. Rules of Skill

We have looked at how ethical considerations can enter design solutions, as in the Japanese toothpick with its aim of mitigating disease, and I have claimed that ethical considerations enter all design solutions because they all have some configuration of beneficial and harmful consequences once realized in an artifact. But we have not examined the space between the idea for a design solution and its realization in an artifact. Ethical considerations enter there as well.

Consider that Japanese variation of the toothpick. There is the idea and then the toothpick itself, the artifact that realizes that idea. Between the two, an engineer must lay out the original idea in detail and make sure that the idea makes practical sense. Can it be manufactured with those grooves at one end? If so, how long should it be, what circumference should it be, what should be the depth of the grooves so that the end can be readily broken off when the toothpick has been used and yet not break off when being used, and so on? Engineers are not finished, that is, after coming up with an idea for a design solution. There is also the execution of the design.

What is needed to go from the idea of a design solution to its realization is a mastery of the rules of skill someone must learn to become an engineer. An engineer is no different from, say, an oil painter in executing an idea. A great artist has great ideas executed

in a stunning way. These two features of an artist—the capacity for creative ideas and the ability to execute those ideas—are distinct. One can exist without the other. Someone may have wonderful ideas, but lousy technique. Someone may have great technique, but lousy ideas. Neither can be a great artist. A poorly written book with a great plot is still poorly written, and a well-written book with a poor plot still has a poor plot. Just so, an engineer may be superb at the detail work, but not creative enough to imagine good design solutions or fail at the detailed work needed to turn great design solutions into anything. Just as an artist needs to master delicate brush strokes and subtle tonal features, among other things, an engineer needs to master a wide range and variety of rules of skill.

Such rules tell us how to do something. They are conditionals of the form, "If you want to achieve so-and-so, you must do such-and-such." We have been learning them since we were children—how to open a door, turn on a faucet, or unlatch a hatch to get at the cookies. We are now masters of many such rules. They underpin our lives. Having mastered some skills so well they have become habitual, we do not have to think about how to open a door, walk along a sidewalk filled with other pedestrians, or use a cell phone.

Rules of skill tell us how we ought to achieve some end. For many rules of skill, that "ought" is a practical matter. To make a cake, we need to follow a recipe. That tells us the ingredients, how much of each is needed, the order in which they are to be mixed together, and so on. We will have a palatable cake only by luck if we fail to follow the instructions. But the rules of skill professionals must learn to become adept at their professions also have ethical weight. In being taught a profession, students are being taught its core ethical values through the rules of skill they must learn.

The rules of skill of a profession are its tools of the trade, as it were, and using them properly is not just a practical matter, what is needed to accomplish some end, but an ethical matter as well, what they ought to do as professionals. The rules obviously differ from profession to profession. Learning how to maneuver a colonoscope through the

twists and turns of a colon is difficult and dangerous, with the risk of breaking through the colon wall. Luckily only physicians specializing in such matters need to master that skill. Learning how to saw with a Japanese saw is not for everyone either. You pull rather than push as with a Western saw. Lawyers need to learn how to read legal documents carefully and must learn legal terms like motion in limine, cestui que trust, and feoffment. They do not need to learn anything about Japanese saws any more than internists specializing in colonoscopies need to learn about legal terms.

So when engineers are calculating stresses, they have an ethical obligation to calculate them according to the rules for such calculations. Otherwise they will get it wrong, and the result will be harm of some sort, a bridge weaker than it ought to be, a beam not strong enough. Although it may not seem like it, those quantitative skills engineers learn, the ones that make it seem as though engineering is a wholly quantitative discipline, have ethical weight.

When we teach children that 3 + 4 = 7, we are teaching them what they ought to get in adding three and four, and we correct them when they make a mistake. That is, 3 + 4 = 7 is normative. The norm is not ethical, but it can become ethical in a context where harm can occur, and that is any context in which there are effects from its use. Splitting the remaining cookies fairly? If there are two children and four cookies, simple division tells them that each is to get two cookies. That is what they ought to get in dividing four by two, and that would be fair as well.

It may seem odd for calculations to have ethical weight, but in learning quantitative skills, as well as all the others they must have mastered to become engineers, they are learning what they ought to do as engineers. Just as we will not succeed in baking a palatable cake if we do not follow the recipe, we will not succeed in building a trustworthy bridge if we do not use the relevant rules of skill and use them competently. We would end up with a practical failure, a structure that would not pass inspection and could not be used as a bridge. But it would also be an ethical failure if only because of the harms we have created.

When engineers make errors in calculations, that is, the mistakes can cause great harm, and that is why the quantitative skills they learn tell them not just how they ought to proceed in calculations to get things right, but how they are ethically required to proceed. Getting the calculations right is the right thing to do, ethically as well as mathematically, and getting them wrong? That is an ethical failure as well as a mathematical mistake. Calculations have ethical weight for the same reason artifacts have ethical weight. They have real effects, some beneficial, some harmful, and a failure to do the calculations or do them correctly avoids harm only by luck.

It is all too easy to find examples of such failures. The collapse of a walkway spanning the lobby in the Hyatt Regency Hotel in Kansas City in 1981 provides us with an example of both. The engineers failed to calculate correctly how to support the walkway given its original design when it was to hang with another by single rods. Their calculations resulted in its supporting only 60 percent of the load required by the city. Then they failed to calculate at all the effects of a change in the construction when the single rod was replaced with two, one rod holding up two walkways. When the walkway collapsed, 114 were killed and over 200 injured.[9] Calculations have ethical consequences.

Rules of skill define a profession's ethical core: physicians cure patients, accountants analyze financial information, and architects design buildings. When individuals become professionals, they enter a role with a set of moral relations that define the profession, and when they practice their professions, they are to act morally in realizing their roles in those moral relations.

> **1. Role morality:** In becoming an engineer, a person takes on a set of role-specific relations regarding the practice of engineering—for example, ensuring that calculations are made correctly.

The role carries with it ethical obligations. It is no small matter that calculations be made correctly. Engineers are not allowed to guess how thick a road surface must be to withstand the expected traffic. They are required to calculate what is required so as to avoid a road's breaking

up, accidents, the expense of tearing up and then rebuilding the road surface to the proper specifications, and so on.

Among the moral relations an engineer takes on in becoming an engineer, one set has special status, and deserves separate consideration, because the set defines the intellectual core of engineer, capturing engineering's creative center:

> **2. Design solutions:** The intellectual core of engineering is solving design problems, and because at a minimum, ethically, an engineer ought to cause no unnecessary harm, solving design problems requires ethical considerations if only to avoid a solution which causes unnecessary harm.

An engineer cannot avoid the role-specific ethical relations of being an engineer and the ethical relations connected with solving design problems. A person cannot be an engineer without acting on these ethical relations. They are internal to the profession.

§6. Concluding Remarks

To repeat what should now be obvious, the range of possible solutions for any particular design problem is large, and in choosing among the possible solutions, engineers must make value choices. Sometimes cost is of more value than aesthetic appeal; sometimes effectiveness wins over cost; sometimes reliability wins over ease of manufacture. In making these value choices, an engineer is necessarily making moral choices because, as we saw, whatever design solution an engineer proposes, its realization in an artifact will have its effects in the world, being more or less beneficial, causing more or less harm—through obtaining the material chosen to make the artifact, through manufacturing the artifact, through moving the artifact from where it is manufactured to where it is to be sold, through the use of the artifact after it is sold, through the disposal of the artifact after its useful life is over. It is thus always appropriate to ask, "Could a different design solution have produced less harm?"

That question presupposes that we have moved from a design solution to its realization in an artifact, and that movement requires that an engineer properly execute the details of the solution. A mistaken calculation, a misjudgment about the kind of material to be used, a failure to see how a change at one stage reverberates through the rest of the design—all these and more are problems that can occur because an engineer has failed to follow through on a design solution to make its realization possible.

From choosing a design solution to executing its details to determining what configuration of benefits and harms it produces, engineers are engaged in an ethical enterprise. Engineers may well blanche at the idea. For, they may think, if the design solution depends, even in a small part, on ethical considerations, something qualitative, vague, subjective, and contentious will have found its way into that pristine quantitative realm they think is the heart of engineering.

That concern is understandable, but rests upon a mistaken contrast between engineering and ethics and also upon mistaken understandings of both engineering and ethics. On a standard view, engineering rests in a purely quantitative world completely separated from the messy world of our lives where we use what engineers create. Engineering has nothing to do with that, the standard view goes. On this view, ethical issues arise about what people do with what engineers create, but engineers are not responsible for the use others make of what they do. The engineers who design a car are not responsible if a driver runs down a pedestrian any more than the engineers who design a pen are responsible for a child poking out an eye, or so the standard view would have it.

But as we have seen, ethical considerations are integral to engineering because they are integral to its intellectual core, solving design problems. An engineer's decision about what to do to solve a particular design problem does not rest wholly on the crystalline clarity that quantification provides, but on ethical judgments—whether engineers realize it or not or, indeed, whether engineers intend to be ethical or not. The engineer's intent is as ethically irrelevant as the intent of any

professional acting professionally: the daydreaming dentist who drills through one of my teeth is acting unprofessionally, and unethically, despite having no intent to cause me harm. The role-specific ethical relations of the engineer come with the territory independently of whether the engineer wishes to take them on or is even aware of them.

I am not suggesting that ethics ought to be introduced into engineering. I am pointing out that it is already integral to engineering. Being ethical does not require that engineers do anything more than what they already generally do. They solve design problems and work to squeeze out unnecessary harms and produce more benefits than harms in what they design. By asking engineers to look upon their standard practice through an ethical lens, I am just describing what engineers already do. That description does not change what they do or distort it in any way, but brings to light a feature of what they do that has been bleached out by a mistaken understanding of what they do and opens up the possibility of a more expansive understanding of their role as engineers.

2

Analyzing Accidents

§1. What Can Go Wrong

Accidents tell us how to do things better—provided, of course, that we find out what went wrong. When we have an auto accident, for instance, the problem may lie with something the driver did or neglected to do, with some unusual feature of the situation, with the vehicle, the artifact in question that is, or with some combination of these three variables. These variables—the operator, the circumstances, and the artifact in question—must be examined in any accident.[1] A driver may have hit another car because the brakes failed, or the driver was distracted and failed to stop, or black ice made the brakes useless. Whether it is the artifact, the operator, or the circumstances will make all the difference in trying to prevent a repetition.

1. Operator: We cry "Operator error!" if the operator

- did not have the intellectual ability to learn what needs to be done,
- had the intellectual ability, but was not well trained, or
- was well trained, but was off in some way (e.g., inattentive because texting).

Each of these three possibilities covers a wide variety of kinds of failure. We can fail to be off in some way, for instance, for many different kinds of reasons.

Think of people driving. They may fail to avoid another car because they are distracted (by a bird just missing a windshield, for example), engaged in something else that requires too much of their attention (talking on a cell phone, turning to chastise a child in the back seat,

fiddling with a phone to text message), drunk or high and so unable to concentrate fully on what they ought to be doing, angry and so thinking about something completely different from what they should be thinking about, and so on. They may be preoccupied—as were the NWA pilots who flew 500 miles without radio contact and overflew their landing site in Minneapolis by 150 miles.[2] They may be asleep—as perhaps were the pilots on a Go! Airlines flight that at 21,000 feet flew 15 miles out to sea past Hilo, its landing site, before turning around and landing.[3]

The phrase "off in some way" is meant to cover the variety of ways in which we can fail to engage fully in what we are doing even though we have the intellectual ability to have learned what needs to be done and have been well trained. Even the most intelligent and well-trained people can still be distracted or find their minds wandering or, as it were, inoperative at crucial times. In investigating an accident, we must come to grips with all these possibilities, a difficult matter in any event, but especially if the operator has died or was plagued with more than one problem.

We are all familiar with being on top of our game, in the zone where we can do no wrong. Either we have experienced it or read about or saw someone for whom everything went right. We may wish that experience were not so rare as we sometimes stumble our way through life, but the point of the phrase "off in some way" is to capture all the ways in which we can stumble. There seems to be no general term available to cover all the ways in which we can fail. "Unmotivated," "distracted," "out of it," "inattentive," "absent minded," "drugged," "sleepy"—the list is long and obviously covers a great many different ways in which we can fail to be fully engaged with what we are doing. I mean to cover all those possibilities with that phrase "off in some way."

Poor training? Training can go wrong for any of a number of reasons. It is difficult to train us out of a habit. Especially in times of stress, the habitual reaction is likely to take over. It is easier to train us to follow simple instructions than complicated ones. This is particularly true for instructions that tell us to do one thing most of the time but

something else in one particular circumstance. Even when instructions seem easy, they may be misunderstood. Everything that can go wrong with communication can go wrong with training, and that covers such a variety of failures it is not possible to guard ourselves against them all. A set of instructions always has a design, and the design itself can be better or worse, helping or hindering understanding.

So in investigating an accident, we must examine exactly how the operator was trained. When an accident is in the offing, was the training good enough that the operator will know what needs to be done? In investigating the crash of TransAsia Airways Flight 235, investigators heard the captain say on the flight recorder when one of its two engines flamed out, "Wow, pulled back the wrong side throttle"—an odd comment given that he thereby condemned the plane to a crash that would kill him and forty-three others. The plane was designed to fly on one engine, but the captain had killed the working engine. It turns out that the pilot had initially failed that part of the training where pilots have to respond to an engine loss, showing "insufficient knowledge leading to hesitations in 'both EEC (electronic engine controls) failure' and 'engine failure after V1' situation" where "Vi is the speed beyond which takeoff can no longer be safely aborted." He later passed, but we will never know whether he was not sufficiently trained or, trained well enough, was off in some way. We have here a good example of how difficult it can sometimes be to sort out exactly what goes wrong, but nothing was wrong with the plane that a well-trained and attentive pilot could not have handled without crashing it.[4]

The aim in assessing the quality of training is to determine if the training needs to be modified in any way. Those who pass through training ideally ought not to fail what they were trained to do when the expertise they supposedly gained is needed. In some cases, obviously, the training itself can contribute to the accident and so needs to be corrected. We might even find that the training was counterproductive.

Buddy Holly died in 1959 in a plane crash that killed all aboard. The pilot was relying on instruments because visibility was limited. He had had "a little bit of instrument training" and so was "not totally

unprepared," according to Bruce Landsberg, executive director of the Aircraft Owners and Pilots Association. But, he says, "The instrument that was installed on the aircraft read differently than the instrument he had trained on. So if the aircraft was making a right turn, it would appear on this instrument to be making a left turn—which makes it very difficult to sort things out quickly when you're close to the ground and in moderate turbulence." The crash occurred because the pilot was "not able to keep the airplane upright by reference to the flight instruments." Here the training was counterproductive, teaching the pilot to do exactly the opposite of what he would need to do to keep the plane upright.[5]

Not intellectually capable of understanding what needs to be done? We know that even the brightest people can get things wrong—locking ourselves out of our car, for instance. Scratch a genius, and you will undoubtedly get a story of a silly blunder. So even with a brilliant operator, doing something wrong may have been a factor in an accident. Just so, we know that even those not so gifted intellectually may have excellent common sense and moments of genius. So when investigating an accident, we cannot draw any specific inference simply from a person's general intellectual level. We will need to look out for aberrant behavior.

One difficulty in investigating an accident is that behavior can be so outside the bounds of what we would consider normal that the possibility will not have occurred to us. "How could anyone make *that* kind of mistake?!" This is a source of delight—and horror—at the Darwin Awards: How could anyone have thought to play Russian Roulette with an automatic?[6]

These three possibilities—intelligence, training, and being on—work in tandem. If we determine that an operator has the intellectual ability to learn what needs to be done and is well-trained, we focus on the operator's condition to see if something about that was causally relevant. Distracted? Tired? Depressed? If we determine that the operator is intelligent and is fully engaged, we hone in on the training. Did the operator have enough hours using that machine? Can we be

confident the training was sufficient? Was the training course thorough? Was the operator hurried through it or given time to understand fully the various kinds of problems that can arise using that machine? If we determine that the operator was well-trained and fully engaged, we hone in on the operator's intellectual ability. With all the will in the world, people without the intellectual ability to learn what needs to be done are not likely to make the most of their training and are more likely to make mistakes. Is that what we have here?

Making a judgment about why we have done something is never easy. Even the most commonplace of actions may have multiple motivations. We eat that particular dinner because we enjoy it, because we are hungry, because it is healthy, because someone made it for us and we cannot well refuse to eat without being impolite, and so on. Determining which motivation, or how many, were causally significant can be difficult for the person eating the dinner, let alone for someone else observing the behavior. It is harder still when we must make a judgment about whether an operator in an accident is somehow responsible and if so, how. We not only have to look at many different possible motivations, but at the person's general intelligence and preparedness, and we have to do so after the fact, not knowing for sure that we have been able to take into account everything that is relevant. A combination of the relevant factors may be responsible, and so the possibilities are many. The best we can often hope for is to identify the most likely possibilities and try to protect ourselves in the future against these possibilities.

2. Circumstances: In any event, whatever we may discover regarding the operator, we need to examine the situation to determine if some feature of the conditions in which the accident occurred contributed to the problem. What about the pilots for Go!Airlines? Were they trying to avoid a storm? What about an auto accident or, more dramatic, a multiple-car accident on the interstate? Did someone slow down suddenly to answer a cell phone? Could drivers not see because it was so foggy? We must examine all the features of the situation to try to isolate what it was about the situation that was crucial.

How different the situation is from what we designate as "normal" will play in our assessment of what needs changing. Reflectors on the side of the road or on the median strip would help when the fog is light, but perhaps make no difference when the fog is heavy. Even the most intelligent, well-trained, and highly motivated individual, working with an artifact designed to be as foolproof as possible, can have problems that cause an accident if the situation is sufficiently abnormal. Even a captain well-practiced in docking a ferry can have an accident when the waves have been churned by hurricane winds. Even a driver used to ice and snow can be surprised by a patch of black ice. The conditions in which an accident occurred can be a crucial causal factor.

Assessing how much the circumstances contributed to an accident can be as difficult a matter as determining what circumstances were critical—even when no issue about the operator or the artifact arises to complicate any determination further. Hitting a patch of black ice does not always lead to an accident, for instance. Sometimes we can drive out of the skid it produces, but a failure to do that does not necessarily mean that we are somehow at fault. Some small variable in the circumstances—the patch of black ice running longer in the direction in which we are supposed to turn in such situations—can make even what seems the best response to the problem a mistake.

3. Artifact: Yet even with the worst of conditions, and even with what may seem operator error, we need to examine the artifact in question to determine how that may have contributed to the problem. If something about the artifact in question was a contributing factor, we should know that sooner rather than later, and waiting to determine whether the circumstances or the operator or some combination was completely at fault means delaying any fix to the artifact and risking yet another accident. So we should ask, when looking into the circumstances and any difficulties with the operator, "Was there something about the artifact that contributed to or caused the accident?" As we well know, there often is.

It is one of life's common annoyances in this technological age that the artifacts of our lives provoke, encourage, or permit errors and so create

problems for us. Cell phones that appear to operate one way but operate in another, shower handles that do not turn the way they appear to—the list is long, and it takes only a query of friends and acquaintances to elicit all sorts of examples of common objects so designed as to cause accidents and provoke errors on our part—even in the most pristine of circumstances when we are motivated and think ourselves intelligent enough and well enough trained to use what is causing us problems.

Life's accidents do not come neatly divided into those caused by the operator, those caused by circumstances, and those caused by the artifact, but we can understand how these three variables can each contribute to an accident and in some clear cases can separate out one variable as the most causally relevant for an accident.

For instance, when we hear that a small child has driven a car into some sort of obstacle, we can presume the child is highly motivated but obviously untrained. "Operator error!" is the appropriate response. The circumstances do not matter, and the car is not to be faulted. The problem lies wholly with the operator in such a case, and clearly some operators can cause grievous harm—as with the train operator in California who sent twenty-nine text messages while on the job, including one twenty-two seconds before the train he was operating ran head-on into a Union Pacific train,[7] with twenty-five lives lost. He was so distracted that he ran right through a red light and as the chair of the National Transportation Board said, he "really did not have his head in the game."[8]

Even an operator with "his head in the game," intelligent and well-trained, may be unable to avoid an accident if the artifact fails. We know this because we all know that shovels break, brakes fail, and electrical systems short out. The world is full of artifacts that fail, putting the best of operators, in the best of circumstances, in an accident. The artifact may have a link that finally gives out or a fault that finally shows itself when subjected to a particular stress. Things wear out, as we all know. Even something that has worked well for a very long time may suddenly fail because of age or because we put stress on it that is just different enough to cause it to break. We know that even the best of us, in the

best of circumstances, may be unable to avoid an accident even with well-designed and properly used artifacts. The artifact can hardly be held at fault in such situations any more than we can.

But we also know that we can have faults in the original design solution or faults introduced as a design solution makes its way to realization in an artifact. A change during the construction of the Citicorp Center in how the wind braces were fastened is a classic example of how a design solution failed realization. The architects had specified that the wind braces be welded, but they were bolted instead. That change made no difference to how the building would withstand winds perpendicular to the walls, the only measure required by the New York City building code. But the change put the building at risk of failure if winds of no more than 80 miles per hour hit the walls at a 45° angle.[9]

There is no doubt many mishaps that come about because of factors introduced as a design solution is being realized, and many of those may be avoided by changes in the design itself. A design solution that requires immense care in its realization is more likely to lead to a failure than one that does not.[10]

The design for the original space shuttle is a case in point. When shuttle rockets blast off, they produce a twang, a vibration that moves the entire shuttle as it gathers strength to lift off. If the shuttle rocket were a single long cylinder, the twang would not harm it, but if the shuttle rocket is composed of segments, stacked on top of each other, the twang creates a separation between the top of one shuttle segment and the bottom of the next one. Hot gases may then blow through that separation. The only way to prevent the disaster that blow through could cause was to line each segment with O-rings resilient enough to spring back into place almost instantaneously after ignition. But the O-rings had to be put in place with incredible care since even the tiniest mistake—a hair falling upon an O-ring—could cause a catastrophic failure. It is no doubt true that many design solutions must incorporate features that require such incredible care in its realization in an artifact, but this solution was not the only possible solution and courted failure when others would have been less likely to fail.

So one feature of design solutions we should be wary of is complexity. The more complex a design solution, the more ways in which problems can arise. Simplicity in a design is an important value for a number of reasons, but one main reason is that it lessens the chance of problems occurring because of the interplay of an artifact's parts. That is not to say that a simple design cannot cause problems.

The design may be so poor that it permits or encourages errors. It may be so badly designed as to provoke errors for the most intelligent and well-trained individuals who "has his head in the game" even in the most pristine of circumstances. If the circumstances are the most favorable and the operator satisfies all the features needed for operating the artifact—intelligent, well-trained, and in the zone—and does not make a mistake, then anything that goes wrong can reasonably be attributed to the artifact itself. Something about it must be the cause of what goes wrong for the best of operators, fully engaged in operating the artifact, in the best of circumstances for using it.

The harms produced by such designs can vary considerably—from minor annoyances to catastrophic disasters. It is a minor annoyance to find ourselves unable to wash our hands at a sink operated by putting our hands under the faucet. When nothing happens, we cannot tell whether we have somehow not quite got our hands in the right place, whether we are supposed to move our hands rather than merely put them in the right place, whether the mechanism is broken, whether the sink appears to operate when our hands are placed in it but actually operates some other way, by pushing a pedal, for instance. With nothing to tell us when the mechanism is broken, we can only move to another sink and try again or leave. That sort of problem is minor, but can be more than minor, and immensely annoying, when we have just changed our baby's diaper, for instance.

It is far more than an annoyance for an artifact's design to increase the likelihood of death. We shall examine several cases where a failure to think through a design solution led to catastrophic failures—from crushing a patient to death on an X-ray table to airplane clashes that killed hundreds. We shall find in such cases that the artifact is at fault

and that the engineers who designed the artifact failed to design it properly.

We shall concentrate first on artifacts that are so badly designed that they provoke even the most intelligent and well-trained operators to make mistakes even when in the zone. By examining such badly flawed design solutions, what I call error-provocative designs, we shall be able to see clearly how engineers can do harm, even without intending it. We will be able to see clearly how ethics enters into engineering practice itself. If even the best operators are led to make fatal mistakes because of an engineering design solution, the design solution is at fault.

3

Error-Provocative Designs

§1. Artifacts Can Cause Accidents

We know that sometimes the fault is ours when things do not work the way we expect. We push the wrong button on the TV remote because we are not paying attention or lock ourselves out of our car because distracted. We can hardly blame the remote or our keys for our mistakes, but sometimes the fault does lie in the artifact—buttons placed so close together we have difficulty pushing one without pushing another or a computer keyboard so designed that "the keys get stuck, start repeating or fail to work entirely."[1] As we all know, technological artifacts—television remotes, cell phones—are among modern life's most ubiquitous little annoyances.

There is no designing any artifact to prevent a person from making a mistake when the person lacks the intellectual ability to operate it, has not learned how to operate it, or is distracted or inattentive. But surely, if the person is intelligent, well-trained, and paying careful attention, we think, the person is not going to make a mistake. But some design solutions are unique in that high intelligence, the best training, and the highest of motivations make no difference. The artifact does not just permit those who use it to make mistakes or even encourage them to make mistakes. Something about the design provokes them into making mistakes. We can even imagine that the worse of error-provocative designs makes use of a person's intelligence, training, and motivation to provoke errors. The more intelligent and more highly trained and motivated an individual is, the more likely that individual is to make a mistake. The design would make thinking about it and past training

and even high motivation impediments to using it without error. Dumb luck would be an asset in using such artifacts.

How can an artifact cause an accident? A toaster just sits there. It is not going to cause anything at all. The idea that an artifact could provoke someone into making a mistake may seem so counterintuitive that it is worthwhile spending some time illustrating it. To do that, I am going to use a standard problem given engineering students: What is the best way to arrange the burners and knobs on a stove top? Solving that problem will also illustrate just how embedded ethical considerations are in engineering.

§2. Stove Tops: How to Confuse a Cook

We are presented with the following:

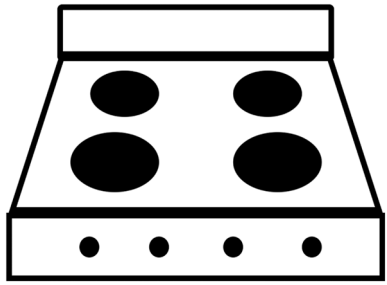


Figure 4 Stovetop with burners in a row. © Wade L. Robison.

We have four knobs to control four burners: Which is to control which?

If we were asked to design a stove top, we would need to consider how the burners are to be positioned so a cook can put cookware on and off each burner without serious risk of touching anything hot on an adjacent burner. We would also need to determine whether the burners should vary in size, and if so, how, so as to fit the various sizes

of preexisting cookware sufficiently well to provide enough heat to the cookware without wasting any. The question we are being asked has been pulled out of a question with more complexities, that is. So it ought to be easier to answer.

Unfortunately, it is anything but. The arrangement in Figure 4 makes it anything but obvious to someone using the stove which knob controls which burner for the simple reason that with four burners and four knobs, and each knob controlling one burner, there are twenty-four different ways we could arrange the knobs and burners. The first knob could control any of four burners, the second any of three, the third either of the two remaining, and the last knob the remaining burner. So which of the twenty-four configurations is best? Would any of them make it obvious to a cook which knob controls which burner?

The way this problem is presented already incorporates a significant decision, having four knobs for four burners rather than three or five, say. It may seem odd to suggest that a knob might control two different burners, but having a single knob or switch do multiple tasks is not that unusual. The light switch on some Dodge Caravans, to mention just one example, turns on the lights by being turned to the right, clockwise, and turns on the running lights by being pulled out. Nothing about the knob tells a driver that it serves the second function as well as the first. A driver needs to read the instruction manual to discover that the single switch serves a double function. So, for the stove, there could also be two controls for a single burner, a switch to turn it on and a knob to regulate how hot it gets, for instance.

When we consider that there are twenty-four possible ways of arranging the knobs and burners, we can imagine how confusing it would be to have one knob control two or more burners. Such an arrangement would really confuse a cook new to the stove, but limiting ourselves to four knobs and four burners still leaves us with way too many possible combinations. For what reason are we to choose one combination over any other? It would seem that any arrangement would be completely random and so leave us, and a cook, at a loss as to how to start.

Suppose we chose a combination at random. We can imagine how confusing a random combination would be by supposing ourselves standing in front of the stove, trying to figure out which knob turns on the burner that has the pan with our eggs to scramble. First one on the left? Maybe. Maybe not. Second one on the left? If the distribution is random, the only way to answer the question of which knob controls which burner is to experiment and see what happens.

To understand how disconcerting a random distribution could be we need only imagine many artifacts in our lives with randomized controls. The lights and switches in a house could be so arranged that the switches do not correlate with lights nearby but with some distant lights in some distant rooms. Or perhaps sometimes when we turn on the light switch in our car the lights go on and sometimes the windshield wipers, and sometimes the windshield wiper control opens a window and sometimes turns the radio on. That we have patterns of correlated controls is not a trivial matter but makes it possible for us to have habits of behavior and so live a life without having constantly to learn anew everything we normally do.

The only way to proceed when things are arranged randomly is to experiment. We try a knob to see what burner it controls, but if the arrangement is random, nothing about the information gained in that attempt gives us a clue about the rest of the arrangement. We would have to try three knobs at least to figure out which knobs controlled which burners. We are not likely to remember the arrangement the next time we use the stove, and we cannot carry the information we have gained from this stove top to any other stove top. Approaching another stove would be like coming into a foreign country where the road signs are in a language we do not understand. In fact, the oddity of any random arrangement ought to make us leery of the next stove top we encounter working in the same way.

We would approach stoves with the same hesitation we would have if we had to experiment each time we came to a closed door. Turn the knob to the right? To the left? Pull? Push? If each door required

an experiment to open, we would have turned what was a habitual response into a problem we must solve anew at every door.

§3. The Ethics of Confusing a Cook

It would be irritating, at the least, if we had to approach doors not knowing how to open them, and dangerous if we were trying to escape a fire, for instance. The same is true of stove tops. Cooks have enough to do without having to stop and think about how to lower the heat for one dish or raise it for another. We not only risk overcooked meals, but at some point someone will likely leave a burner on, being called away by a phone call, perhaps, without realizing that a right-hand burner was left on and a left-hand one was turned off. We need only imagine something overflowing from a cooking pan and the cook being unable, under the stress, to find the right knob to turn the burner off and so starting a fire—just like the person who "irreparably damaged" the "internal mechanism" of that toaster by using the lever when the bread started to burn.

The potential for harm, and particularly the significant harm that could be caused by a fire, raises an ethical red flag. The problem of designing stove tops is presented as an exercise in ergonomics: how can we design something so as to minimize human error, maximize production, enhance safety, and reduce fatigue, among other things? But it is also an exercise in making ethical decisions. We interact with artifacts, and the aim of the exercise is to emphasize that design solutions need to map onto our natural ways of behaving.

The solutions have the form of conditionals: "If I place the knobs here and the burners there, then someone using the stove top will see which knob controls which burner." That conditional is a factual claim, a claim about how a particular placement will affect any user, and so it may seem to have no ethical weight at all. After all, an ethical judgment is normative. It says that we ought or ought not to do something.

But when we make a judgment about how best to lay out the knobs and burners in a stove top, we are already making a normative judgment. The use of "how best" brings out its normative character. We value ease of use, and so even at that level, we are making a judgment that the design *ought* to be such-and-such if the stove top is to be easy to use. But we value ease of use not just in and of itself, but so those using it will not be misled about how to turn off a burner where a mistake could cause a fire. So when we choose one design for the knobs and burners over another, we are making an ethical judgment.

The problem exemplifies how ethical considerations enter into design solutions without any requirement that we think about ethics—about Kant, or Mill, or Aristotle or any of the complications of ethical theories. In solving such a design problem, we are making factual claims—"Putting the knobs this way will make it easier for a cook to see which knob controls which burner than putting them that way"—that carry an ethical punch so that the factual claim embodies an ethical judgment as well. It is not necessary, that is, that engineering students be introduced to ethical theories in order to be ethically engaged in their discipline. They are already ethically engaged.

It was this point I was making in the first chapter when I said that I was not trying to introduce ethics into engineering, but pointing out that ethical considerations are already integral to the solution of the design problems that form the intellectual heart of engineering. I am simply describing what engineers already do so as to make it clear that they are in fact making ethical decisions. As I said, that new description makes no change to what they do and does not distort it in any way, but it does bring to light a feature of what they do that has been bleached out, as I have said, by a mistaken understanding of what they do. That we can find ethical considerations entering into even the simplest of design problems, the ones first-year students get to introduce them to ergonomics, is, on my view, only to be expected.

But we still have to figure out which of twenty-four different arrangements we ought to choose. We now know better the significance

of any choice. It is not just to make matters easy for cooks, but to prevent harm. It is not just a lesson in ergonomics, but in making ethical decisions.

§4. Simplifying the Problem

A classic study by Chapanis and Lindenbaum of "preferred locations of controls for burners on stove tops" begins with the stove top already configured so that knobs on the left control burners on the left and knobs on the right control burners on the right. The problem has been greatly simplified, and the study thus examined not twenty-four, but "four alternative layouts of the burners."[2]

We have a much simpler problem, but it is still a problem. Let us call the burners left front (LF), left back (LB), right front (RF), and right back (RB). We could have the left knobs of each pair control the front burners and the right knobs control the back—in the order LF, LB, RF, and RB. Unfortunately, that is only one of four different possible arrangements if the left-hand knobs control the left-hand burners and the right-hand knobs the right-hand burners. The knobs could be arranged so that the outer two knobs control the back burners and the middle two control the front ones—LB, LF, RF, and RB. Or we could have the outer knobs control the front burners and the inner two knobs control the back ones—LF, LB, RB, and RF. Or we could have the left knobs of each pair control the back burners and the right knobs control the front ones—LB, LF, RB, and RF.

None of these arrangements is any more natural than any other. One solution is to label the knobs. The directions on my current stove top spell out the words in capital letters: LEFT FRONT, and they are placed next to a set of four small circles, to represent the burners, with the circle for the relevant burner filled in. The stove top thus has written directions, with a pictorial representation—two different ways to instruct users. The directions are immediately in front of the knobs, which are set at a slant to the stove top, and so whenever I reach to turn on a knob, I can see the directions—although they are too small

to read except by getting much closer than is needed to use the knob. That is a somewhat effective solution to the problem, but it is a solution necessitated by an arrangement of burners and knobs that calls for directions because nothing about the arrangement itself gives someone using the stove top any directions.

Needing directions is a sign that a design solution is not optimal. If there were no standard way of turning a door knob, we could put a label above each knob. "Knob turns to the right!" or "Knob turns to the left!" We would then have to note the note, take it in, and respond accordingly. What we now have as a simple habit for opening doors would become a more complicated procedure, slowing us down and forcing us to read the instructions rather than just opening them.

We have a rule of skill for opening door knobs that is so obvious and natural it can easily become habitual, and we need to figure out how to arrange the knobs and burners so that the proper way of using them leaps out at a user, making it all but impossible to make a mistake. We need a rule of skill like the one we have for door knobs.

So how can we place the burners and knobs to preclude mistakes? The usual solution is to follow the lead of Chapanis and Lindenbaum to have the knobs on the left control the left-hand burners and those on the right the right-hand burners and then shift the back burners in one direction, shift the front burners in the other, and line up the knobs with the burners so that, as in Figure 5, just looking at the knobs will tell you which knob turns on which burner.

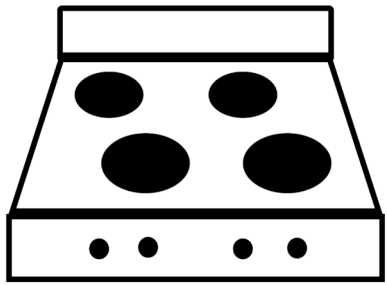


Figure 5 Stovetop with burners and knobs lined up. © Wade L. Robison.

The order of the knobs corresponds with the order of the burners. The knob on the far left appears almost directly in front of the left back burner, the second knob from the left appears directly in front of the left front burner, and so on down the line.

The visual clues we get from the arrangement match the actual arrangement of knobs and burners, and we do not need any additional information to get things right. So there is no need for warning devices of the sort I find on my stovetop. No symbols on the knobs are necessary. Anyone new to the stove can see how it operates, and anyone who has used the stove will know instantly how to use it again and any similar stove. This is an elegantly simple solution to the problem with which we began.

§5. What Is Natural

What leaps out at us when we propose a solution to a design problem may not leap out for everyone. So we should test any potential design solution to determine whether it is idiosyncratic. What may be natural and obvious to some regarding any particular design may not be natural or obvious to some others. What is natural for a right-hander need not be at all natural for a left-hander, for instance. Just think of how door knobs turn. A clockwise motion is natural for a right-hander but requires an effort for a left-hander.

When we look at the simple solution proposed for the stove top the pattern we see is identical to the actual relation of the knobs and burners. That is what makes that design solution natural and obvious. What we see provides us with a visual version of the relevant rule of skill. To turn any burner on or control it once on, use the knob directly in front of it.

That is a rule that is easy to understand and is effectively repeated visually each time we approach the stove top. As with our rule of skill for opening doors, it can readily become habitual, saving us from

having to stop and think before turning a burner on or off. Even those who are blind can readily learn the pattern and use the stove.

Our brains are wired to perceive patterns, and any design solution that runs against the grain of our brain is not going to be optimal for us to use the resulting artifact. That fact about our psychology is one reason engineers need more than mathematics and physics to succeed at the core intellectual endeavor of engineering, the solution to design problems. They need to consider the features of those who are going to use whatever artifact results from their solution. That includes our physical as well as psychological characteristics. It does no good to design an artifact that requires us to hold it with one hand while somehow simultaneously pushing two buttons farther apart than our fingers can spread.

An appeal to what is natural can run counter to another variable engineers need to take into account. Those are the habits we have come to have because of some previous solution to a particular problem. The keyboard arrangement on our computer seems natural—as anyone who has tried to use a different keyboard configuration can attest—but that is only because we are all used to the now-standard keyboard arrangement, the QWERTY. That keyboard arrangement was not designed for ease of use, but, in the original typewriters, for preventing the metal keys from hitting each other and sticking. The design was meant to slow us down to allow time for the metal keys to sink back out of action.

An engineer needs to consider the history of technology and, in particular, previous solutions, if any, to the design problem under consideration. We are creatures of habit, and so we come to new artifacts with embedded habits that we will use if triggered by the artifact in question. There is little sense in designing an artifact, no matter how elegant the design solution, that can only be operated by doing what runs against the grain of what habits have led us to expect. That does not mean being tied down to an old way of doing things. It does mean taking those ways into account in the transition to something new.

The transition from door latches to door knobs in the 1820s and 1830s was proceeded in some cases by an intermediate stage where the door still latched, and the latch was still operated by pulling up on the lever that came through the door, but the latch was underneath a knob. Instead of grabbing hold of a handle and pushing down on a lever, we reach for a knob and pull up on the lever. The knob does not turn on this transitional door handle, but is screwed onto the door and is used only as a handle to pull open the door. I do not provide this as a good example of taking into consideration people's habits about unlatching a door while introducing a new mode of entry, door knobs, but this combination of latch and knob illustrates an attempt to accommodate past practice.

We will need to look at how a problem has been handled historically so as to get a sense of what people are used to and so now find natural. We will need to determine if the past solution has been biased by, say, being arranged to make things easy for right-handers—a value judgment that favors the majority, right-handers, at the expense of the minority. We will need to look at what others find natural and obvious, comparing their responses to ours and making sure that our own responses, however natural and obvious they seem to us, are not idiosyncratic. The list of ways we could go wrong is long, and so our enquiry is not as simple as may seem.

§6. Examples of Error-Provocative Designs

Any of the random arrangements could readily cause a cook to err, by mischance, but to illustrate error-provocative designs, we need examples that cause even the most intelligent, well-trained, and highly motivated cook to make a mistake. We can find one in a variant of a design which seems as elegant and simple as the one we have settled on. We arrange the burners in a circle with the back burners pushed toward each other and the front burners pushed away. The knobs are then arranged in a similar manner so that they line up with the burners. Such an arrangement would look like this (Figure 6.).

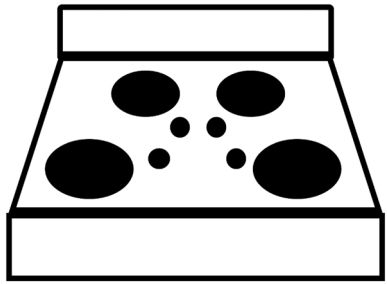


Figure 6 A different stovetop configuration. © Wade L. Robison.

With the back burners set in the center, closer together, the front burners off to either side in the front, and the knobs set in the same arrangement, we have a solution that appears foolproof. Again, the visual clues we get match the actual arrangement for turning on the burners. Or so we would think when we saw such a stove.

I have a friend whose very expensive stove top is arranged just this way. I was watching him cook dinner one evening. He had lobster and angel hair pasta in separate pots on the back burners. I was sitting on a stool, drinking wine. The stove top is gas, and I could see the flames from where I sat. So when the timer rang for the angel hair pasta—90 seconds—I saw him turn off the burner for the lobster, leaving the pasta boiling away. I pointed it out. He said, "I'm so stupid! I do this all the time!" I went over to look, curious about what could have gone wrong. How could he have turned off the wrong burner when it is so obvious which is which?

Since the pasta was on the right-back burner, all my friend had to do was to turn the back knob on the right. To turn off the burner with the lobster pot by mistake, my friend, being right-handed, would have had to reach across that knob and turn the back burner knob on the left. Surely that awkward motion would warn him he was about to make a mistake, and yet he complained about doing it "all the time." It is unlikely that anyone would make that awkward motion time and again without realizing it.

When I asked him to show me what he had done, he pointed to the knob on the right—the one that appears to operate the right-hand back burner, the one with the pasta pot on it. "I turned that knob," he said. Now I really was puzzled. Why did that knob not control the right-back burner? What was going on here?

After some investigation, we discovered that the back two burner knobs had been reversed, as in Figure 7. The stove top worked like this:

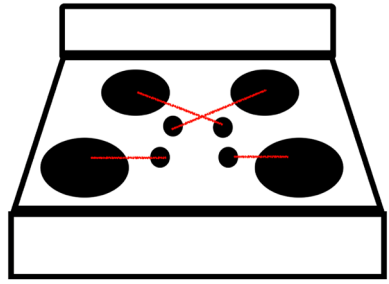


Figure 7 How the stovetop in Figure 6 really works. © Wade L. Robison.

No wonder my friend made mistakes all the time! He was getting a clear signal from the position of the knobs about what he ought to be doing, and he did it. But he was getting the wrong information. He had originally turned off what *appeared* to be the knob for the burner for the pasta and left on what *appeared* to be the knob for the burner with the lobster, but since the knobs were reversed, he left on the burner for the pasta and turned off the burner for the lobster.

This is a paradigmatic example of an error-provocative design. No matter how intelligent and well-trained and on his game my friend was, the design would provoke him into making a mistake. It was a form of entrapment. He was perfectly innocent, but the faulty stove design made him make a mistake, and instead of blaming the stove top, he blamed himself.

Operator error! We often see this response in regard to major accidents. A major meltdown averted at a nuclear plant! The cause of the problem? Operator error. A train wreck in New Jersey. The cause of the problem? The engineer failed to slow down when the signal told

him he should. Operator error. An airplane accident in Colombia? Operator error. When Ford vehicles with automatic transmissions "popped out of park and into reverse," Ford's reaction, and the reaction of the National Highway Traffic Safety Administration (NHTSA), was to blame the driver for not putting the "car fully in park." Toyota and NHTSA made the same move of blaming the operator with their responses to problems Toyota drivers had with accelerators revving up. The problem, they claimed, was that drivers were pushing the floor mats up under the accelerator pedal.

The executive director of the Center for Auto Safety, Clarence Ditlow, said:

> Both Toyota's and Ford's reaction is to blame the issue on driver error. In the '80s, they said the driver didn't put the car fully in park—they left it in neutral or what have you. In Toyota's case, it's the floor mat's fault. The manufacturers want to avoid a costly engineering recall. For Toyota, any recall that goes beyond the floor mat will be very expensive.

Toyota's problems with accelerators revving up date back at least to 2003, and NHTSA's response then was that the problem was "pedal misapplication . . . blaming the drivers for hitting the gas instead of the brakes."[3] "Operator error!"[4]

My friend's initial reaction, however, was not just that he had made a mistake, but that the whole thing was his fault. As he said, "I'm so stupid!" So one ironic consequence of his stove top's error-provocative design was that he blamed himself for making such a "stupid" mistake. Instead of wondering what it was about the stove top that kept making him make a mistake, he simply threw up his hands and confessed to his stupidity. The irony, of course, is that he blamed himself for what the stove top's layout made it all too obvious that he ought to do.

The fault in my friend's kitchen was not with my friend, that is, but with the design of the stove top. Perhaps my friend should have learned by this time, overcoming each time he used the stove the information he received visually from its layout and remembering that the knobs do not work the way they appear to work. But however one parcels out

responsibility here, the stove top ought to get a large share. It looks to be designed to avoid the very problem its arrangement of burners and knobs create! No wonder he kept forgetting.

My friend's problem with his stove top hit a responsive chord with me. Every time I went to visit my parents, I made a mistake with the stove. Their stove top was laid out so that the burners in the back were shifted to the left with the burners in the front shifted to the right and the knobs lined up precisely with the burners as we saw in Figure 5—the elegantly simple solution to the stove top problem.

My parents had no coffee maker, and so I would have to heat water for my coffee on the stove. The mistake I made was to put the water for coffee on the back left burner and then turn on the wrong burner. Because the stove was electric and the burners took a while to heat up, I failed to see that I had turned on the wrong burner. If I was lucky, I would walk into the kitchen after showering and find the left front burner red hot while the pot for the coffee sat, still cold, in the back. If I was unlucky, my mother would have walked in before me. The water would now be heating up because she had turned off the burner in front and turned on the burner in the back, but she would give me that look only mothers can give: How did you ever survive this long?

What was the problem? Why did I keep making the same mistake? I finally figured it out. Figure 8 shows how the knobs turn on the burners.

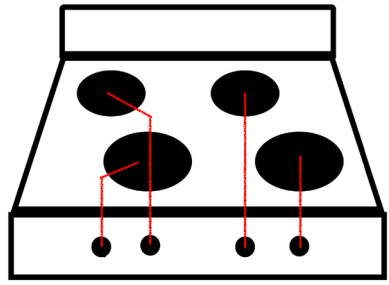


Figure 8 My parents' stovetop, how it really worked. © Wade L. Robison.

I got mixed signals from the stove's design and from the placement of the knobs for the right-hand burners. The offset pattern of the burners

suggests a corresponding order to the control buttons—LB, LF, RB, and RF. But the left-hand knob turned on the front burner, not the back. It did exactly the opposite of what the offset pattern of burners led me to expect and exactly the opposite of what using the right-hand knobs would lead me to expect. It is not that the design is neutral between competing interpretations and that I made the wrong interpretation. The design provoked a mistake. It provoked me to do exactly the opposite of what I ought to do to heat up the coffee water just as the design of my friend's stove top provoked him to do the opposite of what he should have been doing.

My mother was so used to using the stove top that when I remarked on how the control knobs were in the wrong place, she failed to see a problem. There were no instructions on her stove top, but she had so trained herself that using the correct set of knobs had apparently become second nature to her, a habit so deeply embedded that she did not even realize it was a habit and that others, unused to the stove top, might have a problem. She thought the problem was with me, not with the stovetop—"Operator error!"

The most likely explanation for the problem with her stovetop was that the wires connecting the burners to the knobs were switched when installed. The problem with my friend's stovetop is harder to explain. The usual method of control for the gas to a burner is via the knob. A small gas pipe comes in at the knob, and turning the knob opens that pipe and directs the gas down a metal tube to the particular burner controlled by that knob. The lengths of the metal tubes coming from the knobs to the burners will vary in length depending on the distances from the knobs to the burners. To reverse the knob controls for a gas stove top thus requires switching the metal tubes.

We can understand how someone might mix up the wires on my mother's stove top. A worker might well reverse the connections. Her stovetop arrangement may have been a one-off wiring mistake. But the tubes cannot be switched in that way. Had the tubes for the back burners been made just long enough to reach the knobs the design indicates they were meant to reach, they could not be switched accidentally or

intentionally. They would be too short to be connected to the wrong knobs.

What could have happened? Some misstep may have occurred between the execution of the details of the design and its final realization in a stove top. A worker might have run out of shorter tubes, and, as luck would have it, the tubes for the front burners were just the right length to fit the back burners if the knobs were switched. The tubes would have to crisscross each other, and so it ought to be fairly obvious to any inspector, or any worker, that the wrong length tubes had been used. Another possibility is that the manufacturer judged it less expensive to make all the tubes the same length, and so ruin the elegant design solution, than to make tubes of different lengths to save the design.

In any event, whatever the cause of the switch, something trumped the value of ensuring that whoever uses the stove is not misled into making a mistake and thus causing harm. As we know, some resulting harms may not be great. Those who use the stove top will either habituate themselves to turning the correct knobs or, like my friend, continually berate themselves for being "stupid." But the design clearly provokes confusion, irritation, and errors. The errors in question that I have mentioned—overcooked pasta, my own embarrassment in front of my mother—hardly rise to the level of ethical concern, but it is not hard to imagine someone accidentally causing a fire by turning on the wrong burner without realizing it or allowing a fire to spread when a pot flares up by not being able to find quickly the proper knob to turn off the burner. Design errors can be fatal.

§7. Ethics and Design

One advantage of working through in such detail the design problem for a stove top is that misaligned knobs and burners jump out from the visual images. It is difficult not to feel sympathy for my friend with his expensive but flawed stove top. When you look at the arrangement of knobs and burners, it is difficult to imagine how anything could

be made more clear. We see the arrangement and, without any more thought, reach for what for all the world looks to be the correct knob.

The point of the arrangement is to bypass any need for thought about which knob controls which burner. A cook can concentrate on cooking, not on how to turn the burners on and off. My friend was "told" by the arrangement which knob controls which burner and, having done what he was told, without thinking about it, discovered that he turned off the wrong burner. He was caught up short, as we all would be, and wondered what had gone wrong. "How could I have misread what the arrangement of the stove top told me? Stupid me!" But as the visual images make clear, the stove top is at fault.

That stove top would provoke errors in anyone who used it, no matter how intelligent, highly trained, and "in the game." Cooks trained to the eccentricities of this stove top might, like my mother, become so habituated to its odd arrangement of knobs and burners as not to make the mistakes my friend made, and yet might still find themselves sometimes wondering if they had made a mistake, the power of what they would see putting a question to what they had become habituated into doing. Such can be the power of that arrangement on our actions. It is sad, and ironic, that the visual arrangement of the knobs and burners on my friend's stove top appears to have been designed to avoid just the sort of error the actual arrangement caused.

So one thing we have gained from working through the stove top problem are paradigmatic examples of error-provocative designs. It is sometimes said that once we get a word or phrase for something, we can see instances all around us. This is true of the concept of an error-provocative design. It is easy to find examples. For instance, in the public library in the town in which I live, the knob on the door to the men's room on the second floor is on the right-hand side of the door, but opens the door only if turned to the left, counterclockwise. That is such an unexpected way for a knob to turn that the door at one time had a handwritten sign on it that said, "Knob turns to the LEFT!!!" I assume the sign was put there by a librarian who was tired of telling men, "No, the bathroom is *not* locked. Just turn the knob the other

way!" A knob that must be turned in an unexpected way to open the door is a real novelty and sure to provoke errors.

The men who pestered the librarian were all presumably relatively intelligent. They were in the library after all. We can also presume that they were well-trained in opening doors. All of us have been opening doors, or trying to, at least since we first began to walk. And they were motivated. It is a bathroom door. It is a measure of how unusual it is to have a door knob that opens a door by being turned in an unexpected way that so many men went to the librarian complaining that the door was locked.

You can put yourself in their place by imagining a door handle rather than a knob. Suppose that the door handle is on the right-hand side of the door. Put your left hand out to open the imaginary door by grabbing the handle and turning. What did you do? You reached your hand out, with your knuckles on top, and turned the handle down, counterclockwise, ready to pull it open so you can walk through. But suppose the door opens only by being turned upward, clockwise. Try making that motion with your hand—still with your left hand reaching across in front of you and in the same position, knuckles up. It is difficult to open a door that way even if you knew that was how it opens. If you did open it that way, your hand would pull your arm and shoulder out of position to get through the open door without grabbing it with your other hand. That is one reason you would assume the door was locked.

Putting such handles on fire exits would be catastrophic in an emergency. People would run to open the doors and think them locked when they were unable to turn the handles down. Such a handle would be as catastrophic as having an emergency door that opened in rather than out. Both are error-provocative and will produce catastrophic results in such a context.

It is wrong to put individuals at an unnecessary risk of harm, and so any company that installed handles in that manner, and any person who supervised the installation, would be morally culpable. The problem would probably lie in the installation, not in the design of the handle itself. So we would not fault the designer unless something

about the design itself made installing it in the wrong way necessary or likely.

This is not to suggest that the problems with my mother's stove top and my friend's are the fault of any engineer choosing a bad design. As suggested, the problems probably came about because of bad wiring and bad judgment on the part of someone other than the engineers. These examples are meant to illustrate the concept of an error-provocative design—just how a design can provoke errors on the part of even the best of operators—as well as suggest that we might be better served by having the designing engineers follow through on how their design solution is realized in an artifact.

In any event, once the concept of an error-provocative design is clear, with such easily remembered examples, we can proceed to consider other examples where it is not so obvious that anyone was involved other than the engineer solving a design problem. Indeed, that the problems with the stovetops my friend and mother had could have been introduced through design choices by engineers is all we need to make the point that ethical considerations are integral to the intellectual core of engineering.

§8. Summary

Our examination of the stove top problem and the toothpick has told us a great deal about solving design problems:

a. **Design problems underdetermine solutions.** There are many ways to design toothpicks just as there are many ways to design stove tops. An engineering design problem is not like a math problem in which the premises determine the conclusion. It is constrained by quantitative considerations, but since those constraints do not determine one particular conclusion, there is conceptual space for the imagination and creativity of engineers. They need more than the skill to calculate, that is. In the best of cases, with a brilliantly elegant solution to a design problem,

engineers deserve praise for a creative imagination, a difficult talent to realize.

b. **A design problem involves a complex of decisions in which any one decision can both constrain and open up new possibilities.** Once we choose to put burners in sets of two to the right and left, we constrain ourselves to only two different ways of arranging the knobs on either side—unless, that is, we really want to produce an error-provocative design. Similarly, if we choose a design solution for a toothpick that emphasizes breaking it after its use so that it cannot be used again, something like the Japanese solution seems mandated. We have not emphasized the cascading effect of decisions, but it is worth noting if only because we can find ourselves caught in a cascade, trying to figure a way out of the problem we have now come to have, without realizing that a prior decision that could be revisited created the cascade now causing us problems. Decisions have their effects, and one effect is that we end up thinking in a certain way because a decision closes off some possible solutions so we no longer consider them and opens up new possibilities and problems that also constrain our thought. We need to remember, in working through a design problem, the decisions we make as we go along so that we can revisit and reconsider them should we run into unforeseen problems that we cannot readily solve. We may have led ourselves down a garden path, without realizing it, and so become lost without realizing we need to retrace our steps.

c. **The choices we make in picking design problems reflect values.** How design problems are chosen, how they are ranked as worth solving—these are value-laden enterprises, as value-laden as the ways in which a design problem is conceived and stated. In concentrating upon design solutions, we are leaving to one side questions about how we fasten on design problems themselves, but how we choose design problems provides a rich source of issues for anyone concerned to see how ethical considerations permeate the core of engineering.

d. **The choices we make in solving a design problem reflect values.** They can reflect the worst of values, we know, because we know engineers can solve a design problem in a way that provokes errors. The conceptual space left open by a design problem means that no engineer is compelled to choose the worst configuration of values. It is a mistake, that is, to think that the intellectual core of engineering is wholly consumed by quantitative considerations. Whatever design an engineer chooses will reflect a set of values and be ranked the best solution to further that set, the worst, or somewhere in between—brilliant, mediocre, acceptable, or some other less than sterling choice. A recent solution to the problem of opening cans has produced a can opener that leaves no sharp edges, cutting through the can below the edge at the top and bending back the edges on the side and the top as it cuts through. Safety is a value, and emphasizing it in regard to this artifact has fundamentally altered the way a can opener works. The design solution that led to this can opener reflects a value choice and, in this case, a good one that trumped whatever other considerations might have mitigated against it.
e. **Some of these values are ethical values.** As we saw, ethical considerations enter engineering by the very act of engineers choosing a design solution, and they enter as well when engineers take the idea they have for solving a design problem and execute it. Putting a design solution to paper or computer in the clearest possible way is a separate task from solving the design problem and one equally prone to errors. It is an engineer's responsibility to make absolutely clear to whoever is to take the design solution and produce an artifact what needs to be done. Engineers need not be driven by ethical considerations in making design choices or in executing them for those choices to embody ethical values. They need not make explicit, even to themselves, what ethical values they are achieving through their particular design choice or even whether they are achieving any ethical values at all. However they arrive at a choice, that is, whether they choose an

error-provocative solution or one that solves the original design problem elegantly, without unnecessary harms, that choice reflects ethical values for at least three different reasons:

i. Although the design choice itself reflects ethical values, the values can perhaps best be seen once the design is realized in an artifact that embodies them. Its creation will cause more or less harm, depending, for instance, upon how it is manufactured and how the resources necessary for its creation are produced. We have not raised these issues in any of the examples we have examined so far, but the point should be obvious. Choosing a design that uses fewer resources or fewer harmful resources than some other design is not an ethically neutral decision. Choosing a design that can be realized in an artifact with less expenditure of energy than another design is not ethically neutral. Choosing a design that allows for remanufacturing and/or recycling is not ethically neutral. The manufacturer of my friend's stove top may well have decided that it was more cost-efficient to make a single-length tube. That was not an ethically neutral decision. The presumption should be that all decisions about a design carry implications that are ethically loaded.
ii. Once a design solution has been chosen, an engineer is to make use of the rules of skill essential to the profession to execute the solution in such a way as to be clear—as foolproof as possible—so that the solution can find its way to become an artifact. Engineers have a moral obligation, at a minimum, to use the rules of skill of the profession competently, and a failure to use them properly is a moral failure.
iii. Once the artifact is introduced into the world, it will have causal effects. These effects are likely to be a mix of good, bad, and indifferent, and if the total set of effects is more harmful than it need be, it would have been morally preferable to have chosen a different design solution. We need only think of such examples as the ignition switch on some GM cars. Their introduction into

the world had effects. Some were minor—such as drivers being urged to remove everything from the key chain except the car key to keep the weight low and minimize the risk of the switch disengaging while driving, shutting off the engine and the airbags. And some effects were major—such as the loss of those lives that need not have been lost had the proper part been used.[5] Introducing any artifact into the world has effects, that is, and any unnecessary harms among them is an ethical fault.

f. **What an engineer chooses as a design solution will reflect on the engineer's character and moral values.** Though we have not raised this issue in the discussion so far, we need only go through the possibilities to see how a choice reflects back on the engineer. Since we are free to choose as our design solution whatever among the range of possibilities we wish, we would have a difficult time explaining why, among all the possible design solutions, we chose the worst. What would we possibly say? "Why should I care?" Or, "What's it to you?" If we did not choose the best design solution, we would have to say something that makes our attitude and level of competence clear: "I'm satisfied with being mediocre." We would, that is, have a difficult time explaining why we chose a design solution that, once realized in an artifact, caused harm when it did not have to, polluted when it did not have to, frustrated users when it did not have to, and so on. So we can look at a design solution and reverse engineer, as it were, the decisions that led to it, and if a pattern exists, the relevant features of the character that produced it.

In examining design solutions, we have uncovered not only that engineers ought to avoid error-provocative designs, but also that they ought to strive for the best design solution. Engineers are no different than anyone else trying to solve a design problem. A poet makes design choices in crafting a poem, and the aim is the same: solve the design problem in the best way possible. Just as engineers ought to avoid such mistakes as producing an error-provocative design, a poet ought not

choose what undercuts rather than furthers the point of the poem. Just as poets ought not to settle for mediocre choices, but strive for just the right word or phrase or rhythm, so engineers ought not to settle for mediocre design solutions, but strive for the best.

In the case of the stove top, ethics enters as soon as an engineer considers whether the right-hand knobs should control the right-hand burners and the left-hand knobs should control the left-hand burners. Indeed, ethics enters even if an engineer does not consider the issue, but simply assumes an answer. Ethics enters, that is, whether the arrangement of knobs to burners is the result of intentional action or not. It is not the intention that causes harm, but the arrangement, and it is not the engineer's intention that matters, but the failure to try to minimize the harms that will come from using an error-provocative design.

Those harms can be far worse than overcooked spaghetti. Error-provocative designs can be catastrophic, causing a great loss of life. We will examine how by examining a plane crash in Colombia and the crashes of two Boeing 737 MAX's.

4

Airliner Crashes

§1. The Colombia Crash

An airliner crash in Colombia in 1996 killed "all but 4 of the 163 people on board." The plane was to land at Cali, but when the pilot turned on the autopilot by typing in "R" for the navigational beacon at Cali, the plane turned slowly, heading toward Bogota, more than 90 degrees and 100 miles away from Cali. The plane crashed into the side of a mountain before the pilots were able to "figure out why the plane had turned."[1] In fact, for some time, they did not even realize it was turning. They had given up control of the plane to the autopilot and were taking care of other matters.

Nothing suggested that the weather was a factor—no wind shear, no turbulence. So we may put to one side the circumstances as providing any significant contributing factor to the disaster. The problem is going to lie with the pilot, or with something about the airplane, or some combination of those two. What went wrong?

Each navigational beacon has a name, and the software in the autopilot uses the first letter of that name to identify the beacon. The Cali beacon is called Rozo, and so the software identifies it by the letter "R." The captain typed in "R" for the Rozo beacon. "When that letter was entered into the flight management computer, the screen responded with a list of six navigational beacons."[2] The norm is that the computer ranks beacons by distance, with the closest at the top of the list. The autopilot is programmed to fasten onto the top-ranked beacon and guide the plane in without any further action by the pilot. The pilot thought he was done when he typed in "R." He expected the autopilot to take over and land the plane at Cali.

In the list of beacons, the autopilot provided was Romeo, the beacon at Bogota. The "names for the beacons at Cali and Bogota both start with R," and Romeo was one of the six closest navigational beacons. The norm is that beacons are listed with the nearest at the top and the farthest away at the bottom, but when a pilot types in "R," the norm no longer holds. The autopilot will head the plane toward Bogota, the capital of Colombia.[3]

The pilot expected the norm and so apparently did not notice that the autopilot's list had Romeo at the top rather than Rozo. They were jolted alert by the air traffic controller telling them "to take a more direct approach to the Cali airport." Since the plane was on autopilot and only very slowly turning away from Cali, they were at a loss to figure out what was going on. The expectation that the autopilot was landing the plane at Cali apparently got in the way of their realizing that the plane was turning. They could not figure out what was going wrong and "spent 66 seconds trying to follow [the] air traffic controller's orders" before slamming into the side of a mountain.[4]

§2. Operator Error?

The headline in the *New York Times* story said, "Pilot's Wrong Keystroke Led To Crash, Airline Says." The airline attributed the accident, and thus the death of 159 people, to the pilot's error in locking the autopilot onto the wrong navigational beacon.

"Operator error!" is a typical corporate response to such accidents. If the operator made a mistake, it is not the fault of the company involved—except for having hired someone who could make such a mistake. A company has an interest in trying to immunize itself from any fault and so minimize its legal liabilities. If the operator is responsible, the artifact is not and the company's liability is significantly lessened. We should therefore look with suspicion when an accident occurs and the relevant corporate entity says, "Operator error!" We should look with suspicion

on the airline's claim in any event. In this case we have another reason for suspicion.

Attributing the crash to pilot error or saying the pilot made the "wrong keystroke," as the headline has it, hardly begins to describe what went wrong. There are only three ways in which the pilot could have done that.

If he had typed "T" by accident, the key to the right of "R," we would fault him for being careless. It is easy to hit the wrong key on a keyboard. Anyone who has used a computer has made this kind of mistake. But the pilot did not do that. He typed "R."

The pilot might have gotten the name of the beacon wrong, thinking it was "Tozo" instead of "Rozo" and so typing "T." He would then have made the wrong keystroke, but we would fault his knowledge, not his lack of care. But he did not have the wrong name. He typed "R," knowing that "Rozo" was the name of the beacon for Cali.

One other possibility is that he intentionally typed "R" knowing that the autopilot would pick Bogota so that the plane would turn toward Bogota and crash. He would have made the right keystroke, given an intent to crash the plane. Yet nothing about his behavior before or after the autopilot kicked in indicates such an intention. He seemed as surprised as anyone by the discovery that the plane was not heading in to land at Cali.

So saying that the pilot's wrong keystroke led to the crash is, to put it mildly, just plain false. Whether the airline knew it was false is another question, and we shall not pursue it. For our purposes, it is enough to know that the airline had an interest in blaming the pilot and so trying to immunize itself from any fault—and so minimize its legal costs should it be sued.

§3. Predictable Problems

So if it is not accurate to say that the pilot made the wrong keystroke, what are we to say? We can see that this is not a paradigmatic example

where one of the three variables—the circumstances, the operator, the artifact—is completely at fault. The circumstances we may put to one side, but in assessing this accident, we are burdened by not being sure what the pilot knew and did not know and so cannot be sure he does not bear some responsibility.

There are only two options:

i. Either he did not know that the computer was programmed to rank Bogota first when "R" was typed, or
ii. He knew that typing "R" would rank Bogota first even though typing "R" so close to Cali would have brought Cali to the top of the ranking had the program worked the way it usually does, by ranking beacons by distance.

If (i) is true, then more training might have helped or a reminder could have been pasted on the computer keyboard so as to be immediately visible to anyone about to key in the letter "R."

If (ii) is true, then he must have forgotten, or punched in "R" without thinking about it (as when we lock a car door by habit even as we see the keys inside), or been distracted, or whatever.

In either event, whether he knew about the oddity in the software or not, that oddity creates a problem that we can predict with a great deal of certainty would lead to what happened. Instructions provide us with a rule, a procedure to be followed to achieve a goal. The software for the computer is a set of instructions, a rule, for the computer to follow: if the operator types in "X," then such-and-such will happen. We have all been following instructions since we were little children. "Brush your teeth before you go to bed!" "Put on your clothes before you come down for breakfast!" So we know what it is like to follow instructions. We also know, however, that if the instructions are complicated by an exception, we are likely to forget. The rule that we should put our clothes on before we come down for breakfast except for the third Wednesday of the month is going to guarantee, given our nature, that we are going to forget some third Wednesday or other.

The rule we would have to teach a pilot about this autopilot software has just this form, with just that guarantee. The instructions would have to read something like this:

> Type in the first letter of the beacon for the airport at which you wish to land except that, when the letter is "R" the autopilot will direct the plane to Bogota, and if you do not wish to land at Bogota, you must type, well, something else to land at the airport you wish to land at, but we are not sure what, or you must land the plane on your own, without using the autopilot.

Pilots are as prone to make mistakes in times of tension and stress as the rest of us. Given the necessity of instructions like that, we know that some pilot, somewhere, distracted or forgetful or whatever, will type "R" without realizing or remembering that the autopilot will direct the plane toward Bogota. We need only suppose a pilot who never flies into Bogota and has never previously flown into any airport whose beacon begins with the letter "R." A pilot could be experienced with that software, that is, and still make the mistake. And a pilot not experienced in that software, but in software in similar planes, would have no reason to expect an exception to the norm. It is not likely that even the most experienced pilot would have expected the computer to choose a beacon 100 miles away when the norm is that beacons are ranked by distance, with the closest at the top of the list, and he knew that was the norm. So the software will need a way to countermand a choice—as we all know from having clicked "Send" on an email before we were truly ready to send it.

It should be noted that there is at least one alternative explanation for the accident, but one in which the onboard computer also plays a pivotal role. According to this possibility, the crew was told by the Cali controller "to report when it had passed over a radio navigation beacon called Tulua." It took the captain 90 seconds to look up the code for Tulua and "program it into the" computer, but "by the time he had done that, the plane had already crossed the beacon." Typing in the code for Tulua told the autopilot to find the beacon and pass over it, and so, on

this alternative explanation, the plane slowly began to turn around. The captain and the First Officer did not notice the turn for some time, and when they did, they turned to another computer "that directs the plane's autopilot through 'heading select' dials. They dialed in the heading they thought they were supposed to be flying," and the plane turned to the right, all the while continuing its descent. The captain took over the plane when "the ground proximity warning blared" two minutes later, but was unable to prevent the crash.[5]

§4. Guarding Against Error

We know that complicated instructions with exceptions will lead us to make mistakes. We will forget the exception or forget when it is to occur, and we can try to counter our inevitable failures in only two ways:

1. We could create a warning sign, something on the autopilot. We could put a physical block on the letter "R"—a cage that needs to be removed before "R" can be typed. That way the pilot has to do more than one thing to type "R" and so would know that something was out of the ordinary.

Such warning devices are standard when a bad design is likely to mislead an operator, but they leave the problem untouched. Playing around with various devices to warn a pilot is like a physician prescribing various medications for the symptoms of a fatal disease without bothering to find the cause. The disease continues along, untouched by the medications; just so, the bad design continues along. Just as it is only a matter of time before the disease kills the patient, so it is only a matter of time before someone misses the warning signs and precipitates a disaster. Warning devices are not the most effective way to handle a badly designed artifact.

2. We could redesign the software so that no warning device is needed. The beacons could always appear with the closest airport

> first. They could also be named so that the same letter is not used twice.

If the software had been designed so that the norm was that the closest beacon was always chosen, the crash would not have occurred—or would not have occurred because of the fault with the software. The feature that precipitated the crash was either chosen or introduced through some fluke in the program the engineers failed to catch. In either event, they are responsible—either for intentionally introducing a feature that increased the likelihood of a catastrophic crash or for designing software that permitted that feature and then not catching the oddity.

We cannot be sure we can exonerate the pilots completely. We do not know if they were aware of the oddity in the software. If they were, they should have anticipated just the sort of problem that arose. So the bottom line is that we cannot say with certainty that the artifact is completely at fault.

§5. Boeing's Failures

It is an ethical fault if you fail to take responsibility for harm you cause and ethically worse to deflect responsibility by blaming someone else. Corporations that cry "Operator error!" after an incident involving their products are guilty of this double ethical fault when their products caused or contributed to the harms. Worse, in deflecting blame, they risk more harms by not examining and fixing what it was about their products that contributed to the harms.

Both Boeing and the Federal Aviation Administration (FAA) blamed the pilots when two 737 MAX's crashed:

> On October 29, 2018, Lion Air Flight 610 (JT610), a Boeing 737 MAX, crashed shortly after takeoff in Jakarta, Indonesia. All 189 people on board perished. On March 10, 2019, Ethiopian Airlines Flight 302 (ET302), also a Boeing 737 MAX, crashed shortly after takeoff in Addis Ababa, Ethiopia, killing all 157 people on board.[6]

The FAA's Associate Administrator for Aviation Safety, Ali Bahrami, called the Lion Air Crash "a 'one off' event and attributed it to poor pilot performance."[7] Boeing held that the problem was what every pilot is trained to spot and resolve, what is called a stabilizer runaway. Boeing issued a bulletin shortly after the crash effectively reminding airlines that the pilots "should have known how to handle the emergency."[8] They just needed to follow the existing procedures, Boeing wrote, by switching off the stabilizer switch, something they could have done within four seconds.[9]

Less than five months later, the Ethiopian 737 MAX crashed. The acting FAA administrator, Daniel Elwell, blamed the pilots, saying they "didn't adhere to the emergency [advisory] we put out" and failed to use the "basic knowledge" all pilots learn so that the problem they faced, and the remedy, would have been "immediately recognizable" to them.[10] As later analysis showed, however, the copilot did follow the standard procedure, turning off the stabilizer switch,[11] but the pilots were unable to right the plane and another 157 people were killed.

Deflecting blame after the Lion Air Crash made that "one off" event the first in a troubling pattern, with both flights having stabilizer runaway problems. Boeing and the FAA needed to look at the 737 MAX operating system rather than blaming the pilots as though they were wholly responsible.

We will see that it would have been exceedingly difficult for any pilot to prevent those crashes, given what Boeing engineers had done with the operating system of the plane, what Boeing failed to tell the pilots and the airlines, and how the FAA failed its regulatory responsibilities.

§6. Instability in the MAX

The 737 MAX was a response to a fuel-efficient Airbus that was eating into Boeing's profits. The new Airbus was saving airlines 15 percent on fuel costs, a significant savings that none of Boeing's existing planes could match.[12] The savings came from larger and thus more efficient engines.

Bigger really is better—at least when it comes to fuel efficiency: "the larger and hotter you can make any heat engine, the more efficient it becomes."[13]

The MAX was to have significantly larger and more fuel-efficient engines than any previous iteration of the 737.

Since proven and available are also better, Boeing put the engines on the 737 body to get the plane out quickly, to avoid the costs of designing and developing a new body for the large engines,[14] and to bypass the need for the millions it would cost airlines to train pilots for a new plane.[15] The 737 MAX was to fly like its predecessor, the 737 NG.

But the engines were so much larger than those on any previous 737 that "they needed to be mounted higher and farther forward on the wings to provide adequate ground clearance." Because they were "well in front of the wing," they changed the plane's "centerline of thrust," increasing the chances of the plane's stalling as pilots accelerated.[16]

We have all stuck our hands out the window of a moving vehicle. We can keep it flat and ride the wind, as it were, without much of a problem, but if we angle our palm up, we increase the surface hitting the wind. At a high enough angle, our hand will tend to fly backward and fall. That is a stall.[17]

Attacking the wind head-on provides as smooth a ride for the plane as it does for our hand when we keep it flat, but when the angle of the wings is too high to allow the air stream to slip smoothly over them, providing lift, the air stream breaks up, creating a dragging effect on the plane. Just as with our hands, increasing what is called the angle of attack creates a tendency to stall (Figure 9).[18]

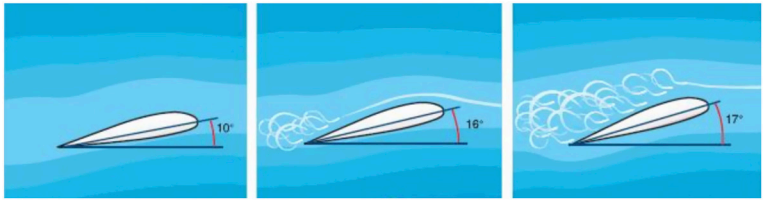


Figure 9 Stalling angle of attack. Public Domain. https://commons.wikimedia.org/wiki/File:AFH_Figure_4-2.JPG.

That tendency is exacerbated by the housings for the engines for the MAX. They work as wings and produce "lift . . . well ahead of the wing's center of lift." They thus push the nose even higher. This causes the plane already "at a high angle of attack to go to a *higher* angle of attack."[19]

Boeing discovered in wind-tunnel tests that the plane did not handle smoothly when in "an extreme maneuver, a banked spiral called a wind-up turn that brings a plane through a stall."[20] That problem of instability needed to be fixed before the plane could be certified.

§7. Engineering Stability

Commercial jets are "nose-heavy," and moving the engines forward on the wings for the 737 MAX not only produced a new "centerline of thrust," but also made the nose heavier still. The fix lies in the "horizontal stabilizers on the tail." They can counteract the tendency of the nose to dip. At the same time, the only way to prevent stalling is to lower the nose, and the "horizontal stabilizers on the tail are needed" for that. So the stabilizers are essential both to prevent stalling and falling. They stabilize the plane. The consequence is that "with a fully loaded aircraft, loss of tail control virtually guarantees that the plane will crash."[21]

Boeing engineers attempted to solve the instability problem caused by the heavy nose by taking another item off the shelf. It is software, called MCAS, for Maneuvering Characteristics Augmentation System. It forces the nose down when it senses a stall.

The software was designed to "activate only when the plane was making sharp turns at high speeds"[22] and "only if two distinct sensors indicated such an extreme maneuver: a high angle of attack and a high . . . acceleration in a vertical direction."[23] But those two conditions were improbable in an airliner. The rarity of a sharp turn at high speed meant that "pilots weren't ever likely to encounter situations where the new

anti-stall system kicked in" so "[t]hey would never see the system in action."[24] That led Boeing, through the 737 Chief Technical Officer, Mark Forkner, to ask the FAA if it could delete reference to MCAS from any training information since MCAS would only kick in "way outside the normal operating envelope."[25]

The FAA agreed—to Boeing's relief because that meant adding MCAS was not a significant addition to the already approved 737 NG. Boeing could thus keep its costs low and the plane on schedule since it would not have to spend the time and the millions it would take to train all the pilots around the world who would be flying the new plane.

Unfortunately, it turned out that the plane "wasn't handling well when nearing stalls at low speeds."[26] So Boeing engineers changed MCAS and other operating conditions in very significant ways. Combined with decisions Boeing made about what was standard on the plane, pilots now had a plane that did not fly like any previous 737. The Chief Project Manager at Boeing approved MCAS, but was unaware of the changes.[27] Boeing made sure the airlines, the pilots and the FAA were unaware of these changes as well despite the MAX now handling very differently from previous 737's.

To repeat, no pilot was aware of any of these changes. So the pilots of the Lion Air and Ethiopian planes would be surprised when the planes handled differently than they had been led to expect. The differences were significant:

- The engineers had the software kick in when the plane was flying at low speeds.

This change meant that MCAS could kick in way *inside* the normal operating envelope. This change occurred before Forkner asked the FAA to delete MCAS from the training manuals,[28] but he was apparently unaware of it since he later noted in surprise when he discovered the change, "Oh shocker alert! MCAS is now active down to M .2"—roughly 150 mph.[29] So, rather obviously, the pilots would be surprised when the plane's nose went down, not having any idea what would be causing it.

Since all pilots had "longtime training that pulling back on the control yoke raises a plane's nose, putting the plane into a climb," as it would have on any other 737, their first reaction to the nose diving would be to pull back on the yoke.[30] That would be their "initial instinctive reaction," but "in this case, that's not going to work for very long."[31]

Previously, when they let go of the yoke, the speed trim system switched off so pilots could take manual control of the plane. But having been surprised by the nose going down, the pilots would be even more surprised when they let go of the yoke after trying to right the plane.

- The engineers blocked pilots from cutting "off electronic control of the stabilizers" by putting back on the control column, the yoke.[32]

Pulling back on the yoke raises the elevators on the tail and so gives lift to the plane to pull it up from a dive. Letting go used to give pilots manual control. So when they let go of the yoke, the pilots would assume they could now control the plane without the speed trim system kicking in. But they would be wrong.

- The engineers programmed the software to cause "repetitive activations."[33]

MCAS was programmed to use the "pilot release of the electric trim switch to reset MCAS activation."[34] So rather than switching off the speed trim system, pulling back on the yoke now reset it to kick in after five seconds and would do so again and again each time the pilots let go after pulling back the yoke. It would repeatedly force the nose down as they repeatedly followed standard operating procedure and pulled back on the yoke to right the plane. So they would do what they had been trained to do to right the plane, but discover that far from righting the plane, they were causing the nose to dip yet again. But matters were made even worse by another engineering change.

- The engineers quadrupled the force with which MCAS would push the nose down.[35]

Previously MCAS had pushed the horizontal stabilizer 0.6 degrees "each time it triggered," but now pushed it 2.5 degrees, more than a fourfold increase.[36] The engineers made the change because "when a plane is flying slowly, flight controls are less sensitive, and far more movement is needed to steer. Think of turning a car's steering wheel at 20 miles per hour versus 70."[37] Unaware of the change, the pilots would obviously be surprised when the plane went down by that much and just as surprised by another change the engineers made.

- They had MCAS "move the horizontal stabilizer a fixed amount, regardless of" its current position.[38]

Instead of calibrating the amount of movement needed for the stabilizer to put the plane on a straight path, the engineers chose to have it move the stabilizer 2.5 degrees even if only a much smaller amount was sufficient. The stabilizer is at its "maximum nose down" at "4.7 degrees,"[39] and without correction, "two cycles of MCAS . . . would have been enough to reach the maximum nose-down effect."[40] Each time the pilots pulled back on the yoke and let go, they would drive the nose down farther so that "multiple MCAS commands resulted in a significant horizontal stabilizer mistrim condition."[41]

- The engineers provided MCAS "with data from only one of the two angle of attack sensors."[42]

The angle of attack sensors are effectively small wings on both sides of the plane next to the cockpit, like your hands outside a car window. They sense whether the plane is flying dead into the wind or angling up or down, and they send that information to the cockpit. Originally, MCAS would kick in only when it received signals from "two distinct sensors," but in the redesign the engineers had it kick in when only a single sensor signaled. The plane was thus "vulnerable to a single point of failure,"[43] and as one of the engineers who helped design MCAS said, "That's nuts."[44] The reason is that angle of attack sensors are relatively fragile, with "hundreds of reports of bent, cracked, sheared-off, poorly installed or otherwise malfunctioning

angle of attack sensors on commercial aircraft over three decades."[45] They are often struck by birds so they become inoperable or provide faulty readings. The engineers' decision to provide data from only one left the plane "vulnerable to a single malfunctioning sensor, or data improperly transferred from it."[46] The sensor on the Lion Air was off by 21 degrees,[47] but the pilots could not have known that and would, in fact, have thought they knew that it was functioning properly. Why?

- Boeing deactivated the warning signal that told the pilots of a malfunctioning angle of attack sensor.[48]

That signal device was standard on previous planes but was now part of an "optional" upgrade. Boeing failed to notify its customers and the pilots that the warning signal was no longer standard. So the pilots would have no warning that a sensor was malfunctioning since the warning light was not flashing.

- Boeing deactivated the "disagree light," which tells the pilots that the two sensors are not in agreement.[49]

Of course, this warning light was not needed since MCAS only received information from one sensor, but it had "been certified as a standard aircraft feature" and was part of the approved design for the MAX and thus required.[50] It is thus all the more puzzling why the engineers would choose to have information sent to MCAS from only one sensor.[51] The disagree light also became part of an optional upgrade that Boeing sold as an extra and so was not functional without airlines paying for the upgrade.

It gets worse. A manual provided to Lion Air "explained how the AOA Disagree alert was intended to work," but gave "absolutely no indication" the alert "was not operational" on their planes. So pilots who checked the manual for help "would have falsely believed that the AOA Disagree alert was functioning properly and would reliably warn them of a malfunctioning AOA sensor. Boeing knowingly deceived these pilots and its customer airlines."[52]

§8. The Pilots

The pilots would obviously be surprised when MCAS kicked in, not knowing that it was on the plane, but

- the engineers failed to take into account how long it would take for pilots to recognize what the problem was and to respond appropriately.

The nose of a plane keeps getting pushed down when the horizontal stabilizer fails to stop at the right position. That is a runaway trim. As we have seen, the standard way of solving that problem is to pull back on the yoke and let go, thereby assuming manual control of the plane. The pilots can then ensure that the stabilizer is in the right position to right the plane. That is basic knowledge for a pilot.

The FAA guideline is that pilots be able to respond to runaway trim within three seconds. Since MCAS was just a modification "to the existing speed trim system," basic knowledge would allow pilots to recognize and resolve the problem within three seconds, Boeing assumed.[53] But even recognizing the problem within three seconds would be difficult.

First, stabilizer runaway is defined as a "continuous uncommanded movement of the tail," but with MCAS the plane would not act "in the same manner as a typical runaway, as the movement was not continuous and pilots were able to counter it multiple times by pulling back on their control columns."[54] The pilots would have trouble recognizing the problem not only because the movement was not continuous, but also because "the cues received by the pilots due to degraded sensors affecting MCAS were significantly different than the cues received with a runaway stabilizer trim, the procedure that Boeing and the [FAA] . . . instructed pilots to use, slowing diagnosis of the problem."[55] One of Boeing's own test pilots took "more than 10 seconds to respond to uncommanded MCAS activation during a flight simulator test." The pilot found this "catastrophic."[56] The engineers at Boeing certainly

should have known that even the best of pilots, familiar with MCAS, would sometimes be unable to respond within three seconds, and that the result would be "catastrophic."

Second, they would be quite startled. As Sully Sullenberger, the pilot who safely landed a plane on the Hudson, said, "I can tell you firsthand that the startle factor is real and it's huge. It absolutely interferes with one's ability to quickly analyze the crisis and take corrective action."[57] The pilots on both planes that crashed were clearly startled when MCAS kicked in, with no warning of a problem and no indication of a potential stall. They could see that their planes were not at angles of attack that risked stalling.

Third, the pilots were inundated with a cacophony of alerts. "A 'stick shaker' noisily vibrated the pilot's control column throughout the [Ethiopian] flight," warning that the plane was at risk of stalling—even though it was not. In addition, "a computerized voice repeating a loud 'Don't sink!' warned that the jet was too close to the ground"—when it was not. And "a 'clacker' making a very loud clicking sound signaled the jet was going too fast." So while "they tried to diagnose the situation," they were inundated with a "cascade of alerts," distracting enough in themselves, but also signaling they had problems they did not have.[58]

Fourth, "multiple warning lights told the crew that the speed, altitude and other readings on their instruments were unreliable."[59] So while they were trying to figure out what was going on and were distracted by alerts, they were being told that their instruments were providing unreliable readings. This presumably meant that at least some of the alerts should be ignored. But they could not know which ones, if any.

It is difficult to imagine anyone coming to grips with such a startling surprise and solving the problem within three seconds even if they knew everything there was to know about MCAS. Even a pilot who knew about MCAS took more than ten seconds, and the pilots on the Lion Air and Ethiopian flights did not know anything about MCAS. In summary, they did not know that:

- MCAS could commandeer the plane while the plane was going only 150 mph.
- MCAS would push the nose down at quadruple the usual force and do so even if the force was more than needed to right the plane.
- Pulling back on the yoke would only provide temporary relief since it no longer broke the circuit controlling MCAS.
- Letting go the yoke would reset MCAS to kick in again after five seconds.
- MCAS would repetitively push the nose down—by 2.5 degrees.
- Only one attack sensor was to provide information.
- Even though the warning light for a malfunctioning sensor was not flashing, it would not flash even if the sensor were malfunctioning.
- Even though the disagree light was not flashing, it would not anyway.

The pilots would have been startled to find the plane's nose pushing down. Their reaction would no doubt have been what it would have been in such a situation in previous iterations of the 737: they would pull back on the yoke. That would perhaps right the plane, but when they released the yoke, MCAS would push it down again. As we have noted, habitual reactions tend to take over in times of stress, and so they would likely pull back on the yoke again. That might straighten the plane out a bit, but however often they pulled back, MCAS would push it down, again and again. Since MCAS pushed it down the same amount whether it was horizontal or already going down, the plane would continue to go down and down, sending "the plane into an irrecoverable nose-dive" as the pilots tried to pull it out.[60]

The pilots would have had no warning that anything was amiss until the nose suddenly went down. Not seeing any warning lights, they would assume that the sensors were sending accurate information, having no way of knowing that only one would be sending information and that they would get no signal from it in any event. Then, discovering, they thought, that their instrument readings were off, they would not know what to think about not getting a warning light.

But now, with the nose continually being pushed down and their doing what had always worked before to steady a 737 in a stabilizer runaway, they must have been at their wit's end to figure out how to solve whatever the problem was.

They did have one additional option. There is "a large wheel beside each pilot that's mechanically connected to the stabilizer." It "begins to spin" when the trim is moved. "This is the manual trim wheel." This spins thirty or forty times each time MCAS kicks in.[61] So theoretically a pilot could grab hold of that wheel to stop it and even countermand MCAS by spinning it the other way. But turning it is "like lifting a ten-ton bucket of cement from a deep well."[62] The force on it is just too great.

So Boeing and the FAA were deflecting blame on the pilots for not doing what they could not reasonably have been expected to do. Even had Boeing been willing to inform pilots and airlines of the changes in software that significantly altered how the MAX handled as compared to any previous version of the 737, the pilots would have been hard-pressed to respond within three seconds. They would have been no different than Boeing's own test pilot who took more than ten seconds to respond even though he knew of the software changes.

We know that Boeing kept pilots and airlines in the dark because they wanted to avoid the cost of training pilots in the new system, training that the FAA would require if the system were in fact judged to be new. It is not difficult to draw the conclusion that Boeing was far more concerned about its bottom line than it was about safety. Its culture changed with its merger with McDonnell Douglas. As its new president, from McDonnell Douglas put it, "When people say I changed the culture of Boeing, that was the intent, so it's run like a business rather than a great engineering firm." So we know why Boeing made airline companies pay extra for what had been standard equipment and why it insisted that the 747 MAX would fly just like its predecessor. What had been "a passion for great planes was replaced with 'a passion for affordability.'"[63]

What we do not know is why the engineers at Boeing made the changes that caused the pilots difficulty. Why were the stabilizers

moved 2.5 degrees rather than just what would be needed to stabilize the plane? Why did letting go of the joystick after pulling it back not completely cut the electronic connection? That created a legacy problem. One of the first things pilots have to learn is that pulling back and letting go of a joystick breaks the connection, and it has to become second nature to them so that they do not even have to think about it. It has to become habitual. Changing the way the joystick operates thus guarantees pilots will have problems. And why were the stabilizers moved 2.5 degrees again five seconds after the pilot let go of the joystick? It will be a long time before we get definitive answers to these questions if we ever do. Boeing will do whatever it can to hold tight any information about the engineering decisions if only because of concerns about legal liability.

We can criticize the engineers' solutions to the problem of having to work with the original 737 fuselage instead of a new one designed to handle more efficient, and thus larger, engines, but the initial fault lies with Boeing management not thinking about developing a new plane and insisting that they had to get a plane off the ground quickly to compete with Airbus. Boeing management pushed hard on the engineers and others to get the job done, even putting up countdown clocks for everyone to see. But the rush to get something out the door can easily lead to problems.

The problem is particularly acute with software. Microsoft's Vista is a case in point. Quite some time ago, long enough that I cannot now find the reference, I read a review of software for determining driving routes before GPS devices were common. The setup required that the user put in an address, but when the reviewer clicked on "Continue," he was informed that he had failed to put down the state—New York, Missouri, wherever he was. He tried to go back, but the software would not let him to do that. He tried to continue on, but the software would not let him do that either. Only after crashing the program, and his computer, was he able to start the process over again. But when he went through the program again, this time paying more careful attention to its requirements, he discovered that the program did not permit

an operator to put in a state of residence. Clearly, the software went out the manufacturer's door without anyone there trying it out to see if it worked, or, worse, it went out even after someone tried it out and discovered it did not work.

As software gets more complex and various updates are added, the likelihood of such failures will no doubt increase.

> On their first deployment to the Pacific, eight F-22 fighter jets experienced a Y2K-like total computer failure when crossing the international date line. . . . All onboard computer systems shut down, and the result was nearly a catastrophic loss of the aircraft. While the existence of the international date line could clearly be anticipated, the interaction of the date line with the software was not identified in testing.[64]

The crash of the Colombian airliner was catastrophic not only because it led to 159 deaths and all the consequent harm to the families and the employers of those people but also because it led to the loss of an expensive aircraft and no doubt a myriad of other harms including, presumably, an examination of the software in other aircraft, revision of the training manuals, and retraining of all other pilots—each an extensive and expensive enterprise. The Boeing 737 MAX disaster not only cost many lives, but Boeing's reputation and over ten billion, and still counting.

We can see how ethics enters into the heart of engineering in understanding how the software designs in the Colombia plane and in the Boeing 737 MAX provoked fatal mistakes. The accidents may seem an anomaly, the oddity of the software being so unusual as to limit the lessons we can draw from it regarding engineering in general. But what drove the accidents is what drives every engineering project, a set of choices about how to design a solution to a problem or set of problems. These choices are not morally neutral even when the designs chosen are themselves free of harm and innocent of any harmful effects. That just means the morally right choice was made. No engineering choice is morally neutral, that is, the solutions to design problems incorporating

choices that have effects once realized in artifacts and produce more or less harm. Ethics enters via the design of the artifacts of engineering.

Since we are obligated not to cause unnecessary harm, ethics is at the center of engineering. We can be faulted for failing to fulfill an obligation even without intending it. No one is suggesting regarding either the Colombia disaster or the Boeing 737 MAX that any software engineer created flawed software so as to cause harm. Moral responsibility does not depend upon anyone intending to do harm. A physician who amputates the wrong limb is morally blameworthy whatever the physician's intention. Software engineers are morally responsible for flaws in software whatever their intentions. It is a moral failure not to think through how the software would create the sorts of problems that led to the crashes and a moral failure not to redesign the software to avoid those problems.

5

Moral Responsibility

Intent Is Not Necessary

§1. Intent Is Not Always Necessary

One issue we have left hanging is the role of intent in being held morally responsible. Consider again the software problem that contributed to the crash in Colombia. Someone may ask, "How can anyone hold them morally responsible when they did not intend to cause any harm?" If I accidentally bump into someone and say, truly, "Oh, sorry, I tripped," that generally gets me off the moral hook. I could be held morally responsible if I were careless, horsing around and not paying attention to those around me. Any person I then bumped could well chastise me for being so careless. But with no intent on my part to bump into someone, I am generally not morally at fault, and the person would be morally wrong to hold me responsible for the bump.

We learn about the relevance of intention very early in our lives. Listen to two children having a spat, or to a parent addressing a child after some misadventure, and you are bound to hear, "I didn't mean to . . ." followed by whatever it was that the child did for which he or she is being admonished. The child is denying any intention to cause harm, the lesson having been learned at a very young age that intention is what seems to make the difference between being held responsible and being let off.

But that is a mistake. We can be morally culpable without any intent to cause harm. Let us first look at the situation where there is intent to cause harm.

§2. Moral Responsibility Because of Intent

Suppose a terrorist had meddled with the computer software on the Colombian plane so that at some time, like a hidden time bomb, some pilot would type "R" for Cali and the plane would turn toward Bogota and into the mountain. We would hold the terrorist morally responsible.

But that judgment depends upon at least two conditions being satisfied.

First, the person must be capable of being morally responsible—old enough, sane, and so on. Toddlers are not responsible should they cause even serious harm. They are too young to know right from wrong and so too young to make the right choice. As any parent knows, the point at which we can reasonably hold a child accountable is not on any growth chart. An infant can get away with murder, as it were, and yet, at some point, we have no hesitation holding a child morally responsible. The line has been crossed somewhere, but some will stray back across it. Reversion to infantile behavior is less rare than we would like it to be, and then there are mental defects such as insanity and dementia that can preclude moral responsibility. A kleptomaniac is capable of being moral and knows right from wrong, but cannot resist the impulse to shoplift. But we do not need to work out the complex subtleties of what it is to be morally capable to understand that we cannot properly judge someone morally responsible if they are not capable of being morally responsible.

Second, people must know that what they do is wrong. Ambien is a recent addition to the remedies for sleeplessness, but some who have taken Ambien have driven to work while asleep, eaten in their sleep, and so on—only discovering what they have done after they have awakened, gone to work, and discovered they had completed the report they were going to work on that day. Sleepwalkers do all sorts of things they do not remember and for which we cannot, reasonably or morally, hold them morally accountable.[1]

When a man kills his wife in his sleep and claims he did it because of a severe sleep disorder,[2] he is effectively claiming that "at the time of the committing of the act, [he] was laboring under such a defect of reason, arising from a disease of the mind, as *not to know the nature and quality of the act he was doing*, or, if he did know it, that he did not know what he was doing was wrong."[3]

Whatever the details of this complex issue about moral responsibility, when someone does something and cannot know that what they are doing is wrong—the Ambien syndrome, as it were—we do not hold that person morally responsible. They cannot intend to do anything wrong.

But if someone has the capacity to be moral, knows that the act in question is wrong, and intentionally does it anyway, we have all the reasons we need to hold the person morally responsible. Had the software engineers deliberately introduced the software flaw in that Colombian plane, there would be no room for doubt in holding them morally at fault.

We would hold them at fault even if they failed to hack the software and no harm was done. They would not get off the moral hook if they intended to cause harm and failed. When children are old enough to know better, we punish them for trying to hit a sibling, even if they miss. You do not have to succeed in causing harm to be morally culpable if you intend to cause harm. The intent to cause harm suffices as a foothold for moral criticism. We have no foothold if someone does the right thing, knowing it is right, without any foreseeable adverse consequences. If any one of these features is missing or less than sterling, we have at least a toehold for moral concern.[4]

Indeed, any variation in any one of them will affect our necessarily nuanced moral judgment. If the engineers introduced the software flaw by accident and tested the software thoroughly, but failed to find the flaw, we would soften our judgment about their moral culpability and try to determine what about the testing misled them into thinking the test was thorough. At least they tried to do the right thing.

If we have in mind the gold standard for moral responsibility—intentionally doing what is wrong or harmful—we may find it difficult

to think of any situation where someone could be responsible without the relevant intent. We can readily imagine a person of bad character doing good—by accident or as a way of encouraging trust, for example. We can readily imagine a person of good character accidentally doing something wrong. We can readily imagine good acts producing bad consequences and bad acts producing good ones, but how, we may well ask, could someone be morally responsible for doing something wrong without intending to do what is wrong?

§3. Moral Responsibility Without Intent

We can easily find situations where we refuse to excuse someone who causes harm even when the person lacks any relevant intent. If I hit a child while driving too fast in a residential area, I am not off the hook morally when I say to a parent, "Oh, sorry about that. I didn't mean to kill your kid." My intent is irrelevant. If I am engaged in target practice and a toddler wanders into my field of sight, I am not off the hook morally if I continue to shoot even if I do not intend to hit the toddler. I am morally culpable for putting the toddler at risk even if I think I am such a good shot that the risk is negligible or nonexistent. "I wasn't using him for target practice!" will not get me off the hook morally any more than "I was here first!" Even the best of shots can make a mistake, and continuing target practice while a toddler toddles close to one's line of sight is too risky to justify. Putting someone at risk of harm is itself a harm.

We find many such examples in our ordinary lives as well as among professionals. We read from time to time of an attorney falling asleep during a trial. Before making a judgment, we do not ask, and do not need to ask, "Did the attorney intend to fall asleep?" We do not ask because the attorney's intentions do not matter. A sleeping attorney cannot hear the evidence or testimony so as to be able to rebut it or take advantage of it, cannot make objections to inappropriate remarks made by the opposing counsel, cannot, in short, properly defend a client.

Attorneys are licensed, and a condition of their obtaining a license is that they have completed a course of work and passed an exam that at a minimum proves them qualified to practice law. A client has every right, in hiring an attorney, to expect at least a minimal level of competence, and that is not possible if the attorney is asleep during the client's trial. The lawyer's intent is irrelevant.

In a recent case, Texas state courts decided that, to quote the defendant's new attorney, "The state does not believe that you have a right to a lawyer who stays awake." In the case in question, the lawyer fell asleep a number of times during the trial, once for over ten minutes and once with his head on the table. The defendant's new attorney said he was "as responsive . . . as a potted plant," but the Texas prosecuting attorney successfully argued there was no proof that the lawyer's sleeping made any difference in the trial.[5] When the new defense attorney appealed to the US Appeals Court, it said, "Unconscious counsel equates to no counsel at all."[6]

The problem for the attorney's client, and for the court, is that a lawyer is not at a trial just for show. A sleeping lawyer might as well be a potted plant for all the good done for the client. We might find that the lawyer was perfectly competent, but had mistakenly taken an Excedrin PM or was suddenly overcome with narcolepsy. Our moral judgment would have to take that into account.

We generally presume that someone who has obtained a license to practice a profession has acquired the requisite knowledge and skills and so is competent, but we can, yet again, find examples of professionals so incompetent that they cause harm without any relevant intent. They are so bad at what they are supposed to do that they cause harm just trying to do what they are supposed to do.

At a VA hospital in Philadelphia, Dr. Gary D. Kao made mistake after mistake. In one case, he put most of the forty radioactive seeds that were to kill a prostate cancer in a patient's healthy bladder. He corrected that mistake by rewriting his surgical plan "to match the number of seeds in the prostate" and then proceeded to implant more seeds in the patient, this time in the patient's rectum rather than his prostate. Over a six-year

period, the VA hospital "botched 92 of 116 cancer treatments," with Dr. Kao apparently the attending physician in most if not all of these cases. It is difficult to call him "Doctor" Kao without irony. Someone who makes those kinds of mistakes, and makes them repeatedly, certainly lacks the specialized knowledge and skills necessary to be a physician even if they have somehow passed a qualifying exam and obtained a license to practice.[7]

We do not know whether "Dr." Kao lacked the relevant knowledge or lacked the relevant skills to use that knowledge or, more likely, lacked both. To become a professional, we need two kinds of knowledge, knowledge that and knowledge how.[8] We can refer to a surgeon's knowledge that a kidney is not a gizzard, to a lawyer's that a continuance is not a dismissal and that a dismissal is not necessarily a dismissal with prejudice, or to an engineer's knowledge that a strut is a kind of brace or that the holding strength of bolts is different from that of welds. These are all examples of the kinds of information that a professional must learn to become a professional, examples of knowledge that something is the case.

We refer to knowledge how when we reference the rules of skills someone must learn. We learn to ride a bicycle. That is a skill. But in learning how to ride, we may have no knowledge about what the parts are called. We do not need that knowledge to learn how to ride. We learn how to use a software program that allows us to calculate stresses easily. We do not need to know anything else about the program's code to become skilled in using it.

These two kinds of knowledge are distinct, but becoming an engineer, a surgeon, a lawyer, or any professional within a discipline requires both—knowledge about the details of the specialized discipline and about how to use that detailed knowledge to accomplish whatever ends the discipline is supposed to achieve. Even those who only minimally qualify for a profession must, we presume, have reached a relatively high level of competence: the training is long and arduous, the qualification tests fairly rigorous. That presumption can be rebutted, as it would be in the case of Kao, but it is that presumption which justifies us in holding morally culpable a professional who causes harm, even

unintentionally—as when a surgeon cuts an artery thinking it a vein, or a lawyer fails to fill out a form properly so that a will is not legally valid, or an engineer fails to calculate a load properly. The professional ought to know better.

Aristotle pointed out how difficult it can be to do the right thing—to act "at the right times, with reference to the right objects, towards the right people, with the right motive, and in the right way."[9] The reason it can be so difficult is that learning a skill requires learning all manners of things, any one of which could go wrong.

A surgeon must learn not only to distinguish arteries from veins but exercise enormous caution and care. Someone who fancies lightning moves, a thrust-and-parry cutting away of an appendix, or who has a lightning temper, moved to anger at the slightest problem, is not well suited to be a surgeon. Too much is at stake, and too much can go wrong, to risk irascible surgeons who fancy themselves fencers in an operating arena. The process of making someone into a surgeon must weed out such traits—or individuals with such traits.

In the same way, engineers must learn to be risk-averse, unwilling to resolve engineering problems in ways that risk unnecessary harm. They must be exceedingly cautious about the possibility of mistakes and so careful to check and double-check their calculations. Budding engineers who fancy lightning solutions or think themselves immune from the errors that plague us all will not long survive the rigorous training essential to making a competent engineer or survive in the real world of engineering should they somehow make it through that training. They will discover gaps in their knowledge and skills as problems arise they have never thought about.

Included in the requisite knowledge essential to any profession is the capacity to fill in the blanks in their professional knowledge. A lawyer must "know the law," but that does not mean knowing everything of legal import—the substance of every case ever decided, for instance. It does mean knowing how to find out what is of legal import relevant to a case. So one skill professionals must learn is how to learn what they do not know within their disciplines.

They must also have the capacity to keep up with professional practice. An engineer who relies wholly on what was available in four or five years of undergraduate work in engineering cannot claim competence for very long in the profession. New discoveries and techniques impact professional practice, and an engineer must keep up just like every other professional. Becoming an engineer by getting an engineering degree is not the end of a person's learning to be an engineer.

It does not take much time for a discipline to advance enough to make professionals who rely on the knowledge and skills they had when they entered their profession to become less than fully competent. Legislatures pass laws, courts decide cases, and townships change their ordinances. Within a few years, lawyers are left behind who do not keep up. If competent, they may become only minimally so. Just so for engineers and every other professional, and, of course, it is always the case that a professional may not be competent enough regarding what is at issue. We would hold such a professional morally responsible even without an intent to cause harm.

So we hold professionals morally culpable when they lack the knowledge or skills they were supposed to learn to become professionals and when they fail to keep up with what is new in their field. We hold them morally culpable when they have that knowledge and have the skills, but fail to use them in the way they should have learned to use it as professionals. We hold them morally culpable if their level of competence falls below the level they really needed to do the job they were supposed to do and, as a result, they cause harm. We hold them morally culpable in all these cases even if their failures are unintentional.

§4. Those Software Engineers

The software engineers who designed the autopilot software in that Colombia aircraft failed the company that hired them, the pilots who

relied on them, and the passengers they put at great risk by having designed software with a fatal flaw.

That flaw led to the crash. We might hold the pilot responsible for not double-checking that in hitting "R" he engaged the autopilot to land at Cali, but clearly the bulk of the responsibility lies with those who designed the software that required checking because it was flawed. The software engineers were responsible—not because they intentionally designed the flaw into the software, but because, having designed the software with that flaw, they failed to design the flaw out.

They could have failed for two different reasons:

1. They may not have known it was there.

But they ought to have known. They were better positioned than anyone else to understand the software and see that they had written code making the default for the autopilot the closest beacon and another that made Bogota the default for "R"—although it is certainly arguable that it is often those most deeply engaged in an enterprise who are least able to back off to see any problems with it.

2. Or it is possible they knew they had designed software with competing lines of code, but failed to think through the implications.

Either they knew of the flaw or not, and either way they were responsible for the subsequent loss of life and the plane.

They failed to design an artifact that solved the problem. One criterion for successful autopilot software is that it take over the controls of a plane to land it safely in the airport the plane is supposed to land in. The software they designed failed to do that, and that tells us that the engineers not only failed to solve the design problem they had, but also failed to test the software thoroughly to see if they had solved it.

Engineers design artifacts to solve problems. The artifact can be a piece of software, a tractor hitch, a door handle, a car. The kinds and numbers of artifacts that engineers design seem as numerous and diverse

as anything in nature. Engineers are to check what they have designed to see if it works the way it is supposed to work. An artifact that does not solve the problem it was designed to solve fails the most crucial test engineers are obligated to conduct before letting the design out the door.

It does not let these engineers off the moral hook to know that they are in good company. Our modern technological lives are filled with flawed artifacts—rear-view mirrors that drop off the windshield because the glue fails, two-ton concrete slabs that fall off tunnel ceilings, cellphones that cannot be held without risking pushing buttons on their sides that will interrupt calls, remote controls so complicated we struggle to find the mute.

The more complex something is, the more likely it is to have flaws and the more unlikely it is that anyone will notice the flaws—particularly when the flaws are not in individual parts, lines of code in this case, but in the combination of distinct parts.

But, again, that is the point of testing. Had the software engineers tested the software as they should have, they would have found the problem, and, having found it, they should have fixed it. There is no reason typing "R" ought to override the normal default setting and direct the autopilot to fly the plane to Bogota. That line of code is not essential to the software, and we can readily predict an accident given the two different defaults.

So we quite properly hold the software engineers morally culpable for failing to test the software, discovering the problem, and then redesigning the software to remove it. It makes no difference if they unintentionally introduced a flaw. They failed the competence test, failing to reach even a low level of competence in designing software that solved the problem it was supposed to be designed to do. Intentions can certainly matter in making moral judgments, but unintentionally causing harm is not always a moral excuse.

6

Permitting, Encouraging, and Provoking Errors

§1. The Argument So Far

We now know that:

- Design problems are open-ended. A problem does not determine its solution but leaves conceptual space for creative imagination.
- The chosen solution will select one set of values over another and, when realized in an artifact, produce one set of effects over another.
- The choice of a design solution is thus ethical, the set of values chosen reflecting one of many and the effects producing more or less harm than other choices.
- Engineers make moral judgments in solving design problems whatever their intent.

We also know that:

- To become an engineer, a person must come to have the specialized knowledge and rules of skill essential to being an engineer.
- A failure in either raises an ethical red flag: the role morality of an engineer requires that knowledge and a competent use of the rules of skill essential to the profession.

The best examples of how ethical considerations enter into the intellectual core of engineering are error-provocative solutions. The argument is simple. If engineers could intentionally choose error-provocative solutions, they would then be making a moral judgment—

not a good one, of course, but a moral judgment nonetheless. So in choosing solutions which are not error-provocative, they are also making moral judgments, at the least judgments not to provoke unnecessary harm. These are not trivial judgments.

§2. An Evil Genius of an Engineer

Engineering so permeates our lives that it is difficult to imagine what the world would be like if engineers tried to cause harm. They are at the center of our technological lives, designing everything we might think of as exemplars of our lives—our highway system, mobile phones, stoves, planes, cars, the electrical grid, and on and on. The list is almost endless since it is difficult to imagine any artifact untouched by an engineer.

To see how much we owe to engineers, to engineers going about their jobs with the competence they expect of themselves and we expect of them, we can suppose the world's engineers were evil geniuses, striving to introduce as much harm into our technological world as they could, taking advantage of decision points in solving design problems to introduce harmful results. Even a few well-placed evil geniuses, choosing just the right weak points in our technological world—the electrical grid, computer software—could turn our world into a chaos of malfunctions. We have a glimmer of what kinds of harms a few well-placed and very adept individuals can cause by seeing what can and has gone wrong with the internet, especially with what was supposed to be secure information.

Evil engineers would have no trouble wrecking havoc in our technological world. They could create a world where nothing worked—no phones, no cars, no stoves, no furnaces, no water heaters, nothing at all. They could create a world in which everything looks as though it works but fails—cars start but then stop, stoves turn off as soon as we turn them on, and phones ring but cut off when answered. They could create a world in which everything appears to work one way,

but instead works another—where everything was error-provocative, producing harm whenever any operator did what the design of the artifact signaled ought to be done.

If they were really perverse, they would create a world where enough things worked the way it appeared they worked and worked well enough to give us sufficient confidence to move about and try to do things, not always wondering whether something will work this time or whether that new artifact in our lives will cause the sort of frustrations we hope to avoid. We would have enough regularity in the way things work not to find ourselves always worried, but would then find ourselves caught up short when things went wrong—when nail guns randomly misfire, when steering wheels come off in our hands, when gas stoves suddenly explode, and when airplanes crash because some random part was designed to fail unpredictably.

An evil genius of an engineer could do much harm in this world of ours because in solving a design problem, there are many ways to introduce features that produce harm. The decisions engineers make in solving design problems are not morally neutral, that is. Those decisions instantiate moral judgments—whether engineers are aware of that or not.

We seem to note their moral accountability only when something goes wrong. We ask, "How could someone who claims to be an engineer have done something like that?" But engineers act morally whenever they solve a design problem, whether unnecessary harm is produced or not. They either make the right decision, the wrong decision, the best of a bad lot, the worst of a bad lot. They choose a solution and so act ethically—or not.

Their choice will reflect a particular configuration of values, and they are making a moral decision in choosing that configuration over others. It is not a morally neutral decision to emphasize cost over efficiency, for instance, or ease of manufacture over safety. Different configurations of values have different implications, depending on which values are favored and which frustrated. That is one reason different design solutions embody different sets of harms and goods when instantiated

into artifacts, and engineers have an obligation, at a minimum, to minimize the harmful effects.

We do not live in a world of chaotic malfunctions because—no surprise here—engineers generally do what they ought to do. So the obvious question to ask is why it is important to show that whatever they do, they are making ethical decisions?

§3. So What Difference Does It Make?

Pointing out that ethics is internal to engineering practice makes explicit what is implicit. We are only looking in a different way at what engineers already generally do. But if engineers generally do the right thing without thinking about ethics, why should they think about ethics? What is the gain? Like ethics, the gains permeate engineering practice.

1. What counts as a design problem? If engineers look at their solutions to design problems as making moral choices, they can see problems they might not otherwise see. Of all the things that can go wrong to cause an accident, the worst for an engineer is for an engineering artifact—software, for instance—to be implicated because it is error-provocative. To point out the obvious, being wholly at fault for causing what can be great harm—159 dead, for instance—is not a good position for anyone to be in, but to avoid that kind of problem, engineers need to think about how an artifact will be used and query various design solutions to determine if they are easier or harder for those who will use them when instantiated in an artifact. A design problem is not just a set of specifications to produce a certain end, but, once solved and instantiated in an artifact, will have effects in the world. Engineers are responsible, at a minimum morally, for ensuring that their designs do not themselves provoke unnecessary harms when realized in an artifact.

To repeat, it is unnecessary harms that are to be avoided. It is difficult to imagine a design solution that avoids all harms. No matter what

the material from which it is made, there will be a carbon footprint in obtaining it, another in manufacturing the artifact or the artifact in which it is to be placed (as software is placed in computers), and so on. But to avoid unnecessary harms, we need to expand our view of the nature of a design problem and consider the whole range of harms associated with any engineering solution. They are all open to moral consideration.

2. What counts as a harm? We have focused on design flaws that produce harm for those using the artifact. Error-provocative designs are the most striking, but concentrating upon error-provocative designs can itself provoke an error on our part in understanding all the ways in which engineers can introduce harms into the world. Many engineering artifacts, perhaps most, are not properly described as artifacts that can mislead an operator—bridges, for instance.

The design process is not limited to determining how something should be designed to be used properly. Engineers need to consider what materials to use (and so how dangerous it may be to get it and how much harm is involved in obtaining it), how complicated it will be to make the artifact (and so how much energy and time and money will be consumed), how complicated and costly it will be to store the artifact until it is sold, how long its useful life is, how easy or hard it is to repair and at what cost, what will happen to the artifact once its useful life is over (and so how much of the artifact can be recycled and how easily), and on and on. These are choices engineers are making in solving a design problem, and none is ethically neutral. The engineer who designed mercury switches presumably did not think through what would happen when the switch broke or needed to be discarded,

3. What counts as a solution? We have focused on what engineers ought to do *at a minimum*. "Do no unnecessary harm!" is the bottom moral line, and it is at the bottom. No one wants someone only minimally competent—whether an engineer, a lawyer, or a surgeon. We may presume that professionals can be ranked on a bell curve of competence, going from the most brilliant to the good to the worst. Our educational requirements are, or ought to be, such that the worst

professional is still pretty good, competent enough, if an engineer, not to design error-provocative artifacts at least. If not, we ought to move the floor higher.

Neither society nor any engineer ought to be satisfied, however, with solutions to design problems that display only minimal competence. We ought to presume that anything can be made better—design solutions and us as well, and though we cannot obligate anyone to do or be the very best, we should hope that every engineer would look on each solution as less than optimal, even if they cannot now see how to make it better, and look upon every stage of their lives as a stage for improvement as well.

We can think of error-provocative designs as being at one end of a spectrum of possible design solutions with foolproof designs at the other end. A foolproof design is one that even the most unintelligent, untrained, and unmotivated cannot screw up—at least for artifacts that require operators. Just as engineers ought to avoid error-provocative designs, they ought to strive for foolproof designs. That would be to aim for the very best. Unfortunately, as we all know all too well, there are too many different kinds of fools to design something that is proof against all mistakes. We all have to shake our heads sometimes when we hear of some mistake someone has made that, we would have thought, no one could possibly have made. "What were they thinking?" is a rhetorical question in such situations because we have no idea what they could have been thinking—or even if they were thinking. So a foolproof design is at best an ideal, but it is an ideal worth striving for. "Do no unnecessary harm!" should be complemented by "Strive for the best!"

We shall consider in more detail what counts as a solution and what counts as a harm in the next chapter. Here we will consider what counts as a design problem. The division is to some degree artificial. If we fail to understand a design problem fully, we are far more likely to introduce harms we could have avoided and fail to solve the problem successfully. So each example we examine could well have been placed under a different heading.

§4. What Counts as a Design Problem?

Aristotle said of being ethical that "it is possible to fail in many ways . . . while to succeed is possible only in one way (for which reason . . . one is easy and the other difficult—to miss the mark easy, to hit it difficult)."[1] He could just as well have said this about solving design problems. There is more than one way for an engineer to hit a bull's eye solving a design problem, but there are so many variables that need to be taken into account that it is all too easy to miss the target and fail to get things right.

We saw one way of failing when examining the software flaw responsible for the Colombian crash that killed 159 people. The engineers failed to think through how what they designed would work in practice and so, in that way, failed to solve the problem. A design problem is not a theoretical matter, that is, but a practical one. Any solution must pass a practical test: Does it do the job once realized in an artifact?

This is not the only way in which engineers can fail to understand what counts as a design problem, but it is a far more common problem than it may seem. Each of the following examples illustrates that point.

1. Cadillac trunk: In some older Cadillacs, you are to lower the trunk lid to within a foot or so of the latch and then let go. A motor takes over and gently closes the lid. If you push the trunk down to latch it, you break the mechanism. Once the mechanism is broken, the trunk will not latch, and you end up driving a Cadillac with its trunk tied down—hardly the upscale image Cadillac would like to convey.

Repair is costly because it requires taking out part of the trunk compartment and the back seat to get to the mechanism that must be replaced. You end up with a cascading set of effects, a trunk latch broken, the trunk tied down, and a costly repair, all because you or someone else tried to latch the trunk the way we normally do.

The self-closing mechanism creates a problem waiting to happen. We all know that sometime, someone, even with a warning not to close the trunk by hand, will break the mechanism. The trunk opens just the

way normal trunks do, with no sign on or in it indicating it is to be treated any differently than any other trunk. So someone fixing a tire or putting in groceries will get no warning that the trunk should not be closed the way normal trunks are. A single visit to a hotel with a doorman who takes your luggage and slams the trunk will suffice to do in your trunk and your wallet. It will also leave you with an open trunk unless you happen to have or find a bungee cord or rope.

The problem with the trunk of these Cadillacs is not at all unusual. We have in part a user problem. Those who are most concerned that the trunk be closed properly, and best positioned to know how to close it properly because they can read the instruction manual that comes with the car, are not the only ones who will close the trunk, and even they will have to guard against letting old habits take charge. But there are others who will use the trunk—an auto mechanic getting a tire, that hotel doorman—and so there is a risk of harm.

We have in part a legacy problem. People are used to trunks operating in a certain way. Change the way trunks operate, and some people are going to continue to try to operate them the old way just by force of habit. No matter how many warnings the manufacturer puts in the instruction manual, or even on the trunk lid itself, someone is going to try to operate it the old way. We ran into this problem with the toaster lever that, when operated as we are used to operating levers on toasters, will break the mechanism.

So an engineer suggesting a new design needs to consider how things might go wrong because of past habits that will need to be changed. Engineering progress requires pushing the envelope of design and so forcing new habits upon us, but those old habits can cause significant harm.

In this case, the harm is primarily financial—the costs of the time lost, of the repair, of not having the car available. The engineers responsible failed to do anything to prevent those old habits from causing harm—no warning signs, no mechanism to prevent someone from slamming it shut. There could have been a catch on the mechanism, for instance, that prevents someone from closing the trunk lid without touching a

switch or lever, and that would be a warning built into the new design solution that would at least minimize the power of old habits.

Vehicles are a wonderful source of examples of error-provocative designs. "But," one may well wonder, "do these constitute moral problems?" The test is whether there is significant enough harm that could have been avoided, and the determination of harm is not limited to loss of life, for instance, but extends to any setback to an interest we have.[2] Our interest in regard to the Cadillac is to have a functioning car, without unnecessary expense or time spent without the car while it is being repaired. Closing the trunk lid as we normally do in Cadillacs with a self-closing mechanism produces a cascading set of harmful effects. Engineers should try to avoid all those harms if they can design such a mechanism without them.

Because engineers should try to avoid all those harms, we need not get hung up on trying to find a line between morally significant and morally insignificant harms. It is a question that has stymied philosophers, and engineers do not need to get caught up in that query in order to identify the harms that would be produced by a design solution or consider alternative solutions that avoid those harms. What matters for engineers are only two questions: Is there harm, and is it necessary? If there is harm that can be avoided, it ought to be avoided.

In the following example, there is no doubt that the harm ought to have been avoided.

2. X-ray machine: A large X-ray machine was built so that the patient lay on a table with the X-ray on an extremely heavy arm that extended over the table. The arm was as long as the table upon which the patient lay and wide enough to cover the width of the table. It could be rotated as well as raised and lowered so that the X-ray could be focused on a particular spot on a patient. At the end of the day, when the machine was shut down, the arm was automatically lowered to an inch or so above the table to keep the X-ray safe from accidental harm.

X-ray technicians always go behind a lead shield so they will not suffer the consequences of too many X-rays. In this case, the technician operated the X-ray from a console in a room completely separated

from the machine. There was a door into the operator's room, but it was placed so that there would be no danger to the technician. There was, that is, no direct line of sight to the X-ray table or the arm.

The technician controlled the movements of the X-ray arm through knobs and switches on the console. Every movement was programmed by the software specially developed for this X-ray machine and the console.

One afternoon, after finishing up with the last patient of the day, the technician opened the door and called out to tell the man he could leave. The technician then shut down the machine. When the technician went out to leave work, the nurse asked where the patient was. "I told him he could leave." "Well, he didn't come through here." They found him face down on the table, flattened to an inch or so by the heavy arm of the X-ray that had been lowered to just above the table.

In a separate room, the technician had not been in a position to see whether the patient had left, and nothing about the software required that the technician check to see if the X-ray table was clear before shutting down the machine and thus lowering the X-ray arm. The patient had not heard the technician, and, face down, he could not see the machine coming down to crush him.

A little thought about how such software would be used in practice would have revealed the problem.[3] The software was written so that the technician did not need to check on whether anyone was on the table before shutting the machine down. That was an accident waiting to happen—as it did. We know ahead of time, given such a situation, that someone is going to shut the machine down on a patient. What was needed was a check on shutting the machine down that required the technician to go into the X-ray room and hit a button or move a lever on the machine. That way the technician would have to check to see if the table were empty. Or a scale could be added to the table so that anything on it would be detected and that signal would prevent the machine from being shut down. We might find that the scale was faulty sometime, but that safety feature would prevent most accidents.

The general lesson for the software engineers who designed the program is clear enough. They needed to think through how the software would work in situ. "What," they needed to ask, "could go wrong here?" The most obvious things that could go wrong are that the X-ray could misfire somehow and burn patients and that the arm could be lowered onto a patient. So the software engineers ought to have designed the software to preclude both potential harms as much as possible.

The situation regarding the X-ray machine is the same as that regarding the autopilot software. The software engineers failed to think through what was likely to happen when the software was being used by those it was designed for—a pilot, an X-ray technician.

But the questions software engineers need to ask are not limited to what will happen when the artifact they designed is used by someone. They need to check the string of software, obviously. Free of faults? No mistakes? Works? But their questions are not limited to the string and any problems with it. They need to ask, for instance, how the software works with preexisting software. This is a problem like one physicians need to consider when prescribing medication that may not interact well with other medication the patient is taking. A recent example concerns Plavix, an anti-clotting drug given to those who have had a heart attack, and an anti-ulcer drug, Prilosec or Aciphex, generally given because Plavix can irritate the stomach. Those taking both drugs have a 25 percent higher risk of another heart attack. So software engineers need to consider whether new software will work properly with the preexisting software into which it is to be placed. They need to ask, in addition, whether the software gives clear directions to those operating it. Everyone trying to communicate and avoid ambiguity has this problem.

There are so many variables that need to be examined in designing software that it is understandable how a software engineer may fail to think through those effects that are likely to occur when the software is put to use in practice.

Some may think it is difficult enough learning to think like an engineer, and here we are demanding that engineers put themselves

in the shoes of those who use the artifacts they have created—to think like a pilot, or an X-ray technician. But that is not such a demanding challenge. They do not have to be pilots, only think through what it would be like to be faced with two different defaults when trying to land. They do not have to be X-ray technicians, only think through what it would be like to operate the X-ray machine with that software, including closing up the X-ray machine without having any way of ensuring that no one is on the X-ray table. To ensure that their design solutions do not cause unnecessary harm, engineers do not need to stretch their thoughts very far—as the next example illustrates.

3. Defibrillator: Joshua Oukrop was twenty-one when he died. He was on a biking trip with his girlfriend when he called out from ahead, "Hold on. I need to . . ." and tumbled over backward, dead, his defibrillator having failed to work when needed. He had a genetic heart disease and a defibrillator that was to "emit an electrical jolt to restore [normal] rhythm to a chaotically beating heart."[4] Mr. Oukrop's defibrillator shorted out.

The defibrillator failed because of the deterioration of the polymide coating on electrical wires "in a component that sits atop the sealed part of a heart device. The component, called the header, is essentially a junction box connecting a unit's computer and power supply with cables, or leads, that carry electrical impulses to the heart." But "body fluids can slowly seep into the header, which is not hermetically sealed, and cause [the] polymide to deteriorate."[5] The deterioration means that the defibrillator will short out when it tries to send a life-saving jolt to restore the heart's normal rhythm.

The manufacturer, Guidant, discovered the flaw in 2002, three years before Mr. Oukrop died. It fixed the problem, but did not inform those with who had had the flawed defibrillator implanted or inform their physicians. It announced the flaw only in 2005 when it discovered that the *New York Times* was publishing an article about it.

Guidant did not inform the patients with the defibrillators or their physicians because, it said, it judged "the risks, like infections,

associated with surgical replacements outweighed the risks posed by the device."[6] Replacing the defibrillator, it claimed, was likely to cause more harm than leaving it in place—even though the harm of leaving it in place meant that some who relied on it to save their lives would die when it failed. It seems an odd juxtaposition, weighing the certain loss of lives against possible infections, and that paternalistic response prevented patients from making their own judgments and precluded physicians from taking part in judgments about the health of their patients. Neither physicians nor patients gave informed consent that the flawed defibrillators not be replaced. Neither may have wanted to be faced with having to make such a choice, but it was theirs to make, not Guidant's.

Guidant may have made the decision not to inform the patients or physicians because it continued to sell the old model until, apparently, its inventory of flawed defibrillators was gone. After the *New York Times* article, Guidant appointed an independent panel to investigate, and among its findings was the following:

> During a period of approximately one year after the corrective action was taken in response to the observation of arcing, more than 4,000 of the pre-mitigated devices continued to be implanted, approximately 1,300 of which were shipped from CRM's in-house inventory and the remainder in the possession of the sales force and in hospital inventories.[7]

As an attorney for someone suing the company might put it, with great sarcasm, mimicking their reasoning, "Replacing a flawed defibrillator with an equally flawed defibrillator is surely not worth the risk of an operation."

Guidant made at least two unconscionable decisions:

1. not to inform patients and their physicians of the flawed defibrillators that had already been implanted, and
2. to continue to sell the flawed defibrillators, knowing full well that they were flawed, knowing that physicians and patients could not

> know they were flawed, and knowing that the devices would put those new patients at risk of death when they failed.

It was more than a little disingenuous for Guidant to continue to sell the flawed defibrillator while claiming that it was riskier to replace the flawed device than to leave it in place. If the risk of replacing the flawed devices was greater than the risk of leaving it in place, surely the risk created by operating to implant a flawed device must be higher still since the risky operation creates a new risk for the patient because of the flaw in the device. So why would Guidant sell what it knew was a flawed device?

It is difficult not to think that Guidant was moved not to inform patients and their physicians because they wanted to sell the flawed defibrillators. It did not inform the patients or physicians so they could make up their own minds about whether to replace the flawed device because if it had informed them, it would have had to inform them that the replacement devices were equally flawed. They would not likely sell any and would presumably have to write off 4000 flawed devices at $25,000 apiece—a great deal of which was presumably profit since these devices are relatively simple and not that expensive to manufacture even if designed and produced correctly.

By the time Guidant announced the defect, two people were known to have died and over forty defibrillators had failed. Over 29,000 were at risk of their defibrillator failing just when it was needed. They thus faced that unfortunate choice: keep what is there and hope it works when it is needed, or have yet another operation to replace the defibrillator for another that may or may not work properly.[8]

Guidant's morally unconscionable behavior has had another effect, that is—the loss of trust that Guidant is concerned about the health of patients in need of a defibrillator and a subsequent wonder about the industry in general. Guidant was willing to write off the health of patients in place of writing off its flawed devices, and if Guidant was willing to do that, what assurance do patients and physicians have regarding any defibrillator or, indeed, any other medical device?

The engineers who designed the defibrillator were equally at fault for failing to think through how it was to be used and failing to ask themselves a simple question, "Will the parts withstand implantation?" If you are designing something that is to be used in a hostile environment—clothing for use by those fighting fires, for instance—it is irresponsible not to test it in that environment to be sure that it can perform its task. Selling flawed defibrillators is as unconscionable as selling clothing for firefighters that ignites upon contact with fire.

The possible harm from the flawed device is significant—death from a heart attack. It is particularly galling that the source of the harm is the very device that is supposed to save your life. What Guidant continued to sell was a false sense of security.

Without the details about any of the internal workings of the company, we cannot know exactly what kind of moral problem we have here. For all we know, this may be a situation where competent engineers wanted to test the device but were prevented from doing so by management. That is not an implausible hypothesis given Guidant's apparent moral climate. But whatever the details, we do know that the device should have been tested in situ.

This is an important lesson, one that needs to be emphasized because it has not been learned. A "new way of connecting defibrillators to the wires" has been developed, but it was not tested for how it will work in humans. The Food and Drug Administration said that no testing was necessary because "the new wiring connectors are simply a design modification and not a new technology." The history of failures suggests otherwise.

It would perhaps be more accurate to say that the FDA approved testing the new method of connecting wires by waiting to see what happened after the defibrillators with new wiring were implanted in patients. This is an odd mode of testing a product, but it seems the preferred procedure and explains why so many drugs, for instance, are recalled several years after their introduction because they failed to work or caused significant harms.

We now know about one of Guidant's flawed defibrillators, but the problem was not an isolated incident. Two other models had similar problems of short-circuiting, and Guidant ended up recalling at least seven models.[9] Medtronic, another maker of defibrillators, introduced a new thin wire connector in 2004 that "began to fracture and fail at an unexpectedly high rate. By the time they were recalled, they had been implanted in some 235,000 patients," putting all at risk.[10] That number makes the 29,000 put at risk by Guidant seem like only a minor catastrophe.[11]

We should add that it is difficult to assess the risk to heart implant patients because we do not know how many have died because of a failure of their defibrillator. The number of deaths that we know occurred because of a failure with a defibrillator is probably significantly smaller than the number of deaths actually caused by failures. The defibrillators are mostly implanted in older people, and when they die, the cause is attributed to heart failure, and no autopsy would standardly be done to determine if the defibrillator failed. So we do not know even roughly how many have died because of a flawed device. Without that knowledge, we have no way of assessing the risk of keeping a flawed defibrillator versus getting a new one. No one can answer the question, "What is the chance that my defibrillator will fail?" So Guidant was in no position to claim, as it did, that the risk of replacing the device outweighed the risk posed by the defective device. We do not know what the latter risk was, and the Food and Drug Administration was in no position to claim that because a new device is simply "a design modification and not a new technology," it is safe. The most it can say is that the new version is as safe as the previous models—which is not to say that it is safe.

The Cadillac trunk, the X-ray machine, and the defibrillator are examples in which something is wrong with the design solution the engineers adopted. It is not that the artifacts will not work. Anyone testing them will find that they work just fine. The trunk will close as it is supposed to close; the X-ray machine will close down to the table as it is supposed to; and the defibrillator will send the charge it is supposed

to send when activated. That is part of the problem. When tested in isolation from the situations in which they will be used, these artifacts seem perfectly fine. Put into the situations in which they will be used, enough will fail to work as they were designed to work and so cause unnecessary harm, including death in the case of the defibrillator.

The problem is that the design problem for these artifacts was not fully articulated. The engineers needed to develop a defibrillator that could withstand implantation and still work, software that would require that the X-ray table be empty before it could close down, and a trunk mechanism that would not be so likely to break if the trunks are closed as we are all so used to closing trunks. Expand the description of a design problem to include how a solution would be used, and you can protect against such failures. Think here of that odd toothpick that was to fit on the end of one's tongue. It is difficult to imagine that solution being thought viable once we imagine anyone having such a sharp object on their tongue being dislodged and accidentally swallowed.

All these examples—the Cadillac trunk, the X-ray machine, and the defibrillator—are examples of failures to think through how these artifacts will be used. These are all examples of how harms are caused to those who are to use the artifacts realizing the design solutions. At a moral minimum, engineers are responsible for ensuring that their designs do not themselves cause unnecessary harm, and yet that is just what these artifacts do when put to use.

But in restricting ourselves to examples of how artifacts are to be used, we should not forget the other ways in which design solutions can cause harm. We have picked these examples because they are clear and most clearly make the point that solving design problems requires more than simply coming up with a grand solution, however creative. It requires thinking through the potential harms realizing that solution may introduce, and those harms, as we shall see in the next chapter, are not limited to those created for those who use the artifact.

7

Harms and Design Solutions

§1. Unprovoked Harms

We have been focusing on artifacts whose use provokes harm—the autopilot software and the X-ray machine that crushed the patient. There is no doubt about the nature, magnitude, or gravity of the harms—people died, an aircraft was lost—and no doubt about the engineers being responsible for those harms. They designed artifacts that would cause mistakes for even the most intelligent, well-trained, and highly motivated user, and so they are morally responsible for the harms their flawed designs caused.

Yet, as I have said, these examples provoke too narrow an understanding of the harms engineers ought to cull from their design solutions. Not all harms are provoked. Some occur without any help from us at all. It was not any error on our part that caused many Fords to burst into flames. Letting off the brakes caused a small vacuum in the brake lines, and the vacuum caused the seal to invert, weakening over time and letting in brake fluid that corroded the wires.[1] The switch received power whether the vehicle was on or not. The corroding wires would overheat, igniting an electrical fire—even when the vehicle was parked. It was not any error on our part that caused the treads on many Firestone tires[2] and, later, Chinese-made tires to separate, causing vehicular accidents and driver deaths.[3] It was no fault of ours that millions in the Northeast, in the United States and Canada, experienced a massive blackout in August 2003.[4]

Not all of these examples are obviously the result of engineering mistakes. The problem with the Chinese tires was that the

manufacturer decided to leave out the gum strip that keeps the treads from separating. It is difficult to imagine that such a decision would be approved by any engineer knowledgeable about tires. It is much easier to imagine the decision being driven by the manufacturer's desire to cut costs and increase profits. That decision raises a question about what responsibilities engineers have when the companies they work for make decisions that engineers ought to find irresponsible. How far into the manufacturing stage does the responsibility of an engineer extend beyond providing a design solution to a problem?

In any event, the examples illustrate well how engineering permeates our lives and why it does not take an error-provocative design to raise an ethical issue for engineers. The range of possible harms, the gravity of those harms, the kinds of harms, and the numbers of those affected by these various harms—all are missed if we only consider those design solutions which provoke errors.

We will consider in this section two examples of harms that require no mistakes on our part. The examples are both drawn from that rich source of problematic design solutions, the vehicles we drive.

1. The clutch pedal: In Mazda RX-8, the interior edge of the side wall to the left of the clutch pedal curves in to form a lip at just the height of the pedal top. The lip is so close to the top of the pedal that when you try to push the clutch petal down to shift, your shoe gets hung up on the lip unless you are very careful not to push the clutch down in the center, but on its right edge. If you fail to do that, your foot stops before it gets started. The lip is a barrier to pushing in the clutch. If, as you start to shift, you move your foot farther over toward the right to avoid the lip, you can end up putting on the brake when you try to shift. Only if you are lucky enough to have very narrow feet can you shift gears in this Mazda without difficulty.

It is not as though it is the user's fault that the clutch pedal causes problems. Some people have wide feet, some have narrow feet, and it would never occur to us to fault the one or the other for the widths of

their feet. There is no doubt an average width, but it appears that even someone with a foot of average width would have trouble using this clutch pedal, and it is not as though a user missed a sign. This Mazda example is like the Cadillac trunk in that neither sends a misleading signal to the driver or user. Neither sends any signal at all. We have no warning of anything problematic.

This problem of a problematic artifact that catches us by surprise is, unfortunately, all too common. Here is another one.

2. Airbags: When engineers strive for foolproof design solutions, they are not just trying to stymy fools. They are striving to produce a solution which will ensure that no operators are harmed by the artifact. The first-generation airbags are an unfortunate example of how engineers, in trying to make drivers and passengers safer should an accident occur, put some at much greater risk, did so without any warning to those they put at risk, and did so in a way that was biased.

Airbags open with a force powerful enough to harm those who sit within ten inches of the bag or whose fragile body parts—heads, for instance—are at the height of the bag. The first-generation airbags deployed in less than the blink of an eye, at about 180 mph.[5] The bags were designed for "the norm" so that, presumably, it would protect the most number of drivers—those at the norm and, with diminishing effectiveness, those on either side of the norm. People at the norm would be just the right weight and just the right height so their legs would be just the right length to sit at just the right distance from the airbag so that when it deployed, they would not be so close as to be hit by the airbag as it was inflating, but also not so far away that they would slam into the airbag after it had already inflated. Such "normal" people would be the right distance away to move forward into the airbag just as it finished deploying so that it would gently cradle them as it stopped their forward motion.

Modifying the explosive force of the airbag, or the size of the airbag so that it could cover a larger area, would not change the fundamental

problem: drivers come in such various sizes and shapes that one size cannot fit all of them. The norm was determined by height and weight, and the presumption, apparently, was that they were sufficient to determine the length of a person's legs. The length of one's legs is the variable at issue when we adjust our seat nearer or farther away from the pedals—and thus nearer or farther away from the airbag, on the steering wheel. The assumption that height and weight are sufficient puts to one side tall people with short legs and short people with long legs. The result is that designing for the norm ensures that some are going to be well served and some are going to be put at greater risk. That is an unfairness built into trying to make some safe with an artifact not nuanced enough to protect everyone. Some will be put at greater risk, or at the least not made safer, so that others can be safer.

As we look at individuals who weigh more or less than the norm, are taller or shorter, or who have longer or shorter legs, we eventually reach the ends of the bell curve and find those who are so short or have such short legs that they must sit right up next to the airbag in order to drive and those who are so tall and have such long legs that they must sit far away in order to drive. Those tall long-legged people will hit the airbag after it has fully deployed and hit it with a fair degree of force, causing harm. The more they weigh the harder they will hit it. The short short-legged people will be hit by the airbag as it is deploying, their chest or head getting the full explosive force. They are thus at great risk of being killed by what was designed to save the "normal" person. Their weight will not matter much to how quickly they move toward the bag since they will not have time to move much distance at all, if any, but the larger they are, the more quickly they will be struck by the exploding airbag. So what was chosen as "normal" matters enormously.

The norm chosen was the 50th percentile for men. The airbag was "designed to protect an unbelted adult male at the 50th percentile of body height and weight in a severe frontal crash."[6] When the engineers chose that norm, the 50th percentile for men was roughly the 95th percentile

for women. So the first-generation airbags protected most men, but a much smaller number of women. More accurately, what protected most men put a good number of women at greater risk—those who are short in comparison to the male norm and those with short legs who must sit close to the steering wheel to drive. The choice of that norm gives new meaning to the principle of courtesy, "Ladies first."

Suppose a 170-pound 5-foot 9-inch-tall male drives his car head-on into a car driven by a 98-pound 5-foot woman. He is as well protected as possible by the airbag deploying in that "severe frontal crash" because those males in the 50th percentile weighed 171.3 pounds and were 68.7 inches tall when engineers made their initial choice.[7] She is likely to be severely harmed because of the airbag, which should protect her. It is only because she is so far down the bell curve from the 50th percentile for men of normal weight and height that what protects him can injure or kill her. That seems unfair because the engineers' choice is biased against women to the advantage of men.

Yet choosing that norm might be just the thing to do, to minimize the harm to most drivers, if males were the drivers in the vast majority of accidents. We would need to look at the evidence about how many males are involved in accidents. Whatever the evidence, we are making a value choice in determining which group to protect.

Instead of choosing the 50th percentile of males, why not choose the 50th percentile of drivers? Or the 50th percentile of those who have been in accidents? Are those in the 50th percentile of height and weight also in the 50th percentile of those in accidents? Perhaps smaller men are involved in more accidents than larger men. What about choosing as the relevant group not those involved in accidents, but those who cause accidents? Or what about protecting those who are involved in accidents they did not cause, the victims of accidents? What is the 50th percentile of their height and weight? Or perhaps we should take as the relevant group those who are severely injured or killed in accidents.

Height and weight are the relevant variables for determining the explosive force of the airbag and its size once deployed, but some other

variable—for example, drinking habits—may be better correlated to accidents, and if so, we would then need to determine the height and weight for the 50th percentile of those who drink and drive. Again, we have many possibilities for what may be best correlated to accidents—the age of the driver, the training a driver has had, the driver's use of legal or illegal drugs, and so on.

The engineers had many choices, and any choice is value-laden—as the various examples suggest. Why put shorter women at greater risk of harm if it turns out that they are more likely to be victims of accidents caused by those who drink, say? They then are hit twice, once by drunken drivers and again by an airbag whose design puts them at greater risk of injury or death. What is the justification for protecting the 170-pound 5-foot nine male if that should turn out to be the median for those who cause accidents? Why protect best those responsible for the most accidents—if that is the case?

In short, no matter what the evidence we would need to tailor our choice of an airbag, any choice we make about whom to protect and whom to put at greater risk is a value choice. Either we value protecting those who cause accidents over those who are victims, or we value protecting those who do not drink and drive over those who do, or we protect women and children first over larger males, and so on. No matter what our choice, we provide greater safety for some at the expense of others, and the criteria for who falls into each of those two groups will reflect a value judgment we have made—consciously or not. As suggested, the engineers might have chosen the median for all drivers, for instance, male and female alike. They may then perhaps have made more drivers safe, depending upon what the evidence shows, and certainly would have saved themselves from the charge of sexism.

To note the obvious, their choice did not produce an error-provocative design. The drivers at the ends of the bell curve did not need to do anything, let alone make a mistake, to be subject to great harm. Engineers are morally obligated to avoid error-provocative

designs, but as these two examples show—the Mazda clutch and the airbag—they are morally obligated to cull harmful features out of their design solutions, if they can, whether those features provoke the users into making mistakes or not.

§2. Missed Signals and Other Harms

A design is a sign. Any design solution sends a signal, intended or not, about how it is to be used. The things that can go wrong mirror all the ways in which we can fail to communicate with someone. We shall examine only a few instances of this kind of failure.

1. No information: Some artifacts provide no information to the operator when most needed. We mentioned the automatic faucets that turn on when you put your hands beneath the faucet. We find them in airport restrooms, for instance. They malfunction, but nothing tells the people wanting to wash their hands that the faucet does not work. This is particularly galling to those who have not seen such a faucet before. They are unable to make it work and assume they must be doing something wrong since others are succeeding where they are failing, but cannot for the life of them see what they are doing wrong.

The same kind of problem of an artifact giving us no information when we need it arises for the double doors we find in, say, banks. Typically, one door is unlocked—the one on the right as you come in. The other is fastened by bolts top and bottom on the inside edge of the door. We go into the bank without any difficulty, but when we try to come out, we get stuck at the door we would normally use—the one now on our right. We get knocked back because it is locked. We learn from experience to be cautious in exiting such places so as not to injure ourselves.

2. Useless information: Some artifacts provide useless information. Here is an example received while trying to send email (Figure 10).

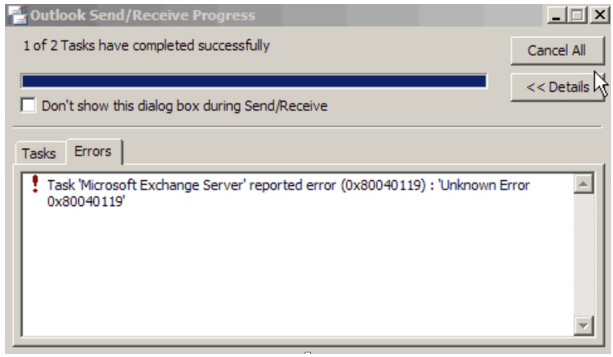


Figure 10 Notice of Microsoft Exchange Server error. Screenshot by Wade L. Robison.

What is fascinating about this "Unknown Error" is that it has a number: 0x80040119. Presumably other unknown errors have other numbers—which suggests that they can be tracked down and identified, though not by you, the user.

This sort of thing is annoying, to say the least, and software is notorious for problems like this. We are all told we should back up our files. So a friend of mine bought a backup program and proceeded to set it up to back up a bunch of files—a batch backup. When he clicked the "Batch Backup" button, a box popped up which read, "Nothing to back up" with an "OK" button to click. Not being able to figure out why he was being told there was nothing to back up when he had lots to back up, he clicked the "OK" button, only to have yet another box appear: "Nothing to back up" it read, with an "OK" button to click. He clicked it, and another box appeared with the same message and the same button. He found himself at the edge of an infinite regress.

He later discovered that when the software said, "Nothing to back up," it was not referring to what needed to be backed up. It was as though he had two boxes, one with stuff in it and one without. He was trying to move the stuff from the first box to the second, but was told, "There's nothing there to move." He had stuff in the first box and so knew that was not true, but it turned out the software was telling him there was nothing in the second box to move. Since he was not moving anything from the second box, he did not need to be told there was

nothing in it. It is incomprehensible why the program would stop and apparently tell him he had completed his task when he had not done anything at all except click the link. And it is incomprehensible why it would then give him a chance to click "O.K." It would seem that all it can tell him is that he successfully clicked the "Batch Backup" button.

When we read something we do not understand, we can sometimes figure out from the context what must have been meant. But with this "information" from the backup program, we have no idea what is meant and no way to figure out what could have been meant. Worse, we cannot proceed to back up our files because we cannot get past the incomprehensible message that we do not have anything to back up—when we obviously do. Every time we click on the button to back up our files, we are stopped dead in our tracks with incomprehension. The only thing to do seems to be to click on the button again, and that takes us nowhere. So the information provided was useless for my friend—and harmful besides since it was not until long after that he was able to figure out how to get past that dead-end in the software so he could back up his files.

This software example shows how an artifact can provide us with information we cannot use. The way this artifact fails is not the only way an artifact can fail to provide helpful information. Many of us had had the problem of trying to figure out the instructions to put together a child's toy on Christmas Eve, unable to make heads or tails of the "information" provided—with a tab marked "A" to be put in a slot marked "A" when the only slot in the diagram provided is marked "a" and does not seem quite the right spot anyway. And many of us have had the problem, which gets worse the worse your eyes become, of trying to decipher the exceedingly small print that sometimes gets printed on instructions—an offer for an extended warranty in five-point font underneath the line for your signature, saying that when you sign, you are thereby authorizing the company to charge your credit card that amount every year. The print provides the relevant information, but the font is so minute that you are likely not even to notice that it says something, let alone be able to read it without searching out a magnifying glass.

(3) Ambiguous information: We are all familiar with situations where someone says something ambiguous. We take it one way and

proceed accordingly when we should have taken it another way. After his loss in the 1962 California gubernatorial election, former Vice President Nixon was asked whether he would run for president. He famously said that he would not run for any other office. Newspapers headlined that he was quitting politics, but what he said was ambiguous. He could just have easily been saying that he had made a mistake in running for some office other than the presidency, a mistake he would not repeat. And that is in fact what he apparently meant.

Artifacts can give equally ambiguous signals. In one national brand store in the city near me, two sets of doors open to let in customers. Both are opened automatically and so signal to customers that they need not concern themselves with the doors, but can walk in and continue talking, looking after children, thinking about what you are there to purchase. Unfortunately, the second set of doors opens only after you have walked through the first set, and on the other side of those doors, set in the middle about three feet back, is an electronic post that emits a signal if someone tries to leave without paying for something. The post is just high enough to do serious damage if you walk into it, but not high enough to be particularly noticeable to someone otherwise occupied.

Here it is the configuration of these objects that creates the ambiguity. I can attest from my own experience that it hurts to walk into the post. It would have hurt even worse if I had been rushing into the store. I took seriously the signal the automatic doors gave me: "Welcome, come right in! Don't worry about a thing! We'll even open the doors for you!" Placing the electronic post just on the other side of the second door, with no warning to those walking, is similar to enticing someone to do something and then causing them harm if they do—a sort of entrapment. Whether an engineer was involved in figuring how out to configure these artifacts, we know that even a halfway competent engineer would not have permitted such a configuration.

(4) Other bad signals: Some artifacts are designed to send us signals. A stop light tells us to stop, go, or proceed with caution, using red at the top, green at the bottom, and yellow in the middle. A stop sign tells us to stop, and as the examples of different stove top configurations tell us,

artifacts signal to us whether designed to do so or not. In the worst of cases, an artifact's signal provokes an error even for the best, those we would presume most adept at understanding such things because they are the most intelligent, the most highly trained, and the most motivated. But there are many other ways in which an artifact's design can mislead.

Cars and trucks provide a raft of examples of how things can go wrong. The problems range from an engine so placed in its compartment that one cannot change a spark plug without taking the engine out to a supposed safety feature that will not let you start a car unless your seat belt is fastened. Fastening the belt completes a connection and leaves you at the mercy of wires going through the door that flex each time the door opens and closes and eventually break, leaving you unable to start your car. I had a VW Rabbit with that "safety" feature. I found myself one day far from home and any service station, unable to start my car—until I got so upset I slammed the door shut. I sat there and then tried to start the car one last time. It started, much to my amazement. I had apparently reconnected the broken wires when I slammed the door. Scratch a mechanic and you will find a raft of various examples of some engineering mistake or, at least, bad judgment.

a. Shoulder harness: My 1992 Subaru SVX had a harness that attached to the door so that opening and closing the door opened and closed the harness. Close the door and the harness is across one's chest. The design is awkward since when the door is open, the harness is directly in front of your chest, making it difficult to lift anything out of the car. The design is also dangerous. Both the harness strap itself and the instruction booklet for the car make this point. A tag on the harness strap reminds you to fasten the seat belt or face serious injury, and the instruction booklet says that you may experience "severe head trauma" if you do not fasten your seat belt. Why?

If you do not fasten your seat belt, the harness will impede you moving straight forward in an accident, but not from sliding down. As you do, your trunk and head will go down and your chin will catch on the harness. If the impact is severe enough, the edge of the harness can sever your neck.

The problem is that closing the harness across your chest makes you feel safe. You are strapped in, after all. I almost always had to ask or remind passengers to fasten their seat belts, and they would inevitably reply, the first time, "Why? What's this?" I would say, "That's the harness. You still need to fasten your seat belt." So you think you are being made safer with the harness when you are being put at greater risk.

One oddity about this arrangement of harness and seat belt is that commonly a seat belt and harness are continuous so that by fastening your seat belt, you fasten your harness. The arrangement in the Subaru does not save any effort. You still need to reach down and fasten your seat belt. That may be another reason why people are puzzled that they still have to do something. It seems unreasonable.

I am not suggesting that the Subaru engineers intended to cause passengers problems with their design. I suspect that they did not think through what complications would ensue from having a combination of an automatic harness and a seat belt that needed to be fastened by hand. The arrangement was unnecessary.

b. Shower faucets: Plumbing is also a rich source of misleading signals. Scratch someone who showers, and you will find stories of mishaps. Almost everyone has stories to tell. I am used to shower fixtures that turn on when a knob is pulled out of the main faucet, diverting the water from the faucet to the shower. I found myself in a shower stall in a motel where there was no knob to pull. Indeed, I could not see how to turn the shower on. I then noticed a handwritten sign on the wall next to the shower that said, "Pull the ring down!" Others had also had this problem.

So I looked at the fixtures, hunting for a ring—without success. I then thought that perhaps, like the sign, the ring was outside the tub. So I looked around outside. No ring. Eventually I found what might be "the ring" at the tip of the tub faucet, but it would not move. Only by sitting in the tub was I able to get a purchase on it, but it would not come down. After much struggling, I was able to turn it counterclockwise. I was then able to pull it down—whereupon I, and the bathroom floor, got drenched as the shower water came on full blast.

This is a nice example of at least three different problems we can have with engineering artifacts. As with the Cadillac trunk, nothing about the artifact gives us a clue about how it operates. So the first problem is that we cannot tell by looking how the thing works. Second, we bring different histories to artifacts and thus habits of use that can interfere with our using an artifact that works in a different way than our history has primed us for. That is why, when asked, different people give different examples of problematic plumbing fixtures and why some may strike some of us as not problematic at all. A third problem is that we bring different bodies to the artifacts. My mother would not have been able to take a shower in that motel. She would not have been able to turn the ring. Perhaps a more telling example concerns the "child-proof" pill containers she found elder-proof. I have no difficulty with them. She had severe arthritis; I do not. The trade-off in designing child-proof containers is that anyone who has difficulties pushing and turning at the same time will find the containers proof against their opening them.

Over time problems that arise in original solutions are generally resolved by modifications in the artifact. The artifacts in our everyday lives are generally themselves the result of evolutionary pressures where problematic designs are weeded out or changed to become less problematic. Pressures work against this evolutionary process, of course. Companies want to differentiate themselves by having a different product, and progress would halt if we did not constantly push the envelope of design, creating new ways of doing things and so creating new problems to weed out. But engineers need to consider habits of use as they push the envelope of design.

§3. The Artifact: Sustainability, Recycling, and Remanufacturing

In solving design problems, engineers make decisions about the artifacts that realize their design solutions—what it is to be made of,

what process will most easily produce it, whether its components can be recycled or remanufactured once the artifact has run its natural life, whether the components can be safely disposed of, and so on. Ethical considerations not only enter into the idea for a design solution, that is, but enter as well into decisions about the artifact that realizes the idea.

Discussion of the problems that call for sustainable solutions requires a book in itself, but we can get a sense of the harms that can occur, and of the difficulties in precluding further harms, by considering the following examples.

(1) Mercury: Designing artifacts with mercury in them—electrical switches, for instance, or older kinds of batteries, or fluorescent light bulbs—puts us all at risk when these artifacts are trashed. Mercury is a poison that can harm our brains, our kidneys, and our lungs. The more mercury in our products, the more likely it is that we will end up with mercury in our food—in fish, for instance, but also in crops grown in soil contaminated with even small amounts of mercury. Mercury accumulation is cumulative, and so someone with continued exposure from infancy to old age has a greater risk of significant harm. It would clearly be best for engineers to avoid designing artifacts requiring mercury.

Mercury in products would not be a special problem were it easy to isolate and easy to recover so that little, if any, escaped into the environment to poison our water and soil and us. But once mercury is in artifacts, it is difficult to prevent its escape into the environment. We might think of making the companies that produced the risk of mercury contamination responsible for reducing the risk, but no company is likely to accept easily the burden of removing it.

A rather depressing case in point concerns the mercury in the 36 million trunk convenience lights and antilock brakes in vehicles built prior to 2000. Roughly half of these vehicles are General Motors products, and GM joined a partnership in 2005 to recover the mercury. Because of that program, 2.5 million switches were recovered, containing 6500 pounds of mercury. This was a good program, with a good track record, and relatively inexpensive, costing GM less than a million a year.

But that was the old GM. The new GM resulted from the bankruptcy of the old GM in 2009 and claims that though "GM's former entity remains a member of the partnership," the new GM "has never produced vehicles with mercury switches and has no mercury switch responsibility under the terms of the bankruptcy court order."[8] We have entered a wonderland of doublespeak. To say that "GM's former entity remains a member of the partnership" is disingenuous in the extreme since it no longer exists and cannot contribute money. In refusing to take responsibility for the vehicles manufactured by "GM's former entity," GM's current "entity" will increase the risk of mercury poisoning for all of us to save less than a million a year.

Still, it is difficult not to admire GM's new entity for its disingenuous way of shifting responsibility so it no longer has to pick up the costs associated with GM products or, rather, products made by a company called "GM" that no longer exists. By calling the former GM "GM's former entity," it is able to keep the name GM and perhaps make use of what good its "former entity" has done while shirking any costs associated with products it—or, pardon us, its former entity—produced. It is easy to figure out why GM's new entity might want to refer to its former self—or, rather, to paraphrase its locutions—the "former entity also known as GM" in that way.

2. Throwaways: When we cannot recover or recycle the parts from an artifact, we are condemned to all the attendant harms that come from what we must bury or burn—polluted water, air, and soil—as well as those attendant on having gotten the original raw materials and the new harms produced in getting more raw materials to make more throwaways.[9] We have come to live in a world of artifacts that cannot be repaired—toasters and coffee makers that must be tossed, wristwatches, cell phones, and TVs that cease working or are replaced by newer models, cars that begin to go bad after 80,000 miles. The list is long.

Even if an artifact could be repaired, companies make replacement components so expensive it is not worthwhile buying one. Brother makes a laser printer that will come to the point of needing a new

drum, as they all do, but Brother charges $140 for a new drum. An updated model of the same printer costs $159. So for $19 more, you can get a new improved laser printer with a new drum and ink cartridge.

Planned obsolescence is profitable. Throwaways must be thrown away, to be replaced with new throwaways. Few strategies could be worse for us or our environment. This is particularly so when the obsolete artifacts contain harmful substances or when the cost of removing the artifacts is high enough—old tires, for instance—to tempt more than a few into dumping them wherever they can. We end up with health hazards we could have avoided.

One solution is for engineers to solve design problems in ways that permit the artifacts that realize those designs to be repaired if broken or, when they cannot be repaired, to be reused or remanufactured. Even if manufacturers continue to produce throwaway artifacts that cannot be repaired, or repaired easily, we can bypass some of the harms involved by designing them so the materials and/or parts can be salvaged.

For example, by 2011, at least, Mercedes had "a recyclability rate of 85 percent and a recovery rate of 95 percent."[10] The company made a commitment in the early 1990s "to implement a total vehicle recycling program with two main elements: vehicle design and vehicle recycling." The "design efforts . . . include choosing environmentally compatible and recyclable materials for components, reducing the volume and variety of plastics used . . . and avoiding composite materials as much as possible."[11]

We might wonder what constitutes the 5 percent that cannot be recovered or the 15 percent that cannot be recycled. It is not the batteries. It

> [t]urns out that the 12-Volt battery is the most recycled product in the world, according to the U.S. Environmental Protection Agency. In the U.S. alone, about 100 million auto batteries a year are replaced, and 99 percent of them . . . are turned in for recycling. Roughly 97 percent of the lead in a 12-Volt battery can be recycled. The electrolyte, especially sulfuric acid, can be neutralized, repurposed, or converted

into sodium sulfate used in fertilizers or dyes. Even the plastic case can be ground up and reused.[12]

What we do with batteries is a good model for what we should try to do with every artifact.

The design and recycling program Mercedes began was driven in part by the European Union requiring manufacturers to take back what they produced after the useful lives of their products was over, but Mercedes also had financial incentives. It saves money if an artifact's parts can be recycled and recovered. If GM's "former entity" had been so prescient, it would not have polluted our lives with over 90,000 pounds of mercury.

The solutions to these problems will depend on more than engineers, of course. We need policies in place that encourage sustainable development and provide companies with incentives to eschew short-term profit and pursue long-term goals less inimical to us and to our environment. We will not proceed with those matters here, but the examples given are illustrative of the kinds of issues engineers need to consider if they are fully to fulfill their obligation not to cause unnecessary harms.

§4. Other Harms

The harms engineers can cause are as extensive and varied as the various interests we have. We have interests in living a long life, in living it without serious injury, in being fairly treated, in being able to use technological conveniences without inconvenience, in driving our cars without unnecessary risk, in climbing ladders that remain stable as we mount them, and on and on. A harm is a setback to one of our interests, and if the setback is serious enough, the harm raises to the level of ethical concern.[13]

We will not try to draw a line between trivial harms, however annoying, and those that raise to the level of moral concern, and we

will also not lay out in any systematic way the various kinds of harm that engineers can cause through faulty design solutions or map out the potential harms an engineer must consider, upstream and downstream, in solving any design problem.

Every design solution has implications upstream and down. We can cause harm through how we obtain what we need for manufacturing and for how we create the artifact once designed. We can cause harm through how we produce substances like various kinds of plastics we use in our artifacts. We can cause harm going from a design solution to a manufactured artifact, and we can cause harm in how we handle an artifact once its useful life is over.

The design solution determines the nature of those harms as well as their extent, and since the sequence of events determined by that solution is so extensive, we may think of engineers as stewards of the world. It is their design solutions that determine the features of that sequence and so determine what shall be mined for the resulting artifact, what chemicals will be necessary, and the nature of the waste that results—matters of environmental and moral concern.

Some design solutions will cause more harm than others equally effective, and since unnecessary harms ought to be avoided, the choices engineers make about how to solve design problems matter enormously to whether our environment is unnecessarily harmed. That is why engineers are stewards of the world.

Every item in the sequence that leads up to an engineering design solution and every item in the sequence that follows after the solution's realization in an artifact is as much an object of moral concern as the process of going from a design problem to a design solution. Moral considerations enter that sequence at every point. The paradigmatic example of how harms enter the design solution is an error-provocative design, a solution which will ensure that even the best and brightest will cause harm, and we can easily see how unnecessary harms can enter the sequence at the beginning all the way through the end. Any particular sequence is itself an artifact, that is, the result of choices that need not

have been made had another design solution been chosen to create a different sequence.

Engineers are to avoid not just those designs that provoke errors, but those designs that are unnecessary and harmful, whether the harms they produce are the result of an operator being provoked into a mistake or not. What matters is not that an operator be an agent in producing harm, but that the harms produced by an engineering artifact could have been avoided by a different design solution.

We have considered a variety of harms caused by engineering mistakes, and it is easy enough to find other examples of problems with the big artifacts of engineering—the Hyatt-Regency in Kansas City,[14] the Big Dig in Boston,[15] the flood walls in New Orleans,[16] and the Interstate Highway bridge in Minneapolis.[17] As we all well know, things can go wrong with engineering artifacts, sometimes causing great harm. In some cases the engineers are responsible; in some cases, not. But we do not need to look at complex engineering projects to find artifacts engineers have designed that cause harm. We can look, as we have, to the simple artifacts that could readily be the work of a single engineer.

In sum, an engineer is making a wide variety of choices in solving a design problem and must be cognizant of what other choices follow from choosing a solution. The engineer must thus think through various ways in which possible solutions might work when instantiated in an artifact, make the necessary calculations for each possibility, probe the ways in which this or that solution may fail and trace out the consequences of potential failures to determine which design would have the most extensive and expensive ones, which the worst failure rate, which the least damaging, which is the easiest and least expensive to manufacture, to ship, and to store, and so on. Engineers need to trace out possible design choices to see where they would lead. That requires the engineer to look downstream to see what happens once the design solution is realized in an artifact and upstream to see what is needed to manufacture the artifact. Each of the decisions an engineer makes regarding a design solution can introduce the potential for harm downstream or upstream. None is necessarily easy.

All are moral choices—as we shall see in looking at a few examples of design solutions.

§5. What Counts as a Design Solution?

Engineers are no different than other professionals in second guessing the solutions they have found for the problems they face. We often think back over what we did to solve a problem and find something we could have done differently that would have been better. It is at the heart of what it is to be a professional that we presume that we could do better than we did. Writers think about how they could have said something in a different and better way; surgeons think about how they could have cut an operation's time and benefitted the patient by using a different method; engineers think about how some alternative solution that had not occurred to them might have been better.

So what counts as a solution to a design problem always carries with it, or ought to carry with it, a tentativeness. We strive, or ought to strive, for the best, and that carries with it the admonition, "Perhaps we could do better!"

As we have seen, it is not difficult to provide examples of design solutions that could have been better. I will provide one here that could have been much better and then provide an example of a solution which strives to be the best. These examples both have to do with signage, a wonderful source of examples for what can go wrong.

1. Road stripes: It is common problem to handle heavy traffic turning at an intersection to have two lanes for turning, and the accidents that subsequently occur are predictable. A vehicle in one turning lane turns into the other lane and hits the vehicle there. Such accidents are most frequent when a new turning lane is added where there had only been one, when drivers do not realize there are two, and when drivers fail to see the dotted lines between the lanes. Fender benders are the most frequent result because the vehicles are turning relatively slowly, but they cause harm, obviously, in bending fenders and creating traffic jams.

One cure is to make the dotted lines between the lanes solid, the signal not to change lanes. That cure still requires drivers to pay attention and also presumes they will do what the law requires, stay in their lanes, but on the presumption that it would help, the highway department for Rochester, New York did just that for an exit off the interstate. When you take the exit to your right, it is one lane, but that one lane immediately widens into four, and the two on the left go underneath the overpass that carries the interstate.

The highway department did not just paint a solid line between those two lanes, but also on either side of those two lanes, preventing—or, more accurately, making it a traffic violation—to move out of the lane you were in, and the solid lines went all the way under the overpass to the road beyond.

I happened to use that exit just as the newly painted lanes were being opened up for use. I was in the lane farthest to the left, and I discovered that far from solving the problem of drivers shifting lanes, the lines aggravated it.

As is typical for exits off interstates, there is an entrance on the other side, and to enter the interstate from underneath the overpass, a driver has to get into the center lane, the one between the two lanes taking the traffic that has just exited from the interstate and the two lanes going in the opposite direction. But the solid lines to keep vehicles from wandering into other vehicles had been painted so that anyone using the lane I was in ended up in the center lane, the lane reserved for those going onto the interstate. I found myself unable to get onto the proper lane to continue on my way and ended up going back onto the interstate—in the direction from which I had just come.

I could not get out of the lane I was in without crossing a solid white line—a traffic violation, and, in addition, the next lane over was filled with those vehicles that had been in the other left-turn lane. Even if they had realized there was a problem, the drivers in that lane could not move over to the empty lane to their right because they too would have had to cross a solid white line.

I called up the county engineer after I went to another exit and got home. I explained what had happened. He said that they would just wait until the new stripes wore out and then repaint. I suggested that he would not have the luxury of waiting, that the county would be sued long before the paint wore out, and that he might want to go out and look for himself at the problems the lines were creating. He called back later and said that the lines would be painted over in black and new lines would be in place quickly. The problem was solved by the time I next used the exit several days later.

I presume that the problematic solution was a result not of the country engineer having made a mistake in locating the solid lines but of the painters misunderstanding what they were supposed to do—one of those problems that can occur as a design solution moves to realization. We can put that unfortunate initial solution at one end of a spectrum of solutions where it is easy to see how things could have been done better. Our next example is of a solution that is paradigmatic of how to do things right, using a series of experiments over a long period of time to hone a solution that creates a much safer environment for drivers.

2. Clearview: Signage is a continuing source of examples of how things can go wrong. From one-way signs that face each other at a dead-end street, leaving drivers with nowhere to go, to the incomprehensibly complex signs giving information about when a driver can park and when not, signs are a continuing source of misunderstanding. Some of the problems are just what we would expect would infect attempts to communicate—ambiguity, unclarity, grammatical infelicities that create confusion, and poor word choice that clouds the intended meaning. In addition, of course, features peculiar to signs can create problems. Those who read them must be able to make them out. Their distance from the viewer, the size of the font, how close together the letters are, the type of font—all these affect the ability of a viewer to make out what the sign says. If you put an unusual font on a sign, for instance, you are asking for someone to have trouble reading it. We get so used to certain fonts—Helvetica, Times New Roman—that a different font, especially

an unusual one, requires more care for us to be sure we have read the text properly, and requiring more care carries with it the increased risk that some will fail to read as carefully as necessary.

The problems of making out what road signs say are complicated by the speeds at which those who need to see them are whizzing by as well as by the various capabilities of those who need to see them. Can they read? Can they read fast enough to understand what a sign says? Can they see the sign? We know that one problem is "the amount of light reaching the retina of a healthy sixty-year-old is one-third that of a twenty-year-old."[18] So the dim light that does not bother a young driver may make it impossible for an older driver to see what a sign says. In addition, someone with poor eyesight, even with glasses, can have trouble with glare and light reflected on the glasses that interfere with making out what a sign says. The challenge is to create signage that is readable at a great distance, in different kinds of weather, to drivers with a wide range of capabilities going at high speed.

The Clearview project was a ten-year-long "research program to increase the legibility and improve ease of recognition of road sign legends while reducing the effects of halation (or overglow) for older drivers and drivers with reduced contrast sensitivity when letters are displayed on high brightness retroreflective materials." It also investigated "the ease of recognition of mixed case displays in lieu of all capital letter displays."[19] The project led to the Clearview font and to the use of mixed cases, for example, "Cincinnati" rather than "CINCINNATI."

The font is significantly different from any of the six different typefaces in Highway Gothic, the official font of the Federal Highway Administration. What is known as the E-modified font has generally been the font of choice from Highway Gothic. "In general," it is said, "the ClearviewHwy lowercase is taller, interior shapes of letters are more open to allow clear definition of each letter, and letter spacing has been designed to accommodate the needs of older drivers when used with both regular and high brightness sheeting materials."[20] The following shows the font's evolution and configuration compared to what has been the standard (Figure 11).

Figure 11 Clearview font. Credit: Meeker & Associates, Inc., and Terminal Design, Inc.

ClearviewHwy was created by Don Meeker, an environmental graphic designer who got interested in the issue around 1990, and James Montalbano, a type designer who worked on Meeker's original solution. As Montalbano put it:

> The fundamental flaw of Highway Gothic is that the counter shapes are too tiny . . . referring to the empty interior spaces of a typeface, like the inside of an "o." When viewed from a distance, and especially at night under the glare of high-beam headlights, the tightly wound lowercase "a" of Highway Gothic becomes a singular dense, glowing orb; the "e," a confusing blur of shapes and curved lines. Meeker puts it more bluntly: "They look like bullets that you couldn't put a pin through."

So Montalbano opened the type up, creating more space within the letters. "He understood that Clearview's success would come not from where its shapes are on the sign but precisely in where they are not—the open spaces in Clearview's letters are what make it so readable."[21]

Highway Gothic had never been tested to see how easy, or hard, it was for drivers to make out the font. The versions of ClearviewHwy were tested over and over again to ensure that each iteration was easier to see. As Montalano said, "Signs that you'd be hard pressed to read at 700 feet [in Highway Gothic] were legible at 900 or 1,000 feet," and for a stationary viewer there was "an approximately 40 percent gain, or 200 feet of added reading distance using a 10-inch-high letter on the demonstration panel."[22] A Pennsylvania Transportation Institute study showed significantly increased legibility for an early version of ClearviewHwy.

> For drivers traveling at 45 mph, that legibility enhancement could easily translate into 80 extra feet of reading distance, or a substantial 1.2 seconds of additional reading time. On a road with a posted speed of 45 mph, a driver [going at the speed limit] is traveling at 66 feet per second. With Clearview-Bold, the desired destination legend is recognized 1.3 seconds earlier (84 feet) and with greater accuracy, giving the person significantly more time to react to the information displayed.[23]

One crucial insight in developing the typeface is that we more readily recognize patterns created by a mixture of upper- and lower-case than signs in upper-case only. Even if we cannot quite make out the letters, we can recognize a pattern—"Chicago," say, in place of "CHICAGO." The other major insight was that by increasing the height of the lower-case letters, the amount of counter shape—that hole in the "a" for instance—is increased, thus increasing a sign's legibility.

What is admirable about Meeker and Montalbano is that they kept "returning to the font for minor changes: an adjustment in thickness here, a change in letter spacing there. 'Those guys are tinkerers,'" it was said. "They were always playing around, wondering how we could optimize it. We had something we called Clearview, but was there a Clearer-view? Or a Clear-est view?"[24] They assumed, that is, that the font could always be made better and kept working at making it better until they achieved a real breakthrough in legibility.

Highway Gothic, we now know, is surely a less than optimal solution to the problem of making signs legible to a variety of drivers going at high speed, and ClearviewHwy is certainly better because it is more legible and so gives drivers more time to make what may be quick decisions. But we should not presume that ClearviewHwy is the best we can do for road signage any more than we should presume that the highway department in Rochester, New York picked the best way to ensure that drivers not cross into other lanes when there were two lanes turning in tandem. What the ClearviewHwy project shows—clearly—is that things can be better than they were, and it is that general truth that engineers ought always to presume.

A design solution is a contingent choice, made at a particular time by a particular engineer or set of engineers, and at another time, with another way of looking at the problem, or another way of testing the results, or with a different engineer or set of engineers working on the problem, or with technological advances, a different and better solution may present itself.

At one point the US Department of Transportation decided to rescind its interim approval of Clearview, much to the chagrin of some, especially those over sixty, who have found the font significantly clearer than the Department of Transportation's Highway Graphic.[25] We can presume that cost was a factor. Highway Graphic is free, and Clearview carries a cost.[26] But Congress mandated that the Department reinstate its interim approval.[27]

§6. Value-Laden Choices

It should not surprise us that our choices can be value-laden. They reflect and embody values. We express our values in the choices we make, and some of those values are moral—because of who we are, how we have been trained, what we think or any other personal feature. Values enter even in seeing something as a problem, but I have put that to one side to argue that we find values embodied in design solutions if only because the design has effects when instantiated in an artifact that is introduced into the world, and those effects may be beneficial or harmful, or, obviously, both.

Seeing that ethical choices are embodied in the design solutions of engineers ought to change the way engineers look at what they do and so open up new or more careful considerations in design solutions—on what counts as a design problem (so that the way a product is to be used is taken into account, as it was not for Guidant's defibrillator), on what counts as a harm (so that engineers ensure that an artifact's parts can be recycled, that the entire process from manufacture to disposal be sustainable), and on what counts as a solution (so that it is always

assumed that things can be made better than they are, as the designers for ClearviewHwy assumed for road signage).

Seeing that ethical choices are embodied in the design solutions of engineers also ought to change our understanding of how to determine the bell curve of competence of engineers. We have focused primarily on what engineers ought to do *at a minimum*. The bottom line is that they ought to cause no unnecessary harm. That moral principle is at the bottom. Causing no unnecessary harm is the least a professional can do, and professionals in any discipline ought to be competent enough not to cause unnecessary harm. Engineers ought always presume, however, that both they and their design solutions could be better. The development of Clearview illustrates the sort of aspiration to improve that ought to be a hallmark of an engineer.

"Do no unnecessary harm!" should be complemented with "Strive for the best!" so we have a third moral feature an engineer should have:

3. **Aspirational:** Engineers should always strive to better their design solutions as well as themselves as engineers, improving on their past design solutions, learning from their mistakes and the mistakes of others how to avoid errors, keeping up with the latest engineering techniques, understanding how new materials can make for better solutions, and being dissatisfied, that is, with being merely competent.

Someone can be an engineer with no aspirations at all other than to be mediocre. No engineer need strive to be better to remain an engineer however much we may be saddened to see someone talented enough to be an engineer choose not to continue to strive to be better. At some point, perhaps, should engineering practice change rapidly, someone who fails to keep up will cease to be hired or even considered an engineer any longer.

However unlikely such a possibility may seem for engineering, we find this happening in other professions with some regularity. New technologies and discoveries can fundamentally alter the trajectory

of an entire discipline. Biology departments used to be dominated by field biologists who spent their lives hunting down new varieties or re-examining known ones and making sure they were classified correctly. The discovery of DNA altered biology in such a way as to make such classificatory work almost a quaint byway for the profession—nice to do given the history of classifications, but unnecessary given how powerful a tool DNA is to identify and classify plants. We find the same sort of change in paleoanthropology where our capacity to date ancient bones has altered our understanding of our evolutionary history.

So the idea is not far-fetched at least that significant changes in technology, for instance, may effectively phase out some engineers and an understanding of what engineers do. I suspect, but do not know, that few engineers now use a slide rule just as learning to use one is no longer on any course list for engineering students.

8

Role Morality

§1. The Roles We Have

We are all born into a social position we have no choice over. It is a position determined by the nature of the society within which we are born and generally by the social positions of our parents within that society—rich or poor, educated or not, professional or working class. We take on various roles through our birth. We are a parents' child, perhaps a sibling, a member of a large family, or a small one, and so on. The number and nature of roles we occupy expands as we grow up. We become friends—or not—with neighborhood kids, a student, perhaps a teammate, perhaps an employee as we take on odd jobs, a citizen able to vote. Eventually, some will become professionals, and it is the role morality of professionals and especially of engineers that is of concern here. What is true of professionals is true of engineers, and so we begin with a sketch of the role morality of professionals.

At the risk of some confusion for engineers, I use the term "professional engineer" to refer to those who have graduated from an accredited engineering school (or have through their experience obtained the equivalent education) and thus can be hired *as engineers*. A person becomes an engineer by successfully completing that process. It is another matter whether a graduate of an engineering school also obtains the certification necessary to become a professional engineer in the eyes of a state and the profession in general.

§2. On Becoming a Professional

Exactly what conditions need to be satisfied to be a professional is contentious. Must one be paid? Some professionals work for free, and in some sports, amateurs are paid. Picking out and arguing for any one set of conditions is not necessary to make my point about how ethics enters into professions and into engineering in particular. So the list of potential conditions is no doubt longer than those in my list. I will not argue that the ones I list are the only essential conditions. These are necessary conditions, but not necessarily sufficient:

1. **A professional must have special knowledge.** A lawyer must know enough about the law to be able to provide good legal advice where "good" means at least "likely to be upheld by a court if things should come to a trial." A surgeon must know anatomy so as not to mistake the spleen for the kidney or cut an artery. An engineer must know about stresses and materials so that choosing one material or form of construction will solve the design problem, not create a new one.
2. **A professional has special skills.** A surgeon learns to handle a set of tools requiring intricate hand-eye coordination and great care. A surgeon who is into a thrust-and-parry mode of operation will not survive any longer in the profession than the patients. An engineer should be able to think creatively about how to solve design problems, envisage how a design solution will look once instantiated in an artifact, calculate stresses and whatever else needs to be specified, learn how a change in specifications at one point reverberates through a design problem and solution, and so on. The rules of skill anyone should master to become a professional can be complicated, and what we master are not just rules about what to do to achieve a certain end, but a set of features that go with mastering those rules. The norms of a profession are not just the rules of skill that define it. They include the manner in which the rules are applied, the modes of thought

necessary to apply them, and the capacity to tie those rules together into the coherent whole. Professionals do not just master the rules of their profession but learn to act and think as those in their profession.

3. **A professional must be certified in some way.** A state or organization may certify someone as licensed to practice a profession. The requirements vary from profession to profession, state to state, and organization to organization. Sometimes only empirical evidence that the person is up to the job is required. A person used to learn how to be a lawyer by being apprenticed to a practicing lawyer. The proof that the person was a lawyer was the capacity to be a lawyer. Today we have examinations administered by the states to determine if a law school graduate has learned enough to become a practicing lawyer. Physicians must attend medical school and then intern for a number of years, gaining the practical experience that can only come from seeing and taking care of patients.
4. **A professional takes on a special set of moral relations in becoming a member of a profession.** Professions can be distinguished one from another by the differing sets of moral relations they have. A physician who takes on a patient ought to examine the person with great care to see if there are any bodily faults or problems—a probing of limbs and cavities and body parts for unusual lumps, for instance. The physician has a moral obligation to the patient, and the patient has a moral right to careful care. An attorney who examined a client in such a way would provide sufficient grounds for disbarment. "But I'm a professional!" would not suffice to get one off the moral hook. You have to be the right kind of professional.

Anyone with a driver's license is familiar with these features. To get a license, you need to pass an exam. When you pass it, you are entitled to a license to drive. The exam certifies that you have both the relevant knowledge and skills to drive and drive safely. You are to know why,

how, and when to use turn signals, know the difference between the brakes and the accelerator, know how and when to use the windshield wipers, and so on. The knowledge and skills we need to drive are no different in kind from those any professional needs, and moral issues enter in the same way for drivers as they do for professionals.

Get in the driver's seat of a vehicle and you take on a special set of moral relations. Driving is risky business. We need only imagine what it is like to be hit head-on by a vehicle weighing several tons and going at high speed to realize just how risky driving can be. That is a risk you take on no matter how good a driver you may be, and any passengers you have take on that risk as well. But because you are driving, they are dependent on your knowledge and skills, and so you have moral obligations to them that you do not have to everyone else. Of course, you also have moral obligations to pedestrians and other drivers. You are operating a heavy piece of machinery capable of killing people and so have taken on a set of moral relations you did not have before you started driving.

Not everything that you do wrong when you drive raises a moral red flag, but if the harm you cause is significant enough, you will be morally culpable. It does not matter whether you intended to cause harm or not. What makes you morally culpable is that you fail to use properly the knowledge or skills required for driving safely. If you drive through a stop sign and kill someone, you cannot excuse yourself by saying, "I didn't intend to hurt anyone. I wasn't even paying attention!" You are morally culpable *because* you were not paying attention. You are morally responsible for something you did not intend to do because you could have avoided the harm had you paid enough attention to your driving to stop at the stop sign.

A professional also takes on a special set of moral relations when engaged in professional practice, and moral failures can occur when a professional fails to use properly the knowledge or skills essential to the profession.

As with drivers, only some failures are significant enough to raise a moral red flag. Yet clearly some situations raise moral red flags,

requiring investigation—as when a surgeon amputates the wrong leg,[1] removes the wrong kidney,[2] or mistakes a kidney for a gallbladder.[3] We would need to examine these cases in detail to make any moral judgments, but they are troubling just because surgeons whom their patients had to trust left those patients far worse off than before, facing life without legs, without kidneys, without a gallbladder.

We do not need to focus on any one profession to understand how ethics enters professional practice. We need only scan the media to find example after example of ethical problems in a wide variety of professions. There is that lawyer in Texas who slept through part of his client's trial,[4] or the coroner in New Jersey who failed to follow the standard procedure of X-raying the victim's skull and so reported death by a blunt instrument instead of death by the two bullets in the victim's head.[5]

Each of these examples involves a professional engaged in professional practice within their own profession, and each causes significant enough harm to raise a moral red flag. We find such examples in any profession. Indeed, the greater the knowledge and the more complex the skills required, the easier it is to fail. As we saw, Aristotle said about being ethical that "it is possible to fail in many ways."[6] In addition, professions are dynamic. Changes are constant, brought on, among other things, by increased knowledge that makes obsolete some of what practitioners may have learned, by technological developments that require new skills, by the continual refining of old skills and standard procedures, by changes in professional standards mandated by the profession, by legal changes requiring changes in practice.

Such changes can catch practitioners by surprise. I was a medical humanities fellow at the University of Tennessee Medical School when the state changed the law to define brain death as death. The medical group I was with had a patient who showed no brain activity upon being tested in accordance with the standard procedure in such cases, a procedure which had been incorporated into the new law. The lead physician told the extended family that the woman was "in a bad way,"

but that the physicians would do what they could. Once we were out of the waiting room, I asked why the physicians did not declare her dead. It turned out that no one in the group had heard that the state had changed the law. Under the law now in force, the patient was not in a bad way, but dead.

The situations of moral concern are those in which a professional causes avoidable harm. There is that simple, but powerful moral principle at work that we ought always avoid causing unnecessary harm. Given a choice between two courses of action, one of which causes more harm than the other, we cannot justify choosing the one that causes more harm without being morally culpable. If the choice we made is avoidable, that is, we are at fault for causing harm we could have avoided.

Not all the harms we may cause are significant enough to raise a moral red flag, but because the lines will be drawn in different places, for differing kinds of harm, within different professions, it is not worthwhile trying to provide a general rule across professions for what raises a moral red flag. Indeed, figuring out what raises a moral red flag within a profession turns out to be no easy matter. But we shall find ourselves with clear examples of harms that should have been avoided as well as clear examples of harms that do not really matter, and we shall thereby hone in on the crucial lines without laying down absolutely clear markers.

We will first examine issues that arise regarding special knowledge and rules of skill, pulling together their implications for the form of life of an engineer in the next chapter. I will put aside issues regarding credentials because they raise concerns that take us far beyond showing how ethical considerations enter engineering. We will then examine issues regarding the moral relations engineers take on.

§3. Knowledge That

We have distinguished between knowing that something is the case and knowing how to do something. These are different kinds of knowledge.

We consider the first in this section, the latter in the next. But we do not need to lay out the knowledge and skills people learn to become engineers. They must cram in an enormous amount in the five years it generally takes to become knowledgeable about all the different matters of importance to the discipline, but engineering books and lectures and labs lay all that out. What is not often laid out is some knowledge that engineering students ought to learn that does not usually appear on the list of "things to learn before I graduate."

Engineers need to know a great many things other than, say, how to calculate. The values they aim for in design solutions are moving targets. Can a toaster have fewer moving parts? Ones less liable to break? Can it be made easier to use? Easier to recycle? It can be frustrating to realize that any design solution is tentative, always subject to reconsideration and improvement. It can be even more frustrating to discover that solutions that seem ideal fail to solve the problems they were designed to solve. That is one problem with trying to make things safer. Those who use what has been designed and even redesigned to be safer adjust their behavior to increase their own risk. Feeling safer, the users engage in more risky activity. Evidence indicates that antilock braking system (ABS) brakes have led to no decrease in the number or severity of accidents because drivers simply go faster. Providing helmets for hockey players has led to an increase in paralyzing neck injuries because, in part, players feel that they can engage in riskier play, if we may call it that, with the helmets than without. Providing helmets for skiers has the same effect. Feeling safer because of their helmets, those 17- to 24-year-old males most prone to accidents go faster and have harmful accidents. Indeed, equipment that ought to make it safer for some individuals to engage in some activities not only fails to decrease the risk they face, because of their off-setting behavior, but also puts others at greater risk than they would have been.

That sort of knowledge of psychology is not an isolated bit, but part of a far broader understanding of human nature that engineers need to take into account to make usable artifacts. The stove top configurations exemplify how readily we can be misled, and engineers who are not

conversant with how we tend to read our environment will choose less than optimal solutions to the design problems they face.

Engineers also need a knowledge of physiology and, in particular, a knowledge of what humans are capable of doing—the norm as well as the extremes. Child-proof containers for medicine are difficult for many with arthritis and for the elderly who are most likely as a group to be on medication. We approach artifacts with different bodies and differing physical capacities. Solving a design problem in a way that no one is disadvantaged in using it—a matter of fairness and thus of morality—is no doubt an ideal, not easily achieved, but it is an ideal that engineers ought to strive to achieve. We can imagine an engineer purposefully designing artifacts that stymy the best efforts of everyone. "I'd like to see anyone use that can opener without hurting themselves!" We would think such an engineer morally perverse. We would also think morally perverse an engineer who designed an artifact so that it could not readily be used by a particular portion of the population—a door so heavy and hard to open that only the muscular and fit could open it. Such design choices would be unfair.

Engineers also need a knowledge of the history of the design problem they are trying to solve. In part this is to ensure that their solution meets the particulars of the problem. It makes little sense to redesign an artifact without taking into account what was causing problems with the previous iteration, and there are other reasons for engineers facing a design problem to learn the history of the problem and of various solutions.

First, there is no sense reinventing the wheel. We can learn from past attempts, sometimes way ahead of their time, as we try to create new solutions. The Selectric typewriter, with a rotating ball rather than individual keys, had its ancestor in one of the first solutions to the problem of connecting the individual strikes on a keypad with making an impression on paper. Blickensderfer designed a typewriter with a removable type ball in 1891. With only 250 parts, versus 2500 for a standard typewriter, it was cheaper to make, weighed far less, was smaller, and had the capacity to type in as many different fonts as there

were type balls.[7] An engineer would look very foolish indeed who designed a similar machine and then showed it around, proud of the new creation, only to have someone point out that, yes, it is a good idea, and it was a good idea in 1891 as well. We can look back to those earlier designs and figure out how to improve them. So that is one reason for knowing the history of a design problem and its former solutions—assuming, of course, that it is not a wholly new problem.

Second, perhaps more importantly, engineers need to know what expectations we will carry as we come to the new artifact. The standard example is the QWERTY keyboard, invented to slow down typists so that the keys would not mesh. We could type much faster if the most commonly used keys were placed where they were easiest to strike. We would not then have to use our left-hand pinkie finger for the "a." But changing the keyboard pattern will run against the habits of millions upon millions of typists. Even a single-finger pecker would be nonplussed.

Legacy problems are not morally neutral. We saw this problem when we looked at the Cadillac trunk that closes automatically after being lowered to a certain height. Someone, somewhere, is going to do what we are all so used to doing with trunks and so break the mechanism. If we have grown used to something operating in a certain way, and operating a new version in that way will cause harm, engineers have an obligation to reengineer the new version to ensure that harm will not ensue when users bring old habits to bear on a new artifact.

Examples of legacy issues are easy to find, and they illustrate the tension we mentioned when we began this chapter. If engineers are to push the envelope of design, they must be free to change every variable of a previous design solution, but as they change variables, they risk introducing new problems because of residual habits of use even as they try to make things easier for operators. An engineer must thus make informed judgments about how and what to change in solving a design problem.

So, rather obviously, getting the information necessary to make informed judgments is an imperative. Such information is no different

in kind than the information engineering students must learn to calculate properly and understand stresses. It is information they need to know if they are to solve design problems in ways that do not cause unnecessary harm. So it is not morally neutral information, but information they ought to have to do their work as engineers.

If an engineer designs a turnoff valve for a water heater made of high-impact plastic instead of the old material, lead, we can expect someone who turns it off to give the knob an extra little turn, just as before, to make sure that it is tight—the extra little turn that served to ensure that the lead knob was seated. That extra little pressure may snap off the plastic knob. The valve will then continue on for a bit, opening up so gas can seep out. The homeowner will return home to a basement filled with gas, which will explode when the furnace is turned on. The realization of how deeply ingrained our habits can be, as well as knowledge of how the previous iteration of turnoff knobs worked, is as essential to the engineer choosing the correct design solution as is the knowledge of how to calculate the stresses the knob will undergo when it is tightened to the off-position.

§4. Knowledge How

It is such calculating skills that engineers most obviously need. We have images that come to mind when we think of various professionals—a physician with a stethoscope, a psychiatrist with a patient on a couch, a banker with a cigar, perhaps, and, it used to be, an engineer with a plastic sleeve in a shirt pocket with a pen and slide rule. Now it is an engineer with a calculator of some sort.

That image is not mistaken, but it does not capture the full set of skills of an engineer any more than a physician with a stethoscope captures all the skills a physician needs. There are skills an engineer must have that may not be as obvious as knowing how to calculate. We will mention only a few of the many, but enough to get a sense of how far beyond calculating they extend.

1. Tracking consequences: The original plans for the walkways in the Kansas City Hyatt envisioned single rods attached to the ceiling and extending through the "cross beams on which the walkways rested."[8] Those single rods were to be over forty-five feet long, and during construction the plans were modified so that the number of rods was doubled and the length shortened, with one set going from the ceiling to one walkway's support beams, attached with nuts and washers, the second set going from that walkway to another, again attached with nuts and washers. The walkways collapsed, and 114 people were killed and another 200 injured.

A 45-foot-long rod designed to hold two walkways is not your standard construction item. So it is probably not much cause for wonder that the suggestion to use shorter rods was made or accepted. Henry Petroski quotes a reader of the *Engineering News-Record* as saying, "A detail that begs a change cannot be completely without blame when the change is made."[9]

Yet clearly no one thought through the implications of that design change. As Petroski points out, in a telling example, it is one thing to have two climbers on ropes side-by-side going up a stone face and quite another to have one climber on a rope with another climber hanging on to the first climber's legs. The rods that held up the one walkway were also holding up the other walkway.[10] No wonder the walkways collapsed. Indeed, changing the design was not the only mistake made. The walkways would likely have collapsed even without the design change since the original was only 60 percent as strong as Kansas City building codes required.[11]

In any event, it does not take much skill to understand the causal implications of the design modification that left one walkway hanging on another. But it takes some skill to envisage what changes that modification would make in the way the walkways are supported. It is not necessarily easy looking at the original plans, making the change mentally, and then tracking the projected history of that change and understanding its effects.

That projected history has two aspects. The first concerns how changing one design feature will affect other design features, how a design change reverberates through the original design solution, impacting

other design features and requiring changes. The second concerns how the new design solution will play itself out once realized in an artifact. How will the artifact work in practice with that change in place?

This second skill requires a sense of what we may call projective history, of how things play themselves out. That requires understanding the contingencies of life, how completely unpredictable events may occur and change the projected trajectory of an artifact's life. It requires understanding how much space there is between a design solution and the artifact that realizes that design and so how many things can go wrong in realizing the design solution. It requires understanding how people will underuse and misuse the artifact, failing to appreciate, let alone note, its more subtle features and misusing in various ways what they do understand. It requires understanding how even major problems with the artifact may go unremarked, preventing timely corrections.

The collapse of the Hyatt-Regency walkways illustrates these requirements well. Workman noticed how the walkways vibrated when they used it, but they just worked around it. No one pursued the problem.[12] The engineers who designed the original 45-foot-long rods did not think through how they would be manufactured and how likely it would be for that feature to beg a change.

In any event, this skill of projective history is not easy to articulate in all its details. It is a complex skill having many aspects and many requirements for its proper realization. So it is not easy to figure out how to teach it, how to train ourselves into looking at a design change and seeing how it will play itself out when realized in an artifact. It is no doubt even more difficult when we consider alternative design changes. How will it work out in the long term if this change is made rather than that? Is the artifact more or less likely to break? Is it going to last longer or break down sooner? Will that little change cause problems with shipping and storing it?

2. Seeing reverberations: A second skill requires seeing how one design change affects other design features, how a design change reverberates through the original solution. What else needs to be changed if this is changed? One way of thinking about this skill is to see that it relates to another skill engineers need to complete a design solution.

Decisions have their consequences, as we know. One feature of design solutions is that any choice will both open up and constrain other possibilities. Having booster rockets with segments for the space shuttle, rather than a single tube, created problems, for instance. Ensuring that the segments fit together without risk of allowing hot combustion gases to escape inevitably leads to something like the O-rings in Figure 12.

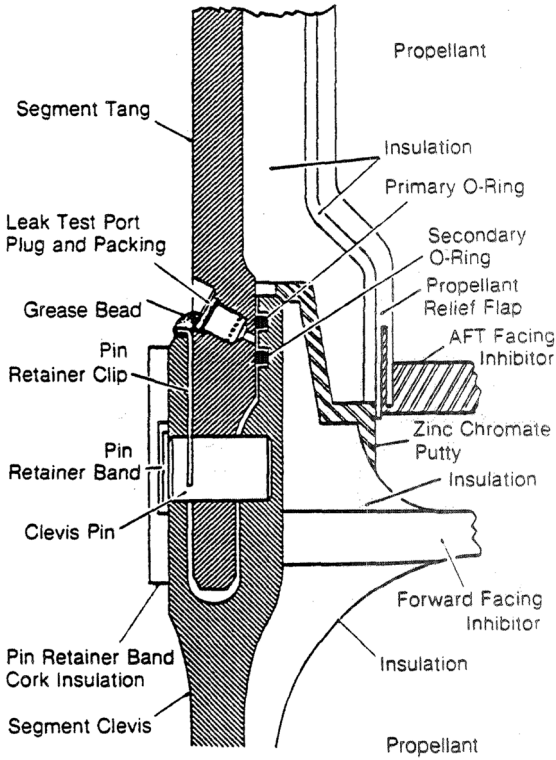


Figure 12 Shuttle booster rocket joint. Public Domain. Courtesy NASA/JPL-Caltech. See also https://commons.wikimedia.org/wiki/File:RogersCommission-v1p57.jpg. See also the *Report of the Presidential Commission on the Space Shuttle Challenger Accident* (Washington, D.C.: United States Government Printing Office, 1986), p. 57. Online at http://www.tech.plym.ac.uk/sme/Interactive_Resources/tutorials/FailureCases/images/CH7Joint.gif.

When the rocket is fired, the segments twang, moving against each other and compressing the O-rings—which are supposed to seal the gaps instantaneously. They are made of a substance that will need to withstand the twang at liftoff and rebound to seal any gap before hot gases can burn through. But they will work properly only if properly seated in the clevis. To ensure that seating, air is forced between them through the valve to the left in Figure 12—drawn in the figure, but unnamed, with the nozzle between the primary and secondary O-rings.

Rather obviously, the less the air pressure, the greater the likelihood that the O-rings are not seated properly, but the more the air pressure, the greater the likelihood that the O-rings, and especially the primary O-ring, will be pushed out of their groves. When the engineers at Morton-Thiokol found that hot gasses had blown past the primary O-ring during a launch the January before the Challenger disaster, they tried increasing the pressure to ensure that the O-rings were properly seated but had no way to determine whether they may have made the problem worse by pushing the primary O-ring from its seat back toward the rocket booster engine or the secondary O-ring from its seat out toward the outer casing. No valve was positioned in a way that would ensure that the primary O-ring and the secondary O-ring were both properly seated.

So we have a decision of segmented booster rockets that has implications for other features of the design. Something like those features seems, in retrospect, inevitable, but those features mean that if there is a later problem, there is no easy way to check to ensure that the O-rings are properly seated.

This skill of seeing how a design decision, or design change, reverberates throughout a design solution is like the skill photographers must come to have of seeing how a seeming minor modification of lighting will utterly alter an image or like the skill that a chess master must have of seeing how a pawn move made now will affect play ten or more moves farther along. We cannot depend upon our intuitions here but must learn how to see such implications.

Part of that learning will come from practice. It is easy enough for a photographer to take photo after photo, under differing light conditions, until the effects of changes in lighting become obvious, and it is easy enough for chess masters to learn from playing and reading many games and varying moves to see their ripple effects through later stages of the game. An engineer cannot practice building walkways to see how best to support them, although computer simulations help, but, in any event, the skill to track the changes of any particular design change must become obvious for the engineer.

3. **Enormous care:** One additional skill we should emphasize is the great care that must be taken in calculating the various components of a design solution. It is a mistake to think that engineering consists in calculating, as though all engineers do is reducible to what they can do with a calculator. Even if that were all they did, they must do it with enormous care, and that skill is no easier to master than any other skill engineers must have. It is easy to think a calculator is always right, but the programs engineers use in their computers for calculating are as prone to problems as any other software program. These programs are artifacts and as subject to flaws as any other design solution.

It has been argued that

> changing a seemingly innocuous aspect of an experimental setup can cause a systems researcher to draw wrong conclusions from an experiment. What appears to be an innocuous aspect in the experimental setup may in fact introduce a significant bias in an evaluation. This phenomenon is called measurement bias in the natural and social sciences.
>
> Our results demonstrate that measurement bias is significant and commonplace in computer system evaluation. By significant we mean that measurement bias can lead to a performance analysis that either over-states an effect or even yields an incorrect conclusion.[13]

Engineers thus need at the least to learn what would count as the right sort of answer to a calculation, one in the ballpark of answers. Before

the advent of computerized cash registers that tell the cashier how much change to give, I was handed change more than once that was more than I gave. The cashier was clueless as to what would constitute ballpark change and so had no idea there had been a mistake. But computerized programs introduce their own problems. We use them and assume we get the correct answer without a ballpark sense of what the right answer should be. That can lead to our not catching mistakes.

We know that any one mistake can throw everything off. An error in calculation, for instance, can reverberate through the entire enterprise, throwing off everything else, and it is all too easy to make mistakes—especially in complex engineering projects. The mistake that doomed the Mars Climate Orbiter spacecraft was that one team used "English units (e.g., inches, feet and pounds) while the other used metric units for a key spacecraft operation. This information was critical to the maneuvers required to place the spacecraft in the proper Mars orbit."[14] So engineers must not only make the right choices but be sure they get the calculations right so that harm does not sneak in because of an error. The Orbiter error was in part due to a lack of communication between the teams working on the project, but that just illustrates one more failure to take due care and check to be sure both teams were using the same units of measurement.

Seeing how a change reverberates through a design, tracking the consequences of a design solution once realized in an artifact, taking great care at each and every step—these are only a few of the set of skills an engineer must master. They also need the capacity to see problems that call for an engineering solution, the skill to analyze the problem into manageable parts, an imagination sufficient to sketch out alternative solutions to the problem, a grounding in the possible to understand what could work and what would not, what could readily be realized in an artifact and what could not, and so on.

An engineer is thus a marvel of numerous skills of a wide variety, far beyond the ability to calculate. Merely to become minimally competent requires far more than being able to calculate stresses,

or measure rods, or understand how to fit pieces of an artifact together without introducing structural weaknesses. Just learning how to analyze a problem without leaving out any crucial piece of the puzzle is difficult enough, but an engineer must also learn to imagine alternative solutions so as to be more sure that the selected design solution is the best available. Part of the role of an engineer is thus, at a minimum, to have a wide set of skills, both numerous and varied.

§5. Potential Moral Relations

A careful detailing of each profession would reveal what a person takes on in becoming a member of that profession and in that way how a member of that profession is distinguished from members of every other profession. The knowledge and skills necessary for one profession are distinct from the knowledge and skills necessary for another. A professor needs to learn how to teach, but not how to defend a client before a jury. A lawyer needs to learn how to read legislation carefully, but not how to use a scalpel. These are features internal to each profession.

Professions can also be distinguished one from another by the differing moral relations they can take on. These potential relations differ from profession to profession. In taking on a lawyer, I empower the lawyer to represent me in a court of law if I am charged with a crime. I could hire a nurse, but a nurse lacks the knowledge, skills, and certification to represent me in a court, and no nurse is empowered by the state to act as my representative in a court of law—unless the nurse is also a lawyer. A nurse has an obligation to make sure that a hospital patient is receiving proper care. A professor does not. A professor is empowered to assign students books and articles to read, papers to write, and exams to take. A psychiatrist is not. A psychiatrist is obligated to help those with psychiatric problems. An accountant is not. And so on and so on.

These are potential moral relations. A professional is not in such relations just by virtue of being a professional. A lawyer is not empowered to represent me unless I engage that lawyer and become a client or the lawyer is appointed by a court to represent me. So a lawyer has the potential to represent me in court. A physician does not. A physician has the potential to examine me for diseases or bodily harms but cannot examine me unless I am that physician's patient and so have given consent—or am in an accident, say, and must have a physician examine me even if I cannot give consent. We would certainly look askance if someone came up to us on the sidewalk and, unbidden, started probing us the way a physician is supposed to. "But I'm a physician!" would hardly suffice as an answer to our "Hey! What are you doing?!" The stranger may be a physician, but not our physician, and even our physician would not examine us on the sidewalk.

The moral relations we are examining here that mark out professions one from another are relations a professional takes on in the practice of that profession as the professional takes on patients, clients, and so on. In becoming certified in some way in a profession, a professional takes on the potential to have those special moral relations, and professions are thus distinguished one from another by the potential moral relations those professionals have.

We can readily see why these relations are moral by looking at examples where a professional in such a relation has failed in some way. We read from time to time of a surgeon cutting off the wrong limb, a leg perhaps. Indeed, cutting off the wrong limb, or the wrong body part, seems to happen frequently enough that the error rate should give one pause if about to have such an operation. Surgeons cut off the wrong leg for an 86-year-old man in Lima, Peru, and then had to cut off the other,[15] and a report about mistakes in 2005 says that surgeons in England removed the wrong disc in eight cases, amputated the wrong leg in five cases, took out the wrong hip in four cases, removed the wrong testicle in one case, gave a hysterectomy to a woman who did not need it, transplanted the wrong set of lungs into a patient, and circumcised a child who was not the patient needing circumcision.[16]

A surgeon's doing any of these things intending to cause harm would be particularly egregious because the patient was presumably under an anesthetic and helpless. More importantly, the patient was under the surgeon's care and so had every reason to expect that the surgeon would do everything possible to ensure that the patient was properly cared for. Intentionally amputating the wrong leg, even if neatly and carefully done, is hardly proper care.

Yet, even if the amputation were unintentional, we would still blame the surgeon. The person was the surgeon's patient. Surgeons take on special moral relations when they take on a patient. If a surgeon agreed to give me a needed operation, that surgeon would thereby take on a set of special moral relations. A drunk or hung-over surgeon operating on me would be unprofessional—and unethical. Hacking at me and not cutting carefully would be equally unprofessional—and unethical. The surgeon asking someone else to perform the operation would be equally unprofessional—and unethical. I empowered that surgeon to operate on me and not any substitute. In putting myself in this surgeon's care, I am obligating the surgeon to operate on me at least to the minimal standards of the profession. If the surgeon amputated the wrong leg, even unintentionally, I would hold the surgeon morally responsible. "Whoops, sorry about that! I didn't mean to cut that one off!" will not work to get the surgeon off the moral hook. Minimal competence in surgery requires getting the problem right and doing right by the patient in solving the problem. Cutting off the wrong limb fails on both counts.

We can readily multiply such examples of various professionals failing those they take on in their professional capacities. We hold them morally blameworthy, and rightly so, if through inattention, carelessness, neglect of advances in their field or a failure to do whatever they are obligated as professionals to do, they cause gratuitous harm to those they have taken on in a professional relationship.

A profession is what it is at least in part because of that set of potential moral relations. If I am a judge and you sit down beside me, I remain a judge. You and I have a relation to each other—we are side-by-

side—but that relation makes no difference at all to my being a judge. What makes me a judge does not depend upon your sitting beside me, but upon whatever features being a judge requires—being elected or appointed to the office and so taking on the features that belong to that office. If I were a judge, I would carry those features with me whether I sat beside you or not. A judge must have knowledge of the law, a capacity to understand how different individuals could interpret the law differently, a capacity to get far enough into each party's position to understand why each party is willing to go to court to begin with, an ability to assess the merits of legal arguments, and a capacity to back off from the competing legal positions, as it were, and make an objective judgment in accordance with the law.

Another way of putting this is to think of various roles an individual may have—as a parent, for instance, or a sibling, or a citizen in a community, or a physician, and so on. Each of these roles is defined in part by a set of moral relations. Parents have obligations to their children—to feed them, clothe them, care for them, and rear them well. Citizens have obligations to their communities—to pay their taxes, maintain their dwellings, and drive carefully. Physicians have special moral relations that neither parents nor citizens have—to examine carefully those individuals who put themselves in the physician's care to determine whether the individual has an illness that needs curing or some bodily fault that needs repair and then to care for those individuals, doing their utmost to cure them of the disease and to repair their bodily faults. Just so with any professional.

Any one individual occupies a number of different roles—child, parent, sibling, citizen of a community, a state, and a nation, an employee or self-employed (each with its own set of moral relations), a professional of one sort or another or not. Moral tensions occur when one moral imperative in one role someone occupies conflicts with a moral imperative in another role that person occupies. What I am required to do as an employee, for instance, may conflict with what my profession tells me I ought to do. These sorts of conflicts between the different roles we occupy are a rich source of moral problems and

are all too often difficult to resolve, the moral imperatives of one role being as powerful and persuasive as those of the other with which it is in conflict.

These sorts of moral problems are not the primary focus of this book although we will briefly discuss them in examining the issues that can arise when working with and for others. We are putting completely aside the moral relations a professional takes on just by becoming a member of a profession. Professionals are at least implicitly licensed by the state, either directly or indirectly because the university in which they received their professional training is accredited. That license exists because the state recognizes a discipline as a profession, and in giving those within that profession a license, it excludes others who are not members of that profession from practicing that profession. That is the reason I cannot legally remove your appendix or represent you in court. What the profession then owes in return for its state-sponsored monopoly of a particular kind of service is that it benefits society in some more substantial way than by simply having its members practice their profession.

In other words, engineers take on a set of moral relations not only to each other when they work in teams and to their clients or employers, but to society. They have an obligation to use their professional expertise to ensure the safety and welfare of their fellow citizens. One way they do that is by investigating what went wrong regarding various engineering disasters such as the attempt by BP to shut down a well in the Gulf, the Big Dig in Boston, the flood walls in New Orleans, and the Interstate Highway bridge in Minneapolis. In taking on these investigations, engineers are fulfilling the moral obligations to society they took on when they became engineers.

9

Forms of Life

§1. Thinking like an Engineer

We take on a role in becoming a professional, and that role makes demands upon us that we cannot ignore without putting at risk our professional standing, not necessarily by losing our accreditation, but certainly by a loss of respect within the profession as someone competent. I was once told of a physician who did all the circumcisions at one of a city's hospitals, three or four hundred a year. He tended to take too much skin, causing the boys much pain as they grew and ensuring that they would need another operation for a skin graft. No physician who knew of this was willing to testify, but, to put it mildly, the physician was not a respected member of his profession.

Being a professional demands, at the least, that one be competent, and that means that we come to know all we need to know to be a professional within our chosen discipline and that we come to have the skills we need to have as a professional. But if we consider only these demands, we will not succeed in understanding fully what it is to become a professional. Becoming an engineer does not mean just learning physics, calculus, and so on, the kinds of things engineers must learn as distinct from those a lawyer must learn—the relevant law or the proper forms. Becoming an engineer does not mean just learning a set of skills—as though it were enough to know how to manipulate numbers or run particular computer programs. To become an engineer, to become any professional, is to enter into a form of life that is distinctly different from any other.

The person who acquires the special knowledge and skills of a profession learns to think in a certain way. Jokes about individuals in various professions depend upon this fact about becoming a professional. The joke about the priest, the physician, and the engineer about to be guillotined displays well the way engineers are trained to think. The priest is led to the guillotine, the cord is pulled, and nothing happens. "A miracle!" exclaim the executioners, and they let him go free. The physician is led to the guillotine, and the guillotine again fails to drop. "Another miracle!" and he goes free. The engineer looks up as his head is being put under the blade and says, "Wait! Wait! I think I see the problem!" That engineer has a form of life, and in particular a distinct way of thinking about the world, that will make his life shorter than it would otherwise have been. Yet learning to think that way is necessary for someone to be an engineer.

Learning to think in a certain way is necessary to become a professional even if it can also be a problem. You need to learn to think like a lawyer, like a philosopher, like a physician if you are to become a lawyer, a philosopher, a physician. The joke illustrates one kind of disadvantage. If we approach all life's problems with only one way of thinking about the world, we may find ourselves creating new problems for ourselves.

These forms of life are not morally neutral, that is. Indeed, a form of life can even be in moral tension. A profession you enter may require competing modes of thought. A colleague of mine at a major Big Ten university heard tittering outside his door one day. It went on, and he went out to tell whoever was doing it to stop. He found that the sound came from a room down the hall where twenty second-year medical students were learning how to examine patients by examining each other. These interns had gone to the same classes together for a year and a half; some had dated; some were dating; some wanted to date. They were learning how to look at a nude body without getting embarrassed and so getting red-faced or, worse, laughing, a typical response to embarrassment. The last thing you would want is to have your physician, upon seeing you for an examination, double up in

laugher. It is one important feature of becoming a physician that you learn how to examine other human beings, and that means seeing them as a mechanic sees a bicycle, as a mechanism that may need repair.

Yet we also want physicians to have a good bedside manner, to be able to relate to you not as a mechanic to a bicycle, but as a person to a person. So those training to be physicians need to learn how to switch back and forth between two different ways of looking at their patients. That is not easy, and one consequence is that we have many physicians with poor bedside manners. For some reason, it may be easier to see patients as mechanisms than as persons, or perhaps those who successfully navigate the long and hard medical training are those who are best able to see patients as mechanisms.

In engineering, we find a similar set of mixed modes of thought. We demand that engineers learn to think quantitatively and that they be risk-averse. It matters in working out the details of a bridge truss to get it right, to do the calculations that ensure the bridge will not fail. To ensure that it not fail, engineers make the truss stronger than it needs to be. They are risk-averse. But we also want engineers to be creative in solving the design problems they face, to push the envelope of design. These two different modes of thought are not incompatible, but they are certainly in tension. Pushing the envelope of design is to risk failure.

The Tacoma Narrows Bridge is a case in point. The design was

> Unconventional . . . in that the depth of the roadway structure was diminished by employing a stiffened-girder design rather than the then-customary and necessarily deeper open truss. This innovation gave a slender silhouette whose appearance was dramatic and graceful, but the shallow, narrow span was also very flexible in the wind.

The bridge was known as "Galloping Gertie" because it "undulated uncontrollably" in the wind. It soon flew off its moorings. "Subsequent analysis of the Tacoma Narrows failure confirmed that the bridge span acted much like an airplane wing subjected to uncontrolled turbulence."[1] Pushing the envelope of design pushed the risk of failure too high.

Taking on the form of life as an engineer is thus to enter into a life of tension between competing imperatives. Engineering is no different than any other discipline in this respect—as we have seen from the example of physicians. It is also to enter into a particular way of thinking. The joke about the engineer about to be guillotined is telling because it is a commonplace that professionals see everything in terms of their own profession. It may be an exaggeration to say that prosecuting attorneys are always prosecuting (though that might help explain their higher than average divorce rate) or that economists see every issue as economic.

We want professionals to become so good at thinking in a certain way that it becomes second nature. They never have to think about how to think about a problem because thinking of a problem as an engineer or as an economist comes naturally. But the better we are trained into a mode of thought that becomes second nature, the less likely we are to realize that we are embedded within a particular mode of thought. An Englishman once said after he circumnavigated the globe that he was happy to be back in England where people spoke the way they thought. Becoming so used to thinking in a certain way that it is second nature risks blinding us to the contingency of that mode of thought. Thinking in English is as contingent as thinking like an engineer, or like a prosecuting attorney, or like a physician, and that is a problem when, like the Englishman, we become so arrogant about our particular form of thinking that we become blind to alternative modes of thought.

We may thus fail to see a problem in all its richness or fail to realize that others are reasoning differently, but perfectly appropriately, given the mode of thought into which they have been trained. Modes of thought elevate some relevant features and depress others, and so, as we shall see, modes of thought are not morally neutral. A failure to understand the limitations of the form of reasoning we have been trained into so as to become professionals within a discipline can lead to confusion and moral problems. Some of the decision-making the night before the fatal launch of the space shuttle Challenger illustrates the issue.

§2. The Challenger and Mr. Lund

The shuttle booster rockets consist of sections placed on top of one another as shown in Figure 12. The problem that mode of construction creates is that the hot combustion gases can escape at the section joints when the propellant fires and the rocket vibrates at liftoff. The solution was to provide a clevis and tang joint with two rings, the primary and secondary O-rings. When the rocket vibrates at liftoff, the O-rings will be compressed, and if they were not resilient, they would not bounce back quickly enough to fill the gaps their compression would create. That would allow hot gases to escape and burn through the side of the booster rockets. The rings are made of a rubber-like resilient material, Viton, and are to bounce back into shape quickly enough to preclude the hot gases blowing by.

The evening before the launch of the Challenger shuttle, NASA had a teleconference with the contractor for the shuttle booster rockets, Morton-Thiokol. The overnight temperature at the launch site was predicted to go as low as 18°F, and Viton was certified only down to 25°F. NASA's question was whether the O-rings would become too cold to retain their resiliency. NASA needed the contractor's approval to launch under such conditions. The previous January, when the O-rings were calculated to have been at 53°F, significant blow-by occurred, with the first O-ring highly compromised and soot deposited on the second O-ring. NASA's query was whether the O-rings would remain sufficiently resilient after the shuttle booster rockets had been subject to an overnight low of 18°F so that the Challenger could be launched at a temperature of 28°F, the projected temperature at time of launch.

The engineers, including their manager, Bob Lund, all agreed that no launch should occur. The risk of catastrophic failure was simply too high, with the temperature of the O-rings far below the 53°F calculated for the O-rings the previous January. How far below is difficult to tell. To determine the temperature, we would need a calculation similar to the one that produced the 53°F figure of the previous January. That

calculation would depend upon how cold it got the night before the launch, how long the booster rockets sat outside in the cold, how much heat the booster rockets retained from before the cold snap, and so on. The engineers could not possibly have determined that the night before the launch. It was sufficient for their concerns, however, that the O-ring temperature would be found to be *significantly* below 53°F, whatever the exact figure may have been. The engineers and managers were unanimous in their recommendation.

NASA insisted that Morton-Thiokol revisit that recommendation. We need not get into the complex details of the exchange that followed.[2] The crucial point came when Mr. Mason, Senior Vice President for Wasatch Operations at Morton-Thiokol, said that it was time for a management decision. He said in an interview that the discussion had reached the point where people began repeating themselves. As Thiokol's Bill Macbeth put it,

> when you get that kind of an impasse, that's the time management has to then make a decision. They've heard all of the evidence. There was no new evidence coming in, no new data being brought up, no new thinking, no new twists being put on it from our previous position, and we were just rehashing. And so Mr. Mason then said, "Well, it's time to make a management decision. We're just spinning our wheels."[3]

He asked the engineers if they had anything new to say, and when no one responded, he said that he supported a launch decision and turned to the managers, asking them, one by one, for their opinion. Two recommended launch, but Bob Lund, the Vice President for Engineering, hesitated when Mason turned to him. Mason then said to Lund, "It's time to take off your engineering hat and put on your management hat."[4]

What has become the standard view is that Mason was asking Lund to look at the problem from the point of view of a manager, doing what managers are supposed to do, taking a different perspective than that of an engineer. When we are well trained into a discipline, the discipline's way of thinking becomes so natural that it may never occur to its

professionals that it is only one way of thinking about things, that a form of thinking is a contingent matter that may be inappropriate in some situations for some kinds of problems. So on this standard view, Mason was asking Lund to stop thinking like an engineer and think like a manager. That perspective was different from that of the engineers in at least two ways:

> First, engineers would not normally include in their calculations certain risks—for instance, the risk of losing the shuttle contract if the launch schedule were not kept. Such risks are not part of their professional concern; such risks are properly a manager's concern. Second, engineers are trained to be conservative in their assessment of permissible risk. . . . Engineers do not, in general, balance risk against benefit. They reduce risk to permissible levels and only then proceed. Managers, on the other hand, generally balance risk against benefit. That is one of the things they are trained to do.[5]

The engineers were looking at the risk to the shuttle from the cold, but the managers were to look at all the risks, including the company's responsibility in delaying a launch and so putting at risk the company's shuttle contract.

If we "balance risk against benefit," taking into account the likelihood and magnitude of each harm occurring and the likelihood and magnitude of each benefit, the risk of a catastrophic failure of the shuttle is just one of many, and the risk is small, the shuttles having launched many a time with a risk of blow-by and having flown successfully. Using a risk/benefit analysis, the choice to launch is not hard to make.

Thinking like a manager is very different from thinking like an engineer. So in asking Lund to think like a manager, Mason was asking him to use a completely different decision-procedure than he used as an engineer. Mason was telling Lund, "Don't think about minimizing potential losses, but calculate the likelihoods and magnitudes of potential losses and gains and then compare the two, letting the results of that calculation determine what to do."

What the Challenger example illustrates is an all too common problem. We are trained into a discipline and so learn to think in a certain way and carry that with us as we approach other problems. That is the point of the story about the engineer about to be guillotined who stops the proceedings so the problem can be fixed. Short-sighted? Yes. But we smile in recognition because the problem is so widespread. I learned as a philosophy graduate student to take arguments, including my own, pin them to a wall, as it were, and then critique them mercilessly: "Well, the first premise is ambiguous and false on either interpretation, and the argument is not valid in any case." It took a while for me to learn that my colleagues in committee meetings—certainly those from other disciplines—did not appreciate the favor I was doing them by pointing out the flaws in their arguments.

This sort of problem is internal to each profession. Lund later said to Chairman Rogers of the Presidential Commission that he had not realized he had changed his way of thinking when he changed hats or that one consequence was that he put himself in the position where the only way to justify not launching was to prove that the "motor wouldn't work"—presumably not meaning that the engines would not fire, since that was not at issue, but that the O-rings would not seal. If he could not prove that the O-rings would not seal at 28°F, the possibility that they would not was just one risk among many.

Within a decision-procedure where everything is a cost or a benefit, in other words,

> Lund was forced to treat a catastrophic failure as just one risk among others. The only way within that decision-procedure to argue for a different outcome would be to prove that failure was not a risk, but a certainty. In failing to realize he had changed his way of thinking, he was caught up having to prove what neither the engineers nor the managers could prove, namely, that the O-rings would not seal.[6]

It is not clear what Lund would have done had he realized that in changing hats, he was changing decision-procedures. Had he realized that, we would hope that he would have asked the obvious question,

"Which decision-procedure is the right one to use?" That is not necessarily an easy question to answer, but it needs to be addressed.

Decision-procedures are not morally neutral. If I suggest we flip a coin for something—"Heads you win, tails I win"—I am suggesting we use a decision-procedure for determining who gets something, and the procedure presupposes that neither of us deserves it. If I take something of yours, and when you realize I have taken it, I suggest that we flip for it, you will quite reasonably be flummoxed at my suggestion. It is yours, after all, and why should you let the toss of a coin determine whose it is when it belongs to you? Flipping a coin to determine ownership only makes sense where no one owns the object in question.

Just so, a cost/benefit decision-procedure is as morally loaded as one based on minimizing potential losses. We need not get involved in a detailed analysis here of those differences to see that they are different, with different outcomes that have moral consequences. The cost–benefit analysis of the managers put the astronauts at risk; a decision based on minimizing potential harm would not have done that.

As necessary as it is to learn to think like an engineer to be an engineer, it can be an enormous disadvantage, as Mr. Lund discovered, not realizing that other disciplines embody other modes of thinking that give different results when put to a problem. Unfortunately, learning to think like an engineer, or like a physician, or like a lawyer is difficult enough. To succeed, we need to train ourselves out of whatever had been our standard way of looking at a problem and then make the mode of thought of our discipline be second nature to us, such a natural way of looking at problems that it would never occur to us, even as newly minted professionals, to think about them in any other way. Our aim is that we never have to think about how to think about problems in any other way than as an engineer, say. The last thing we should want if we are in a group of engineers looking at a bridge at risk of failure is for the other engineers seriously to consider options that are outside the parameters of an engineering solution. Putting up a sign saying "Bridge may fail!" is not a serious engineering option. Preventing the bridge from failing is the problem the engineers are trying to solve, and it will

take engineers thinking of engineering solutions to solve the problem, not sign painters painting a sign.

Yet if the aim is to train ourselves into a mode of thought that becomes second nature, it may seem paradoxical for us to try to get out of our own skins and come to see that we have been trained into a mode of thought that other disciplines may neither share nor understand. Thinking about how we are thinking requires a special set of skills, but we can only come to recognize the contingency and moral implications of any particular mode of thought by getting distance from what has become a natural mode of thought for us and understanding that it is only one among many—just as thinking in English is only one possibility among many. If we aspire to be the best in our chosen profession, we must learn to understand both the strengths and the limitations of its natural mode of thought. Thinking about a problem in only one way is a recipe for disaster.

That is what Mr. Lund's change of mind tells us. Had Mr. Lund fully understood and appreciated his role as a manager, he would have been able to see how differently he was being asked to think when Mr. Mason asked him to put on his manager's hat, and had he also fully understood and appreciated his role as an engineer, he would have been able to see how the differing modes of thought of these two roles were in conflict. He might also have been able to see that the conflict cannot be resolved just by choosing one over the other. It can only be resolved by considering the reasons for adopting one mode or the other in the situation in question.

§3. Inner Morality

Ethical considerations thus enter even into the way engineers think. The mode of thought into which they are trained is not itself morally neutral any more than flipping a coin is a morally neutral decision-procedure. But their form of life is far richer than this examination of their risk-averse decision-procedure may make it appear, and ethical considerations appear in many ways, some no doubt decidedly unexpected.

Let us return to the sort of problem we examined in Chapter 2, an accident that requires analysis for us to understand how to prevent a repetition. It is not an accident involving engineers, but out of this accident we can draw lessons about the inner morality of professionals and engineers in particular.

In a 60 Minutes Report on March 16, 2008, Dennis Quaid and his wife, Kimberly, told about the near death of their newly born twins. The twins had been taken to the hospital a few days after coming home because they showed signs of a staph infection. Part of the standard treatment in such cases is the use of a blood thinner to prevent clotting. But the twins were given a blood thinner that turned their blood to the consistency of water. It was pouring out of them, leaking out everywhere it could—their belly buttons, their noses, their toes.

Kimberly Quaid had a premonition that something had gone wrong, and so Dennis Quaid called the hospital at 9 p.m. to ask if the twins were O.K. He was told that they were, but, in fact, they were not. When the Quaids came to the hospital in the morning, they were met by their pediatrician, the head nurse, and a lawyer from "risk management . . . the liability division of the hospital."[7] The Quaids had not been called about any problem.

The twins should have been given Hep-Lock, a blood thinner for infants. They were given the adult version, heparin. They should have gotten ten units of the infant version. They got 10,000, a thousand times more than prescribed, and they got it at least twice. The president of the hospital where this occurred said of the infants' near deaths, "It was the result of human error." The hospital was not at fault, its president was claiming. The spokesperson for Baxter, the manufacturer of the two blood thinners, said, "The errors that the hospital has acknowledged were preventable and due to failures in their system." Baxter was not at fault, it claimed.

Both statements blame the operators, three in this case according to the hospital: the individuals who put heparin in the special drug cabinets for infants, those who took the drugs from the cabinet to give to the nurses, and the nurse or nurses who administered the drug.

The spokesperson for Baxter said that the way to prevent such errors is to read the label, but the containers for heparin and Hep-Lock are very similar and easy to confuse. They are the same shape and the same size, with labels differing only because one is a slightly darker blue than the other with a different name, but all in the same font.[8]

The previous year, six infants in Indianapolis were also given heparin instead of Hep-Lock. Three died, and as a result, Baxter sent out a warning and redesigned the container for Hep-Lock so that it was visually different from the container for heparin and required the removal of a plastic cover. What Baxter did not do was recall any of the old stock, and the heparin that caused the near death of the Quaid twins came from old stock.

It would be naive to accept the statements of Baxter and the hospital president at face value. Neither can be read straight, as statements of fact. Both are attempts at risk management, both implicitly saying it was not their fault by blaming others. It was "operator error," the fault of those careless nurses and others in the hospital.

It seems both that some in the hospital made mistakes and that there is a reason for their making mistakes, the objects at issue, the containers for the drugs, making it more likely than not that even the most intelligent, well-trained, and highly motivated individual would mistake one for the other. The design all but guaranteed that an accident would occur, as it had the previous year. So two moral judgments about Baxter are easy to make:

- Baxter should have recalled all its former stock so that the kind of accident that occurred in Indianapolis could not occur again.
- The company was in no position to accuse the hospital of "failures in their system" prior to a full investigation.

It seems more than a little disingenuous to accuse the hospital of failures in its system given the company's failure to recall the drugs that caused three deaths the year before.

That is not to suggest that there were no failures in the hospital. We would need a more detailed understanding of exactly how the wrong medicine got into the cabinet for infants, for instance, to get a grip on what went wrong, but, again, some judgments are easy to make:

- The president of the hospital had no right to accuse anyone of human error prior to a full investigation.
- Those in the hospital responsible for the twins were wrong not to inform the Quaids of the problem.
- It was impolitic in the extreme to have a hospital lawyer at the door to the twins' room when the Quaids arrived. That sent the signal that those in the hospital were far more concerned to limit the hospital's liability than to help solve the problem and save the twins.

These moral judgments are judgments about particular acts and omissions by Baxter and by those in the hospital, and none require any significant analysis.

These moral judgments are easy to make in part because of the relations we take up with others once we occupy a particular role. In taking on the Quaid twins as patients, the physicians and nurses at the hospital took on moral responsibilities to the twins and to the Quaids, responsibilities the administrators in the hospital have an obligation to support and encourage. Those in the hospital breached those responsibilities when they failed to inform the Quaids of the problem. These are responsibilities of the hospital having taken on patients. But the manner in which those in the hospital responded to the problem puts into doubt the integrity of those who responded and those responsible for those responses, and it puts at risk the integrity of everyone else in the hospital. Any potential patient would have to wonder whether the problems the Quaids had was a fluke, uncharacteristic of care at that hospital, or the uncovering of a systemic problem, a feature of the hospital's character, as it were.

Why did those responsible not inform the Quaids when they called? It is difficult not to believe that they hoped to take care of the problem

without the Quaids ever finding out. Why did those responsible have a lawyer by the door waiting to receive the Quaids the next morning? It is difficult not to believe that those responsible had a paramount interest in limiting their liability. This is not the sort of behavior we expect from someone of good character, and it is equally not the sort of behavior we expect from those in a hospital, an organization whose stated purpose is to provide care for the sick and whose employees are supposed to act to further that purpose. Through their actions, those responsible are like a physician's saying in such a situation, "I am more concerned about being sued than about helping the newborns." We would think the physician had a character flaw.

Something more is wrong, that is, than just a single unethical act or omission. Consider Baxter's response. Baxter is a pharmaceutical company. It makes drugs, which it then sells so that patients can get proper medication. Patients and medical care professionals cannot know, and have no easy way of finding out, whether those drugs are properly made, whether they are what they claim to be, whether Baxter has taken due care in manufacturing them so that they are always have the same amount of ingredients, with their ingredients thoroughly mixed, in containers properly marked with the right ingredients of the right size. In short, we must trust that those in charge at Baxter have done what its selling drugs obligates them to do. They failed to do that when they did not recall the former stock. They put children at risk and did so knowingly, aware that the problem of packaging had caused three deaths already.

Those in charge at Baxter put profit over the potential harm that it knew its packaging could cause. They did just what those at Guidant did when they discovered that their implant could short-circuit. They traded the company's reputation for money.

Those in charge at Baxter and Guidant and the hospital did not just make a moral mistake. The way in which all responded to the criticism they received indicates a deeper moral problem. Each pointed the finger of blame at others, trying to deflect criticism from themselves rather than trying to determine what went wrong and fixing the

problem so that such harm could not happen again. Because of that sort of response, we have another sort of moral problem. Those at these companies and the hospital have lost their moral compass. Would you trust a Baxter representative who told you, after yet another "accident," that it was not Baxter's fault? Guidant? The hospital? We all make mistakes, and we can excuse even the most grievous of errors if those making it respond appropriately. But these three responded in a way that puts their corporate character in question.

What is even more morally appalling, and the reason these examples have been chosen, is that those at Baxter, Guidant, and the hospital all have taken on special obligations to help by being in the businesses they are in. Baxter manufactures and sells drugs to help the sick; Guidant designs, manufactures, and sells heart implants to those whose lives depend upon electrical circuits firing to restart their faulty hearts; the hospital is licensed to care for its patients. All three betrayed that obligation to help when they responded by blaming others rather than by investigating what went wrong. These companies and that hospital have lost their way.

This is not a moral judgment about any particular act or omission, but about the nature of these companies—their corporate character. Marriage counselors say that a marriage has moved significantly closer to disintegration when one spouse criticizes the other, not for some particular act or omission, but for being a particular kind of person—from "You forgot to take out the garbage" to "You are a lazy SOB." The judgment of a person's character signals a change in the way we are looking at a person—not as someone who just made a mistake, but someone who makes mistakes, not as someone who failed to do something, but the kind of person who fails to do what needs to be done, not as someone who lied, but a liar. Once that move is made and a person's character is put into question, everything the person does is open to question. Where we once presumed a good character, we now presume a bad one, and where we once assumed a problem was a mistake, out of character for the person, we now assume it is exactly what that sort of person would do.

The judgment of character is a judgment about the internal morality of the person, about the kind of person they are, and that is the sort of judgment we are making about Baxter, Guidant, and the hospital. They did not just make a mistake, but responded in a way that illustrated their true corporate character. They were more concerned about maximizing their profits than about doing what they are obligated to do because of the sorts of companies they are supposed to be. They are like toy companies that purvey toys contaminated by lead and seem unable to ensure that their toys are lead-free. Parents have no way of determining before purchasing a toy whether it contains lead or not, and after purchase, it would be an undue burden on them to have a toy tested for lead before giving it to a child. We rightly expect toy companies to bear that burden and ensure that the toys they sell are safe. Just so, we rightly expect companies like Baxter to do what they can to ensure that their products are safe and are safely dispensed—especially when they have the sort of warning Baxter received from the deaths of three children in Indianapolis. Its failure to answer that wake-up call should create doubt on the part of consumers about the company's commitment to their well-being.

The lesson for engineers, and, indeed, for any professional, is that they display their professional character, the inner morality of the position they have come to occupy in being a professional of a certain sort, in a variety of ways—in what problems they choose, by how they solve those problems, and by how they respond to the inevitable mistakes they make and the failures that occur. We are not interested in their personal morality, to emphasize, what they think about abortion, for instance, but in the inner morality, they have as engineers, the way of looking at the world and of solving problems they come to learn as they learn to be engineers.

Engineers whose design solutions have high failure rates under the stress of ordinary use will display their professional character in their responses. Figuring out why the failure rate is so high and redesigning the artifact to reduce the rate is what engineers are to do, not what great engineers are to do, or even good engineers, but even minimally

competent engineers. It is part of the job description of an engineer that an engineer does not leave failures alone, but fixes them. We would laud praise upon the engineer were the problem solved with a minimum of fuss and expense. We would give extra credit for elegant solutions. We would be reluctant to use an engineer on another project who said, "People must be using it wrong. That's not my problem." If a design provokes errors, it is a problem for the engineer.

We may make this clearer by looking at a particular example, an engineer who is assigned the task of designing a better land mine.[9] Some may fault the engineer morally for agreeing to such a task. The only use to which a land mine can be put is to kill and maim those who unknowingly step on or near it, and it is indiscriminate in whom it kills, taking innocent lives of children as well as others. So a moral question must be raised about whether an engineer has a moral responsibility not to work on such a project. But that moral question is an external moral question, a question about what an engineer ought or ought not to do *as a citizen*. The question we are concerned with is what an engineer *as an engineer* ought or ought not to do *given* that the engineer has the task of designing a better land mine.

What ifs the engineer designed a land mine that exploded if it was jostled in any way in shipping? Or that exploded when moved off the horizontal axis even slightly by anyone placing it in a hole? Or that tended to explode while being manufactured? Or some of whose parts so easily corroded that it exploded unexpectedly or not at all? Or exploded after being stored for a while and so set off the other explosives being stored? Or whose failure rate was over 80 percent? Or whose explosive charge often sputtered instead of exploding?

It might be that the engineer had decided to sabotage the land mine, making those manufacturing and using the land mine pay a steep price for taking part in something so heinous or ensuring that the mine would not harm anyone because it would fail to work. We would then say that the engineer had decided that, *as a citizen*, the best protest was to undermine the land mine, taking it on as a project only to ensure that it would not be done properly.

If the aim is not sabotage, however, and the engineer designed a land mine with any of those faults, we would fault the engineer for failing to fulfill the minimal standards we expect any engineer to uphold. "Not much of an engineer," we would mutter, and we would assign the task to a competent engineer and fire the one who claimed to be an engineer. If that person screwed up the land mine design so badly, what could you trust the person to do on any other project?

We should have the same sort of response to such an engineer as we should have to those in charge of a drug company that fails the patients who rely on it, to those in charge of a heart implant company that puts those who use its implants at greater risk, to those in charge of a hospital seemingly more concerned about its financial well-being than its patients.' We can no longer be sure that they are doing properly what we give them a license to do. We are making a judgment about the corporate characters of the companies and about the engineer's professional character.

Engineers enter into a form of life that requires them to learn to think in a way very different from the way, say, lawyers or physicians think, and, as we have argued, that form of life has its requirements—a set of skills that must be mastered, certain knowledge that must be obtained, and a level of competence in using those skills and mastering that knowledge. These are requirements that are essential to, built into, living that form of life. A person cannot be an engineer without those skills and that knowledge. But they make their own demands.

To have a particular skill is to know how to act under certain circumstances. Failing to act in the proper way, given those circumstances, may be explained away as a fluke, but it will not take much more than one instance of failure for us to deny the person has the skill. A red flag is raised by a surgeon who fails to recognize a swollen appendix and so fails to remove it, or who sees it, but fails to remove it properly, or who removes it properly, but fails to remove it from the patient before stitching the patient up. We can think of a myriad of reasons for such a failure. But if it happens more than once, we will be loath to be the surgeon's patient and presume that those who became

the surgeon's patients were unaware of these problems. The surgeon's behavior in those circumstances is more than we need to deny that the surgeon has the appropriate skills to be operating.

Just so for someone who claims to be an engineer but fails to exhibit the set of skills and kind of knowledge incumbent upon someone who has entered into that form of life. Imagine an engineer who keeps making mistakes in calculating, failing to take the time or have the patience to do it properly. The skill of calculating may seem easy, but it is fraught with importance and pregnant with potential mistakes. A mistake can enter in a variety of different ways, from punching in the wrong data, to reading the conclusion wrongly, to having a program in place that will not guarantee the right answer, and, as we saw with the Mars lander, a mistake can be costly. So we will ultimately banish from the ranks of engineers someone who keeps making mistakes in calculating. That person lacks a requisite skill.

I refer to the skills and knowledge of a profession as its inner morality because these function as norms. We criticize someone who claims to be a lawyer, but fails to know how to make out a will or fails to exercise due care in making one out so that the will is invalid. Just so, we criticize someone who claims to be an engineer, but fails to use properly the skills necessary to be an engineer or marshal the knowledge needed. Such a person has failed to fulfill the inner morality of the profession. Someone who cannot calculate carefully is no engineer.

10

Working with and for Others

§1. External Ethical Issues

We have focused on how ethical considerations enter into the intellectual core of engineering, the source of the intellectual joy that animates it. They enter if only because, once a design solution is realized in an artifact that enters the causal stream of the world, it will have a particular configuration of effects, upstream and downstream, that will cause more or less harm and fewer or more benefits and so will be more or less ethical.

Engineers would be lucky if that were the only way in which ethical considerations enter the discipline. Ethical red flags that arise about a design solution can generally be met by working out an alternative that is not ethically problematic. Such red flags can be handled, in short, by engineers doing what they have been trained to do as engineers.

Unfortunately, ethical considerations enter engineering in two ways that are not amenable to such solutions—if they can be resolved at all. Engineers generally work in teams, and as anyone who has been in a team knows well, all sorts of ethical problems can arise—from those free-riding on what the rest of the team is doing to those not good enough to do their allotted share. They also enter because engineers generally work for a firm or a company such as Boeing. We cannot begin to understand what went wrong at Boeing, for instance, without understanding how the engineers had to respond to choices made at the corporate level that constrained what they could do.

Using a rough but helpful distinction, I call these two new sorts of ethical issues external. They do not arise by the very nature of what it is

to be an engineer. They are not internal to engineering like reworking a design solution that raises a red flag. Engineers do that, not physicians or lawyers. But physicians work with other health-care practitioners, and lawyers sometimes work in teams. And the problems that arise for engineers working in teams are no different in kind from those that arise in teams of lawyers or groups of physicians. They are thus external to any one profession although common to all those where professionals work in teams. The same is true of the problems that arise for professionals working for a firm or a company. Lawyers and physicians find themselves with ethical issues that are not the result of being lawyers or physicians, but of being employed or hired by firms or hospitals.

We will first look at the sort of issues that arise from working with others and then turn to those that arise from working in or for firms or corporations. Both sorts of issues are important and each deserves a book of its own, but given my main focus on showing that ethical considerations are internal to engineering, we will only look briefly at the sorts of problems that arise.

§2. Playing with Others

We have all seen a team that fails to gel, with the members not only not playing together but also, in the worst case, undermining others on the team. I coached youth soccer with a team of girls and boys. The girls learned mostly by age nine that the best way to win was to pass the ball to someone positioned to score. The boys? Some never learned while on the team and hogged the ball whenever they got it. The result was a win/loss record that failed to match the team's potential.

Those who work with others are in a team, and the team can fail to gel in a variety of ways. Any group is open to the possibility of some shirking their duties. That may or may not be harmful to the project the group is engaged in. It may even be a relief to have someone not

particularly helpful not trying to help. But even if we may quietly applaud their shirking, we still must hold them morally culpable for failing to do their share of the work just as we would hold them culpable for not doing it competently or in a timely way. They owe it to the other members to do their share and not put the extra burden on the others to deal with them and what they failed to do.

A team member can cause problems in a variety of ways, but the harms that result are the same:

- The project is put at risk.
- The other members have to deal with the person causing problems as well as take care of what the person failed to do or did badly.

The first harm comes from the team having taken on a project. They may have an independent contractor who has asked for something or employers who told them to do something. In either case, they have ethical obligations to complete the project and complete it in a timely manner. A team member causing problems puts both the project and its timely completion at risk.

We can get a sense of how significant a harm that can be by looking at a bizarre and somewhat bewildering example from medicine. A surgeon and an anesthesiologist ended up wrestling on the floor of the operating room while their elderly patient was under a general anesthetic. They began to argue just before the surgeon was to start the operation. One thing led to another, and they were soon on the floor while the nurse looked after the patient.[1]

The two dramatically illustrated a team's failure to gel. They were part of a team because it takes more than one person to perform surgery. It takes a surgeon, an anesthesiologist, and one or more nurses, and they all were obligated to work together at whatever task they had as a team. Their altercation put the operation and the patient at risk, leaving the nurse to deal not only with the patient, but with the two who were supposed to be operating and were instead having a fracas on the floor.

We have a triple whammy of moral faults, three different grounds for holding the surgeon and anesthesiologist morally culpable:

- In taking the elderly patient on, the surgeon was obligated to do the needed surgery, and as part of the operating team, the anesthesiologist and nurse were also obligated to the patient to do what they needed to do for the operation to be a success. The patient had a corresponding right that the team perform the surgery and perform it in a timely manner.
- The team members each had an obligation to work together to operate on the patient. The failure of the team to gel, to put it mildly, put the patient at an unnecessary risk.
- The three were employees of a hospital or clinic, and they were thus obligated to do what they had been hired to do.

That the same failure can be criticized on different moral grounds should be no cause for surprise. Two Air France pilots had "a physical altercation in the cockpit" on a flight from Geneva to Paris. Other crew members "intervened after hearing the noise," with one staying "in the cockpit until the flight landed safely."[2] The pilots put all the plane's passengers at great risk by failing to work together and failing to do what Air France had hired them to do. That is another triple whammy of ethical faults.

So it is not unusual for us to find more than one reason for holding someone responsible. A friend of mine had his kitchen renovated, but the workers blotched part of the ceiling, leaving it sagging. When he complained, one of the workers said, "We did what we said we were going to do." "But you messed up the ceiling!" The worker responded, "The contract says we will do our best, and that's what we did."

My friend thought the worker must be joking and, after a friendly smile, would apologize and take care of the problem, but the worker was serious, and my friend had to hire another company to fix the ceiling.

The workers who blotched the ceiling failed to do their job competently, and they misrepresented themselves as being competent, both ethical failures and each providing an independent ground for ethical criticism.

§3. Team Work

The ethical problems that arise between those who are supposed to be working together are no different in kind than those that arise between any two individuals, and they are to be resolved, if they can be, in the same way. I once had an older student who had come back for a master's degree complain to me that one of those she managed always gave her backtalk. I asked why, and she said, "I don't care why. I just want him to stop." But if we do not know why someone is doing whatever it is that is causing problems, from backtalk to free loading, we cannot change the behavior. We may stifle it and thus ensure that whatever is causing the difficulty remains and will likely surface in some other way, but if we are to change the behavior, we have to determine its cause and change that.

We always need to ask why. Everything has a cause, and though it may be difficult to figure out what is causing a problem, something is. We need to find out what it is because we cannot change the effect without discovering and changing the cause.

Suppose an engineer has slacked off and is not doing the share of work needed, freeloading on what the rest of the team is doing, but also causing an interruption in the project while the team deals with what has been left undone as well as with the slacker. The team leader will need to sit down and have a quiet and respectful conversation with the other team member, giving that person a chance to explain what is going on.

The problem may be ignorance. The slacker may have somehow missed or misread the timeline for the task assigned and once apprised of it will quickly do what needs doing. That is why the first step in such a situation is always to ask what is going on. That may be the first indication the person has that something is going on.

It is of no use, and almost certainly counterproductive, to get angry and berate the slacker. That does not change whatever it is that is causing the problem. It is of no use, and again counterproductive, to make an issue of the matter in front of the other team members to embarrass and

shame the slacker with the pressure of the group. Again, that does not change what is causing the problem and creates new problems between the slacker and the rest of the team. The team leader needs to tell the person what the problem is and then ask, "What is going on?"

There could be all kinds of causes. It could simply be that the person does not feel confident about doing the task properly and is avoiding it to avoid failure. It could be that an ill spouse or dying parent or problematic child is sapping the person's energy and time. It could be that the person has moral objections to doing the work as one might if assigned to fashion hair triggers for landmines. It could be depression, frustrations with the job that have finally boiled over, or a real animosity with someone on the team. We cannot be sure without asking, and so we cannot be sure we are remedying the situation by anything we might do.

What we are doing when we ask what is going on is finding out the person's reasons. We are to do what we ought to do for any ethical problem. We need to construct an argument we can plausibly attribute to the person causing the problem that would justify, if possible, what the person is doing. The aim is to uncover the operative cause: What is the source of the person's behavior? Only when we find that out can we hope to remedy the problem by changing, if we can, the causal conditions that give rise to it.

Having a team member slack off is only one of the many problems a team may have among themselves. A team may fail to gel for a variety of reasons, and the best solution is to try to preempt the problems by getting clarity at the beginning about what each member is to do and how to resolve any issues that arise.

Here is a start:[3]

a. Make sure all have clarity about the design problem.
b. Have clearly documented roles, allocated fairly, with accountability.
c. Respond to conflict with honesty and kindness; give, accept and address feedback.

d. Communicate with each other and keep a written record of what has been and must be done.

Each of these is a matter for the team to consider as a group. The group should go through the design problem, making sure everyone understands everything about it, marking out and then getting clarity about what seems problematic. Who does what should be a matter for the team to consider, with each person assessing their strengths and weaknesses and having appropriate roles. The roles should be chosen, not assigned, and if there is a conflict or a role no one wants, the team as a whole has to consider how to proceed. They may divvy up the role no one wants and draws straws or fashion some other procedure for settling any conflict over a role. In every case, it is the team that decides, not the leader of the team. That way you get buy-in from everyone at the start.

Each of these items will require revisiting as the project proceeds. That is obvious for keeping the written record, but design problems are going to change as the work progresses and the team discovers new issues those who set the problem did not foresee, and everyone on the team needs to have clarity about any changes that occur.

As the problem changes or as team members run into problems doing their tasks, their roles may change, and everyone needs to be apprized of those changes and agree to them. There is no sense having people take on roles they do not want or are not competent, or the most competent, to handle.

Problems can readily arise when members of a team fail to communicate with each other. If a team member runs into a snag, the others need to know since that may impact what they are doing. One way to ensure that communication occurs is to for the team to meet at the end of each day to discuss what was done and what problems occurred. The team should also ensure that the team notebook is thorough, stating the problems as they arise and the team's understanding of what needs to be done and then which team member is to do which part of the problem, with a clearly agreed-upon timeline for completion

or, where that is not feasible, a stated time to check on progress. The notebook should be updated at least once a day and checked daily by every team member to ensure that everyone knows what everyone else has accomplished or whether anyone is behind schedule or needs some sort of help.

The aims are, first, to avoid as many problems within the team as possible and, second, to solve any problems that do arise through a honest and reasoned discussion among the team members. The more the team members work together to solve any problem, the more the team will gel and work together as a team to solve the design problem.

Once the team has arrived at a solution, it needs to consider two other questions before declaring success. The first concerns issues that arise about the solution itself, and the second concerns issues of sustainability.

§4. Is the Solution Viable?

The solution a team has fastened upon may not be viable or incur such high costs that the problem should not be solved in that way. To determine that a solution is viable, a team needs to answer in the affirmative all the following questions.

- Can we do it? Does the team have the expertise necessary to do it?
- Is it possible to do it? Are the resources available?
- Is it worth doing? Are the benefits sufficient to cover the cost?
- Will it work out given human behavior and complex social systems?
- Is it acceptable to do it? Does it comply with the relevant regulations?

At the base of the door that provides access to set and wind the mechanism of my family's old Scottish wall clock, there is a small piece of decorated glass with "TIME IS MONEY" in gold lettering. The obvious implication is that wasted time is wasted money. Wasted time

is a harm. The last thing engineers should do is to waste their time, and their employer's time, on the solution to a design problem that is not viable.

It would seem not too difficult to determine a design solution's viability. After all, if the chosen solution requires expertise no one on the team has, and adding someone with that expertise is difficult if not impossible, the team should move on. The same is true if the resources are available now, but their future availability is questionable. There is little sense committing to a design solution requiring resources that are likely to become scarce or unavailable.

We could go through the list and make the same obvious points, but we would then miss two complexities that will hamper any team's attempt to determine a solution's viability.

The first is that there is no general answer to any of the questions posed. The variables relevant to a design solution's viability vary from problem to problem. The five questions a team needs to answer can be summed up in one: "Is it feasible?" But that is an open-ended question raising different problems for different design solutions. If the solution is for an artifact to be sold, feasibility turns in part on consumer demand. Does the total cost make it possible to sell the artifact for a reasonable price, one that buyers can afford? The total cost includes not just the materials from which the artifact is to be made, but also workers competent enough to handle any fabrication involved, the cost of transportation to markets as well as storage upon delivery, sales taxes, or any special taxes applicable to that artifact, and so on.

If the design solution is for a walkway elevated across a busy street, one variable concerns testing its stability, and so the design team has to be sure it has available the means to test it properly. The walkway at Florida International was designed to be swung into place after being fully built, but its structural failure, and the loss of life that caused, was due to having the bridge tested by a company that thought it appropriate to ensure that it was structurally sound after, rather than before, positioning it over the roadway. When it failed the test, it collapsed onto the busy street below, killing six.[4]

The engineers who worked on the Boston Tunnel thought it appropriate to have two-ton concrete pieces hung over the roadway, but, among other failures, failed to ensure that the metal fasteners that held those heavy pieces in place were kept dry and would last the life of the tunnel. The fasteners were stored outside and rusted, weakening them enough that one of the large pieces fell on a passing car, killing a passenger.[5]

So one problem a team faces is to mark out all the *particular* variables their design solution invokes. Consider the question of resources. If the solution is realized in a product, will there be enough manufacturing capacity? We need only think of the chip shortage that has hampered the automotive industry in 2021–2022 to understand how difficult it can be to ensure that sufficient resources will be available. The same is true of regulations—local, state, federal, and perhaps international. Laws and regulations are not static, but change regularly, and a change in one jurisdiction can affect an entire industry and, obviously, any design problem that arises within that industry. The standard California set for auto emissions is a case in point. The automotive market is so large in California that auto makers cannot ignore the standard and cannot afford to manufacture automobiles meeting a different standard for the other states. Such an apparently local regulation will clearly affect any design team working on an emissions problem, and, unfortunately for such teams, change is in the air, as it were.

That is the first problem a team faces, identifying the particular variables for its solution. As if that problem were not hard enough, predicting how anything new will affect us and society is, again, almost impossible. The telegraph fundamentally altered the way in which we communicate, electronic transmission maturing to move us from a world with limited communication to this world in which people from opposite sides of the globe can communicate face-to-face in real time. Morse could not have envisaged that result any more than Steve Jobs could have foreseen that cellphones would render obsolete entire landline phone systems like those in Portugal because, once phone companies installed cell towers, citizens could bypass the system and the system's problems.

Those are examples of how inventions can fundamentally alter a society in ways in which the inventors would have been unable to predict. Predicting how something new will fare when introduced into the causal stream of the world can be exceedingly difficult. Even what we might consider minor tinkering may present such problems. A new kind of dog leash may not seem problematic, but, still, consumers must buy it for it to be viable, and what makes consumers purchase such commodities can itself change as fashion changes or the economy tanks.

So what may seem like a simple set of questions for a team to answer turns out to require a great deal of detailed work to identify the particular variables of relevance to its design solution as well as reasonable assumptions about its effects once introduced into the world. We know that predictions about how any new artifact will affect us and society are not reliable.

There is at least one lesson to draw from considering a design solution's viability. The point is to avoid unnecessary harms, from wasted time to the sort of disaster of the Hyatt Regency Hotel walkways, and one way to proceed is to use off-the-shelf items when you can. If your design requires something special, like the rods that were to hold up the walkways in the hotel, you risk introducing variables that have not been tested and found trustworthy by experience.

§5. What Harms Will the Solution Cause?

Besides assessing a design solution's viability, an engineering team needs to examine the design solution to see if there are problems with it when realized in an artifact. Harms can come from the artifact itself, from what is required to produce it, from what happens downstream during its life cycle, and what happens when its life cycle ends. The discussion of each calls for far more than I can provide here, but the examples are meant to provide a good sense of what an extended discussion would entail.

1. The end of its life cycle: A team needs to ask at least three questions:

a. Can it be recycled? Is it likely to be?
b. Can it be safely disposed of? Will it decompose? Pollute the air, water, or land?
c. Are there harms attached to its demise?

Mercedes is a prime example here of a company that has committed to recycling as much of its vehicles as it can when they have reached the end of their lives. It has to recycle its vehicles according to regulations of the European Union, but the redesigns of its vehicles also saved it money, allowing it to reuse material it would otherwise have to purchase, for instance, and avoiding the harms of disposing of the material and obtaining more to use.

The aim is always to avoid unnecessary harms and minimize those that are necessary. We can get some sense of how difficult it can be to create a practice of recycling by looking at the number of cans and plastic bottles we see discarded. Even a financial reward for recycling, howbeit small, is not enough to ensure an artifact will be handled properly.

There is also the question of whether an artifact can be safely disposed of if it is not recycled or cannot be recycled. Will it decompose? Pollute the air, water, or land? As we know from plastic waste, we may well end up with minute particles that pollute us as well as the world. This is a particular problem with nanoparticles used in clothing, cosmetics, and washing machines, for instance, since they cannot be recycled and are minute enough that they can easily enter the food chain and us.[6]

(2) The artifact: The artifact itself can cause harm.

a. Is it or anything in its life cycle harmful—toxic (lead in toys), sharp-edged, demeaning, inappropriate?
b. Is the design likely to mislead a user into making a mistake?
c. If it breaks, are its parts harmful and to what extent?

d. Does it work for all who might use it regardless of sex, gender, age, race, size, or disability?
e. Could it have a negative impact on relationships and existing social systems?
f. Is it durable in its environment?
g. Does it have fail-safes if something malfunctions or breaks or is sabotaged or hacked?

We still keep finding toys containing lead, for instance. It "softens plastic, making a toy more flexible to return to its original shape," but, obviously, an infant chewing on a flexible toy with lead risks ingesting some.[7] Some toys or toy parts are so small they can be easily swallowed. Lego makes many of them, and there are no doubt examples of infants and toddlers ingesting them.[8] Some have sharp edges so that those playing with them risk cutting themselves.[9]

We need not, I think, go through the rest of the harms an artifact may cause. The only one that might need an example is how an artifact can be problematic because it is racist, for instance. The most startling example is a soap dispenser that only recognizes white hands. You get soap by putting your hand under the dispenser. The dispenser recognizes an object there and dispenses soap—unless your hand is black.[10]

The rest of the concerns a team must consider are obvious. If the artifact breaks, are the parts dangerous—sharp or toxic, for instance? Is it durable? One of the most frequent complaints in product reviews is the high failure rate. "Things aren't made the way they used to be" is the standard line, and a failure means that much more for the trash and that much more out of your wallet to replace it.

(3) Production: A team also needs to consider the potential harms caused by producing the artifact:

a. Is there harm in getting what is needed to make it—to the environment, to people?
b. Does the manufacturing process itself create harms—to the workers, to the environment?

The mercury in the Cadillac trunk light is yet again a striking example of how a particular design choice can cause unnecessary harms—to those who are obtaining the mercury as well as those who are exposed to it when its useful life is over. And, of course, it also provides a good example of how a manufacturing process can create harms both to those working with the mercury and on the environment from mercury that escapes during the manufacturing process.

It is all too obvious that any engineering team ought to consider how to avoid such harms. The Cadillac trunk light is misleading only because the harms it caused could have so easily been avoided with other available design solutions, but whatever solution a team proposes, it needs to consider where the material it uses is coming from and whether manufacturing the artifact, if it is manufactured, itself causes unnecessary harms.

(4) Downstream: In looking at the harms in producing an artifact, we were looking upstream, on what is needed to make it, but looking downstream is as essential for a design team:

a. What is its lifespan?
b. Is it easily broken and if it is broken, is it easy to repair with parts easy to find?
c. Are resources (energy, water, materials) and waste produced (emissions) minimized in using it?

We examined the problem of planned obsolescence, but anything we make will have a lifespan. Metal becomes fatigued, tires become threadbare, and computers become so antiquated all too quickly, it seems, that they cannot handle software updates essential to their working well.

It is of little use to talk of the "natural" lifespan of an artifact since its lifespan is a function of such variables as cost. Wind turbines are designed for a twenty-year lifespan even though it is possible, at little cost, to design some components to last far longer. The problem is that it is very expensive to have all the components last far longer, and so the planned twenty-year lifespan is determined not by what is possible, but by what is fiscally feasible.[11]

What could be determined for any household artifact, for instance, is how easy or hard it is to break and how difficult, or easy, and expensive it is to repair it. A toaster? Forget it. Once broken, it is best tossed since replacing it with a new toaster is less expensive than getting it repaired. The ideal is a design solution with few parts that cannot easily break or fail, but can readily be replaced inexpensively if they do. That so few artifacts come close to the ideal may be a testament to how difficult it can be to make things simple or, perhaps more likely, a testament to corporations much preferring to sell more of a product than to sell a product that will last a long time.

The concern for profit also drives the use of resources and is the primary incentive for corporations to pollute the water, land, and air if, and only if, they do not have to pay to clean it up or pay upfront to prevent it. Engineers employed by corporations need to be cognizant of that incentive and counter it as best they can through their design solutions, making sure that their solution requires as few resources and produces as little waste as possible.

Regarding all these issues about what is required to produce an artifact to what happens when its life cycle ends, engineers at the least are to scrub out as many unnecessary harms as possible and reduce the likelihood, extent, magnitude, and persistence of the harms that are left.

§6. External Ethical Relations

We have been looking at engineers working as engineers with other engineers without any concern at all about whom they might be working for. But once we consider employers or contractors, we find engineers facing very different kinds of moral problems than those they face working with other engineers.

It may help to contrast the role morality of engineers here with that of, say, servants. It is part of what it is to be a servant that one serve others. One can be trained as a servant without becoming a servant, but to be

a servant, one must be employed as a servant. Being an employee of a certain type is part of what it is to take on that role. And servants are not unique in this regard. A person who is elected to Congress to represent a district is a representative, and the role morality of that position requires that they represent that district. Whether they do or not, and whether they do so well or not, are different issues. But the role itself is like that of a servant: it requires a relation with others. Engineering does not, and so in becoming an employee, for instance, an engineer takes on moral relations external to what it is to be an engineer. An engineer can fail to do a competent engineering job as an employee, but then the failure is subject to moral criticism on two completely different moral grounds. The engineer failed the test of competence as an engineer and also failed as an employee. The same is true if an engineer is working on a project under contract. An engineer can fail to do what the contractor requires and so be at double moral fault.

Engineering history is full of examples of how engineers have been overruled by management. In Flint, the city manager had the city move from taking its water through the Detroit water system to taking it from the Flint River. The engineer of Flint's water treatment plant, Michael Glasgow, informed the city manager that

> "I do not anticipate giving the OK to begin sending water out anytime soon. If water is distributed from this plant in the next couple weeks, it will be against my direction," Glasgow wrote to state officials, . . . "I need time to adequately train additional staff and to update our monitoring plans before I will feel we are ready. I will reiterate this to management above me, but they seem to have their own agenda."[12]

But when told by the city manager to switch to the Flint River, Glasgow went along with the order—presumably so as to keep his job. Whatever we may think of Glasgow's backbone and understanding of his ethical obligations to his fellow citizens, he faced a problem he should not have had to face. Failing to heed the professional judgment of the engineer in charge of the water treatment plant is the city manager's ethical fault, but Glasgow's response illustrates the ethical complications for

professionals when their professional judgments are ignored by their employers. Wearing two hats is not easy, and so we can find many examples of professionals who are employed and faced with competing obligations, one determined by their profession, the other by their employer.

Perhaps a more striking example concerns GM's pickup trucks and the decision by GM to put 20-gallon fuel tanks on either side of the chassis. GM engineers had assessed that "the fuel tank of the next generation pickup must be mounted outside the cab and as near the center of the vehicle as practical." GM's management wanted to "install 40 gallon capacity to get a greater driving range" to use "as a selling point." The only way to get a 40-gallon capacity at that point in the design process was to place 20-gallon tanks outside the frame, one on either side. This location made them "split like melons" when a truck was hit from the side, as the engineers had foreseen, and "over 2,000 people were killed in fire crashes involving these trucks from 1973 through 2009."[13]

The story gets worse, of course. The engineers scrambled to protect the tanks with shielding, for instance, but with no success.

> At the heart of GM's resistance to improving the safety of its fuel systems was a cost benefit analysis done by Edward Ivey which concluded that it was not cost effective for GM to spend more than $2.20 per vehicle to prevent a fire death.[14]

The $2.20 was not the cost of a fix for the problem, but a judgment that GM should not pay more than that per vehicle to fix the problem—and save more than 2000 lives. Assuming that the cost–benefit analysis was done correctly, it provides an illustration of why we should not use that kind of analysis in making such decisions about safety.

There are few better examples of how solutions to design problems are ethical. Chrysler engineers had the same problem the GM engineers had and "specifically rejected placing the tank outside the frame because of safety concerns."[15] Chrysler management listened to their engineers and put the gas tanks within the frame of the truck. There are obviously

no reports of deaths from a ruptured side tank in any Chrysler truck. GM management and Chrysler management chose different configurations of effects. GM chose a configuration that included a 400-mile range as a selling point, but risked, and caused, many deaths. Chrysler avoided that unnecessary risk because it accepted its engineers' judgment.

These examples of Flint and GM both illustrate one problem engineers can have in working for an employer or under contract. Their professional judgments can be ignored or overruled. These cases fall into the same category as that involving the management at Morton-Thiokol ignoring the judgment of its engineers and approving the launch of the Challenger. These are examples of non-professionals telling professionals that their professional judgments have no special standing and can be overridden by such other matters as making a good sales pitch or trying to ensure that the company's future contracts are not put in jeopardy.

The engineers then have an ethical issue, to follow orders, as it were, or insist on their professional judgments and risk being fired as well as being ignored. The engineer in Flint followed orders, as did the engineers at GM. There was little the engineers at GM could have done to push back against management's decision. Roger Boisjoly at Morton-Thiokol noted one reason when pressed on why he had not pushed back on his management by going public, for instance. He said that in his era one's obligations as an employee outweighed any obligation engineers had to the public. You could complain within the company, that is, and if that was unsuccessful, you had no other recourse.

It is unfortunate if that understanding permeated the profession at the time and, obviously, unfortunate if it still does, but the difficulty Boisjoly and GM engineers faced is only one of the many ways in which a company can create ethical problems for engineers.

We cannot understand what happened regarding Boeing's 737 MAX, for instance, without taking into consideration how decisions Boeing management made, and failed to make, shaped the problems the engineers faced. The most obvious from the engineers' point of view was the management's failure to anticipate that it would need a more fuel-

efficient plane. That would require larger engines best put on a newly designed fuselage. But having failed to plan ahead, Boeing management was forced to use the existing 737 fuselage if it was to get a plane off the ground quickly, and the new larger engines had to be moved forward on the wings to be high enough to avoid hitting the runway. That changed the center of balance of the plane, and management made it the engineers' job to correct the problem somehow.

The engineers at Boeing had other problems. It is not clear if they were communicating with each other, as members of a team should, about the various changes they made in the software. Did the engineers who quadrupled the force pushing down on the stabilizers also delete the default practice of breaking the electronic connection by putting back and letting go of the yoke? It is difficult to see how they could have consulted each other without realizing that the changes would ensure that pilots had problems because of the legacy effects of the default practice. In any event, it is clear that there were problems of communication within Boeing. Their primary test pilot did not find out that MCAS kicked in at 150 mph until he was flying and discovered it kicking in. The engineers did not know that one of their test pilots took over ten seconds to stabilize the plane even though he knew of the software changes. You would think that they ought to have known and that his failure would make a difference to the changes they were making since by FAA standards a pilot is supposed to handle a runaway stabilizer within three seconds.

Unfortunately, whatever was happening within Boeing is only a sample of the kinds of problems engineers encounter as employees or when under contract. Some of their problems were internal to the team. A failure to communicate with each other is an example. These sorts of problems are no different than those that arise in team work and can be addressed, if not resolved, within the team. But other problems are external, caused by individuals outside the team such as the managers at GM.

Such external problems take a number of specific forms. There are problems with resources, which are under the control of management, not of an engineering team. At Morton-Thiokol, the engineers tried

time and again to get the resources they needed to find out exactly what had happened the January previous to the Challenger launch. Despite their need and insistence, they could not get them. Problems also occur when management rearranges the resources for a project midstream, as it were, moving some members of the team to another project, for instance. And then there is Brooks' Law, which states that "adding manpower to a late software project makes it later."[16]

There are problems with how a design problem is formulated, particularly in regard to what those who formulated the problem are trying to achieve. The GM engineers were presented with that kind of problem when they were told that the gas tanks in the trucks had to be on the outside of the frame. The problem really was to find a way to have the trucks go 400 miles on a single full tank, and given that specification of the problem, they might have been able to come up with a solution that was significantly safer than the one management required. They might have been able to work out how to line up two tanks in a row within the frame, for instance, but the goal of achieving 400 miles on a single fill-up was not articulated in the original design problem. Unfortunately, the articulation of that goal no doubt came too late in the design process to permit the engineers to work out a redesign. Deadlines for the completion of such projects are hard to move.

We could go on with more examples of the kinds of external problems an engineer or engineering team may face, and the obvious difficulty is that because they are external, the engineers have little or no control over them.[17] The best you can do is to

a. have open and frequent communication, if you can, with those who are causing the problems, their clients or employers,
b. ask them to consider the impact of their decisions on you and on them as well since their decisions may impact how successful you can be, and
c. take into account how power relations may affect design decisions, which stakeholders are heard, that is, and who wins or loses from a project.

Engineers may well find that those in a corporation to whom they report are in no better position than they are. One problem is almost impossible for either engineers or those in management to change. Corporations have a culture, a sense of how they are to do things and of what matters to them. One analysis of what happened to Boeing is that when it merged with McDonald Douglas and their CEO became CEO of the new Boeing, the culture changed from engineering first to profits first.[18] The bottom line became far more important than ensuring that the engineering was done well. That explains the pressure on the engineers and others to get the work done and the time clocks to remind them that a deadline is approaching, minute-by-minute.

Such corporate cultures can be so pervasive that those within its grasp are hard-pressed to realize they are working within such a culture, let alone understand how it constrains them or challenge it in any way.

So ethical considerations enter into engineering in the way they do for anyone working with or for other. They enter when an engineer takes on those moral relations that come from working for a client, being an employee, taking on a contract, or even from working with other engineers as part of a team. When engineers work for a client, they are obligated to represent the engineering problem clearly, ensure that the problem identified is solved without creating any new problems, and so on. They take on special obligations when they work as a member of an engineering team. They are obligated to resolve disputes between themselves in an amicable manner, for instance. They are obligated to do their part and not free ride on the work of others. When they fail to fulfill those obligations, their failure is a moral failure.

These depend on the kinds of moral relations engineers share with other professionals who work as employees, as members of a team, as contractors. In that sense the moral problems engineers face in these situations are not internal to engineering, necessary implications, that is, of being an engineer. Engineers face these sorts of moral problems

because, like all professionals, they can enter into relations that carry moral weight. Just as a physician who takes on a patient has obligations to the patient that the physician did not have before, an engineer who contracts with a company to solve an engineering problem now has an obligation to the company.

11

Engineering and Ethics

§1. Ethics Internal to Engineering

In the preface to *Essentials of Engineering Design*, to cite a typical remark, Joseph Walton says that the last of the ten chapters "raises ethical questions that an engineer may face from time to time, the non-mathematical problems that need more than a calculator to answer."[1] This remark is typical in two ways:

(a) It implies that engineers will run into ethical problems only occasionally and thus that ethics is not essential to engineering. The issue can be put in the last chapter because it will not make much difference if the class does not get to it since only from "time to time" will the students face any ethical questions as engineers.

(b) It implies that ethics and engineering differ fundamentally. Engineers pose the sort of problem solved by using calculators, while ethics poses "the non-mathematical problems" for which calculators are useless. Engineering is quantitative; ethics is not. The implication is that if ethics were integral to engineering practice, engineering practice would be worse off, its quantitative purity muddied by qualitative matters.

This story of the relationship between engineering and ethics is a popular one, the contrast upon which it depends permeating our understanding of how the arts and the sciences differ from one another. It is no wonder, given such an understanding, that engineers may blanche at the idea that ethics is integral to engineering. The narrative

of engineering is that there are right answers to engineering problems, answers determined by the nature of the problem and not by what anyone may wish or hope or prefer. Either a particular metal will survive the stresses when used to fabricate the girders of a bridge or it will not. If it does not, the girders and, presumably, the bridge will not survive. So engineers must calculate—using a calculator—the right answer to questions about metals and stress. If ethics were integral to engineering, by this narrative, the right answers risk being overwhelmed by issues about which there are no right answers, issues determined not by any calculations, not determined at all, in fact, it is claimed, but subject to the vagaries of subjective bias and preference. This understanding of the nature of engineering and ethics is held by engineers and others alike. But, as we now know, it is mistaken.

Ethics permeates design solutions. We have concentrated upon design problems and upon the way in which ethical considerations enter into design solutions because solving design problems is the intellectual core of engineering. You cannot be an engineer without solving design problems, and so if ethical considerations enter into any solution, you cannot be an engineer without taking on a responsibility to be ethical—whether you recognize you have that responsibility or not.

As we saw with the example of designing a pick to get food and other such things from between one's teeth, no design problem determines any one solution. There is thus no single "right answer" to a design problem. There is space for creativity and innovation, with a myriad of design solutions possible for any single design problem—as various kinds of toothpicks illustrate. There are right answers, of course, to some issues that arise because of a design problem. Some wood will not do for toothpicks, for example, because the stress upon a toothpick when used to pick teeth is too much, and some material will not do because the toothpicks would be too rigid and damage a tooth's enamel. These matters are quantifiable. But quantitative considerations alone do not determine a design solution. An engineer's decision about what to do to solve a particular design problem does not rest wholly on the crystalline clarity that quantification supposedly provides, but on ethical considerations.

We may perhaps see this more clearly by thinking about what happens when a design solution is embodied in an artifact—with no misstep between the solution and the artifact. On the one hand, we can readily imagine an evil genius of an engineer, and we can readily imagine, on the other hand, an engineer adopting as the primary principle that the solutions be benign by design. We can readily imagine, that is, the worst and the most benign of design principles: designing so as to ensure that harm will result and designing so as to ensure, as best we can, that no unnecessary harm will not result. And so we can readily imagine the artifacts that would result from the design solutions of these different engineers. They will have different causal effects when introduced into the world, the one by the evil genius of an engineer producing harms because it was designed to do so, the one by the benign engineer minimizing harms because it was designed to minimize them.

We need not invoke an engineer's intentions, however, to show how ethics enters into the intellectual core of engineering. Because an engineer's design solutions themselves embody differing sets of values, and because the artifacts that embody those solutions have different sets of effects, with different configurations of harms and benefits, an engineer is morally responsible for whatever design solution is chosen. What I have called the arguments from design and effects make this point.

1. The argument from design: In choosing one design solution over another, engineers are choosing one set of values over others. The Japanese toothpick is an example of a design choice that elevates health over a consideration of ease of manufacture, for instance.

2. The argument from effects: When a design solution is realized in an artifact and placed in the causal stream of the world, what follows will be some combination of good and harmful effects. Engineers are responsible, at a moral minimum, for choosing design solutions that do not cause unnecessary harms. They are doing what is morally right if they choose the morally best solution, the one with the most benefits and the fewest and least problematic harms. An engineer is thus responsible for whatever predictable unnecessary harms come from

the artifact that fully realizes that design solution. Like all of us, the engineer is morally obligated not to cause unnecessary harm.

When an engineer does not fulfill that obligation, we can end up with an accident—like the crash of the Colombia airliner with all its attendant harms, 159 people dead and a plane destroyed with the added expense of having to check all autopilot software, retrain pilots, pay those who sue, and on and on. The circumstances are not responsible for the harms. The pilot is not responsible for the harm. The software engineers are. If they had been evil geniuses, we would fault them morally for intending such terrible harms. But even without any evil intent, we should hold them morally accountable. That they did not intend to cause such harms is morally irrelevant. Competent engineers should not produce such shoddy work, and an engineer who does is properly held morally accountable for incompetence.

Any time we introduce harm or what could cause harm into the world, we have a moral problem if we are in a position to preclude that possibility—if the harm is gratuitous because it need not be introduced. That we can imagine an evil genius of an engineer and a benign engineer is all the proof needed that ethics is integral to the design process. Engineering artifacts, that is, can be designed to cause great harm or to be as benign as possible. The latter is morally preferable because it is morally wrong to cause gratuitous harm. In solving the design problems that are the intellectual core of engineering, to repeat, engineers thus have a moral obligation to provide solutions, as best they can, that at the least do not cause unnecessary harm. That means that the engineering decision that such-and-such is the best solution to a design problem has moral weight—a negative weight when it causes harm that some other solution, equally acceptable, would not, a positive weight if it is at least benign.

So ethics enters into the intellectual core of engineering because the design solutions that engineers make themselves embody moral values and because an artifact that embodies that design decision will have its effects in the world, including more or less harm. If the design solution, once realized in an artifact, will cause more harm than necessary, that

solution is morally a mistake. A consideration of how ethics enters engineering deserves to be in the first chapter of any engineering text, not the last.

3. The argument from special skills and knowledge: Engineers also cannot engage in that core enterprise without making use of the knowledge and skills they must learn in order to become engineers, and, as we saw, they have a moral obligation to make use of that knowledge and to make, as it were, skillful use of their skills. This obligation is a third way in which ethics enters engineering. A failure to use their special skills and knowledge makes them morally at fault for the result whatever design solution they may choose. They need to turn their idea into plans to create the corresponding artifact, and they can fail to do that properly.

Just as the design solution proposes a rule for how to solve the design problem—"If you want to have a bridge that reaches from this side to that and is strong enough to support heavy trucks, then here is what you need to do"—so creating a design solution requires the use of rules about how to measure, about what sorts of materials are appropriate in what kinds of situations, and on and on. Engineers can go wrong—morally wrong—by failing to use the proper rules of skill or, using them, failing to use them properly, and they can go wrong by not being prepared with any clear rule at all when they ought to have a vetted rule in hand, prepared ahead of time for catastrophic possibilities. Engineers take on the moral responsibility to use those knowledge and skills properly in becoming engineers.

They take on that responsibility not only in detailing how a design solution is to be turned into an artifact but also in the moral relations they take on. That is a fourth way in which ethics enters into engineering.

4. Moral relations: Ethical considerations enter engineering practice when engineers work with fellow engineers or work on contract or for companies. Ethical considerations are not only internal to engineering, that is, but are embedded in the relations engineers take on as they work with and for others.

Although someone can be an engineer without working with other engineers or on contract or for a company, an engineer who becomes employed or works with other engineers takes on new moral responsibilities. An engineer is no different from any other professional in this regard. A lawyer must take due care in making a will, ensuring that it is properly filled out, notarized, and registered. A failure in any one of these regards will invalidate a will, causing problems to those who were to inherit, among others. The lawyer has obligations to clients, and clients have rights against any lawyer they take on. A broker selling equity in a company must exercise due diligence in investigating that company, ensuring that those making purchases from the broker have what they need to make an informed decision.

A full understanding of how ethics enters engineering would need to consider how morality affects what we see as a problem and how we brainstorm to solve problems. Engineers are trained to see certain kinds of problems—just as are all professionals. An engineer may look at an apple tree and see nothing but good-looking apples almost ready to pick. An horticulturist may look and see a tree that needs serious help. An engineer may be working with team members in tension without realizing what a psychologist would spot right away.

The story about the engineer about to be guillotined makes the point well. When the engineer saw a problem with the guillotine, he could not help himself from thinking like an engineer. A Wall Street trader who saw the problem might say, "Bet you a million to one God will grant me a miracle too!" Not the engineer.

Exploring how values affect what engineers, or any professionals, see as problems opens up a universe of issues we shall not examine in any detail here. Some of these issues arise because of social factors that are not likely to register for those working within the society. An American lawyer sees a dispute as a first step to its final resolution before a judge. A Japanese lawyer sees a dispute as a problem that needs to be resolved so that it not go before a judge where one party will win and both parties will thus lose face since even the winner will

lose face, given the cultural values, by making someone else lose face. An American lawyer's job is to sharpen the points of contention; a Japanese lawyer's is to find the areas of compromise so that the dispute is resolved in a way that satisfies both parties. These differing modes of thought reflect differing social values. Japanese lawyers lose face, and business, if their clients have to go to court to settle a dispute; American lawyers revel in a court victory.

Besides the professional and social differences, there are no doubt personal differences too between different professionals within one society and within a profession. One engineer may look at a car and wonder how to make it go faster; another may look and wonder how to make it greener. We will not pursue here the value implications of the initial sighting of a problem by engineers, but we can understand how rich a source of examples, and of lessons to be learned, we could find by a full examination. The problems they see as well as the solutions they offer are not morally neutral.

We will also not pursue here how morality affects brain-storming, affects, among other things, the range of possible solutions an engineer facing a problem engenders. We are witnesses now to a sea change in the scope of possible solutions in the green revolution we are in. Light bulbs had remained essentially unchanged since they were invented, and it is only now, in the green revolution, that engineers have seen their present configuration as a problem because incandescent bulbs waste too much energy. It is only now that a change in the moral atmosphere, as it were, has triggered the brain storms that are transforming how we light up our world.

In any event, my aim has been to show that ethics is integral to engineering. That it is integral to design solutions more than suffices to make that point. Ethics in fact permeates engineering practice—from the perception of a problem as an engineering problem to the end life of the artifacts that embody design solutions. But each point at which ethics enters requires different considerations and different arguments.

§2. Four Responses

1. "We are not responsible for everything": One of the standard responses to the question of legal liability, and no doubt moral liability as well, is that engineers cannot be held responsible for all the things people do with what they create. If someone drives a car recklessly, the driver is at fault, not the engineers. That is surely correct: engineers are not responsible for everything anyone does with the artifacts that embody their design solutions. There are too many idiots in the world, of too many different kinds, for engineers to foresee and so forestall the mistakes people will make, let alone the silly things they will do with engineering artifacts because they are just not thinking or thinking well. Using a screwdriver to test whether the electric line coming in from outside is hot is not something any engineer is likely to design a screwdriver to survive.

The Darwin awards provide us with a slew of examples, and this one about the screwdriver is also drawn from real life. One year when I was away and rented our house, a tenant used one of my screwdrivers for that purpose. I discovered this when I went to get a screwdriver and found the one in question neatly put away, with a blackened handle and almost no blade. I asked him if he knew what had happened to the screwdriver. He said that the lights had gone out one time and that he was not sure whether the problem was internal to the house or general. "So I stuck the screwdriver where the big wire comes in from outside." He added, "Boy, was I surprised! It just flew out of my hand. I had to dig it out of the wall over there." Engineers are not responsible for *everything* people do with engineering artifacts.

They are responsible, however, for some things people do with those artifacts. That is one point of the example of error-provocative designs. If the artifacts that realize the engineers' design solutions provoke errors for those who use them, the engineers are morally responsible. If the design is so bad that even the most intelligent, well-trained, and highly motivated operator is provoked by the design into making

an error that causes harm—as with the software in that Colombia airliner autopilot—then it would be disingenuous in the extreme for an engineer to say, "I'm not responsible for what people do with what I design!" All we need to do is to imagine an evil genius of an engineer who purposefully creates such designs and then accuses those who use the artifacts realizing those designs of causing harm. Not being responsible for everything people do with engineering artifacts does not get engineers off the moral hook of responsibility for some of what people do with engineering artifacts when what they do is triggered by a faulty design.

Besides, responding that engineers are not responsible for what people do with engineering artifacts presupposes that the only moral issue that arises in engineering concerns the use by an operator of such artifacts, but, as we have seen, morality enters in other ways. Designing a switch that uses mercury when alternative design solutions were feasible is morally wrong not because anyone is going to misuse the switch, but because of the problems of disposing of the mercury in the switches without harm to us and to our environment. Designing an airbag that disadvantages women and small children and advantages males is morally wrong not because anyone does anything with the airbag, but because some drivers had no choice but be put in a far riskier position than they would have been without the airbag.

2. "We could design something completely safe": That brings us to the second response my view is likely to provoke. It is sometimes said that engineers could design something that was completely safe to drive—a tank rather than a car, I have heard it suggested—but that no one would be able to afford it or drive it because it would be so heavy and so well-armored. That may be true, but is irrelevant. Safety should not be all that engineers ought to be concerned about, and ensuring that individuals are safe is not all there is to ethics. No one is physically harmed when our software reports "Unknown Error 0x80040119," when the trunk of our Cadillac breaks because someone closed it the way we normally close trunks, or when we cannot wash our hands because we cannot get a faucet to work, and on and on. But our interests

are set back, and so we are harmed in that way. Safety is not at issue regarding such engineering artifacts. That they can cause harm makes it clear that safety is not the only concern engineers have in making their design solutions moral.

3. "And, besides, we are already ethical!": The third response is a form of disbelief. I can hear engineers telling me, "We're not evil! We're already moral! You are just describing what we already do!" Well, sort of. I am certainly not suggesting the engineers are unethical. Quite the contrary, we would live in a far worse world if they were since their fingerprints are all over our technological universe, and if engineers were generally perversely evil, they could wreak havoc for us. So engineers generally do what they ought to do. I am thus describing what is already the general practice of engineers at least in regard to some ethical matters—for example, safety. But I am suggesting that once engineers realize that their current practice is driven by moral considerations, they will widen the scope of their concerns about minimizing potential harms and self-consciously strive to produce morally better design solutions. They will consider more conscientiously, for instance, the life cycles of the artifacts that realize their design solutions and solve design problems in ways that will at the minimum minimize harms.

4. "And if we are not already ethical, where are we to find the ethics in this book?": Engineers may well wonder, "Where's the ethics? Where's utilitarianism? Where's virtue theory? Where's Kant? How do I resolve ethical problems? How do I know I've got an ethical problem?" There is a hint of virtue theory in our discussion of role morality: we take on certain features, that is, virtues, when we come to occupy a role, and we will need to develop those features to become the best at them that we can be. But there is no discussion on the big ethical theories, no attempt to show how they relate, if at all, to engineering practice, no discussion on how they might help resolve ethical problems engineers face. There are reasons for that.

If engineers adopt the principle "Benign by design!" and conscientiously consider how to avoid harms, they will avoid many ethical problems that may arise because of design choices they would

otherwise have made. The best protection against having to settle moral problems, by appeal to moral theory, is to prevent their occurrence, and the best way to prevent their occurrence in engineering is to avoid unnecessary harms—of all sorts. Engineers do not need any ethical theory to justify avoiding unnecessary harms.

Indeed, putting ethical theories between an engineer and understanding that ethics is integral to engineering is both unhelpful and harmful. We do not need any ethical theory to know that we should not cause unnecessary harm, and it is that ethical principle which permeates the text. Each ethical theory justifies that principle in different ways, but the different justifications do not matter for the claim here that ethics is integral to engineering. Each ethical theory is complex and sometimes more than a little difficult to understand, to put it mildly, and if ethical practice depended upon understanding ethical theory, we would have far less ethical practice than we now do. And the leading contenders for the "proper" ethical theory are at odds with one another, each holding up a different vision of how we ought to live our lives. Philosophers cannot agree on which is morally preferable, and if philosophers cannot agree, we can hardly expect engineers to digest these theories and make a rational and moral choice between them before they engage in engineering practice. As it happens, they do not need to.

They will need to weigh and assess competing harms and benefits. Issues may arise about the weight of competing harms, for instance. Is it morally preferable to solve a problem completely now, even with attendant harm, or to minimize the problem rather than eliminate it, but with far less harm? Is it morally preferable to choose a material for an artifact that takes less energy to produce than a material that takes more energy to produce but will break less easily? It is not obvious how to make such decisions, but philosophers are not obviously any better situated than engineers to do that. Engineers are at least used to weighing and assessing all sorts of competing demands for the artifact that realizes their design solution—inexpensive to produce, long shelf life if that is relevant, easy to ship without breakage, and so on and

so on—and so taking harms explicitly into account and assessing and weighing them is within their experiential base. They are far better positioned than any philosopher, that is, to make such assessments, once it is made clear, it is harms and benefits that are being weighed and assessed and that they have, at the minimum, a moral obligation to minimize potential harms.

These responses will probably not, and should not, exhaust the list of concerns engineers will have about the claim that ethics is integral to engineering practice. If it is integral, and engineers recognize that it is integral, then that practice is going to change and how we teach engineering must change. In teaching students how to think like an engineer, we cannot just focus on the quantitative features that are, indeed, essential to good engineering practice. We are going to have to emphasize imaginative and creative thinking, a working understanding of how we think about and so approach the artifacts of our lives, and a sense of the history of a design solution. We do not want the artifact that realizes a new design solution to stymy us because of the habits we bring to it, and we should take full advantage of the creativity of previous engineers who have thought about the issues and perhaps come up with designs that need to be revived. I have tended to focus on how ethics enters engineering for a lone engineer trying to solve a design problem, but engineering is a social enterprise, with a long history of success and of failure, and engineering education needs to reflect that history if engineers are not to rely just on their own creative resources.

Notes

Preface

1 Wade Robison, Roger Boisjoly, David Hoeker, and Stefan Young, "Representation and Misrepresentation: Tufte and the Morton-Thikol Engineers on the Challenger," *Science and Engineering Ethics* 8 (2002): 1–31; Wade Robison, "Ethical Presentations of Data: Tufte and the Morton-Thiokol Engineers," in *Philosophy and Engineering: Exploring Boundaries, Expanding Connections*, ed. Diane P. Michelfelder, Byron Newberry, and Qin Zhu (Dordrecht: Springer, 2016), pp. 151–62.

2 Richard K. Miller, "Why the Hard Science of Engineering Is No Longer Enough to Meet the 21st Century Challenges," esp. pp. 8ff. Online at http://www.olin.edu/sites/default/files/rebalancing_engineering_education_may_15.pdf (accessed December 7, 2015).

Chapter 1

1 Lucy Perkins, "Human Error Caused Virgin Galactic Crash, Investigators Say," NPR, July 28, 2015. Online at http://www.npr.org/sections/thetwo-way/2015/07/28/427160185/human-error-caused-virgin-galactic-crash-investigators-say (accessed August 9, 2015).

2 Alex Davies, "Blame a Catastrophic Blindspot for the Fatal Virgin Galactic Crash," *Wired,* July 28, 2015. Online at http://www.wired.com/2015/07/blame-catastrophic-blindspot-virgin-galactic-crash/ (accessed August 9, 2015).

3 Online at http://www.goodexperience.com/tib/archives/product_design/ (accessed January 18, 2010).

4 Henry Petroski, *The Toothpick: Technology and Culture* (New York: Alfred A. Knopf, 2007), pp. 250–1.

5 Edward Barnett, "Periodontal and Dental Cleanser and Periodontal Stimulator," U.S. Patent No. 3,775,848 (December 4, 1973), quoted in Petroski, *The Toothpick*, pp. 263–4.
6 Aristotle, *Nicomachean Ethics*, trans. W. D. Ross (Kitchener: Batoche Books, 1999), p. 27.
7 Henry Petroski, *The Evolution of Useful Things* (New York: Alfred A. Knopf, 1995), pp. 22–33.
8 Auto Dismantlers Guide to Recycling Mercury Switches and Mercury Lamps, Environmental Protection Agency, Maine. Online at https://www.maine.gov/dep/mercury/documents/guidancemanual0608.pdf (accessed March 31, 2022).
9 Matt Parker, *Humble Pie: A Comedy of Maths Errors* (New York: Penguin, 2020), p. 81.

Chapter 2

1 We are concentrating upon the simplest of situations, where a person operates an artifact (car, can opener, chain saw). The analysis of other sorts of cases—with multiple operators, for instance—will be more complicated, but this simple case allows us to isolate the variables that matter to understand the causes of an accident.
2 Micheline Maynard and Matthew L. Wald, "Experts Puzzle Over How Flight Overshot Airport," *The New York Times*, October 23, 2009.
3 Gene Park, "FAA Probes whether Go! Pilots Fell Asleep," *Honolulu Star Bulletin* 13, Issue 51 (February 20, 2008). Online at https://archives.starbulletin.com/2008/02/20/news/story08.html (accessed June 18, 2023).
4 Tim Hume, 'Captain of TransAsia Flight 235 Shut Off Working Engine after other Failed: Report,' CNN, July 2, 2015. Online at http://www.cnn.com/2015/07/02/asia/taiwan-transasia-crash-report/ (accessed July 6, 2015).
5 "What Went Wrong On The Day The Music Died?," *All Things Considered*, National Public Radio, February 2, 2009. Online at http://www.npr.org/templates/story/story.php?storyId=100209015.

6 Will Stewart, "Russian Roulette Shock as Wedding Guest Shoots Himself in Party Trick Gone Wrong," *Daily Mail*, March 23, 2010. Online at http://www.dailymail.co.uk/news/article-1259841/Russian-roulette-shock-wedding-guest-shoots-party-trick-gone-wrong.html#ixzz3Nl807ZmU (accessed January 3, 2015). See also http://darwinawards.com/darwin/darwin2000-04.html (accessed January 3, 2015).
7 http://abcnews.go.com/travel/aheadofthecurve/story?id=5930052. See also Matthew L. Wald and Jesse McKinley, "California Bans Texting by Operators of Trains," *The New York Times*, September 19, 2008.
8 Matthew L. Wald, "Expert Says Engineer Sent Text Messages Before Deadly Train Crash," *The New York Times*, January 22, 2010.
9 Joe Morgenstern, "The Fifty-Nine-Story Crisis," *The New Yorker*, May 29, 1995, pp. 45–53.
10 Robison, Boisjoly, Hoeker, and Young, "Representation and Misrepresentation," pp. 1–24.

Chapter 3

1 Juli Clover, "Apple's Butterfly Keyboards vs. Scissor Switch Keyboards," *MacRumors,* June 3, 2020. Online at https://www.macrumors.com/guide/butterfly-keyboard-vs-scissor-keyboard/ (accessed April 22, 2022).
2 Cited in Martin Helander, *A Guide to Human Factors and Ergonomics*, 2nd edn (New York: Taylor & Francis, 2005), pp. 101–2.
3 Brian Naylor, "Toyota Recall Shines Harsh Light on Safety Agency," Morning Edition, National Public Radio, February 4, 2010.
4 Jim Motavalli, "Runaway Toyotas? Investigation of Sudden Acceleration Eerily Recalls Deadly Ford Transmission Issue 25 years Ago," Mother Nature Network. Online at http://www.mnn.com/transportation/cars/blogs/runaway-toyotas-investigation-of-sudden-acceleration-eerily-recalls-deadly-Ford-transmission-issue-25-years-ago (accessed February 4, 2010).
5 Bill Vlasic, "G.M. Enquiry Cites Years of Neglect over Fatal Defect," *New York Times*, June 5, 2014. Online at http://www.nytimes.com/2014/06/06

/business/gm-ignition-switch-internal-recall-investigation-report.html (accessed January 6, 2015).

Chapter 4

1 "Pilot's Wrong Keystroke Led To Crash, Airline Says," *The New York Times,* August 24, 1996, p. 9.
2 Stephen Manes, "When Trust in 'Data' Is Misplaced," *The New York Times,* September 17, 1996, p. C9.
3 "Pilot's Wrong Keystroke Led to Crash, Airline Says."
4 Ibid.
5 Don Phillips, "Putting the Pilot Back in Autopilot," *The Washington Post National Weekly Edition,* April 29–May 5, 1996, p. 19.
6 Summary of the FAA's Review of the Boeing 737 MAX, November 18, 2020, p. 15. Online at https://www.faa.gov/foia/electronic_reading_room/boeing_reading_room/media/737_RTS_Summary.pdf (accessed May 11, 2022).
7 Peter A. DeFazio and Rick Larsen, "Final Committee Report: The Design, Development & Certification of the Boeing 737 MAX," September 16, 2020, p. 142.
8 Thomas Kaplan, "Boeing, FAA Face Scrutiny after Deadly Lion Air Crash," *The Seattle Times*, February 3, 2019.
9 Ibid. See also DeFazio and Larsen. "Final Committee Report," p. 111.
10 Dana Milbank, "After Two Faulty Boeing Jets Crash, the Trump Administration Blames Foreign Pilots," *The Washington Post*, May 16, 2019.
11 Boeing's Fatal Flaw, Frontline PBS, at 37:08-35. Online at https://www.youtube.com/watch?v=wXMO0bhPhCw (accessed December 17, 2022).
12 Thomas Billinghurst, "Airbus Aircraft to Reduce Fuel Consumption by 15% by 2015," *Gulfnews*, November 13, 2013. Online at https://gulfnews.com/business/aviation/airbus-aircraft-to-reduce-fuel-consumption-by-15-by-2015-1.1254747 (accessed December 17, 2022).
13 Gregory Travis, "How the Boeing 737 MAX Disaster Looks to a Software Engineer," *IEEE Spectrum*, April 18, 2019. Online at https://spectrum.ieee

.org/how-the-boeing-737-max-disaster-looks-to-a-software-developer (accessed May 14, 2022).

14 DeFazio and Larsen, "Final Committee Report," p. 37.

15 Ibid., p. 141.

16 James Glanz, Julie Creswell, Thomas Kaplan, and Zach Wichter, "Behind the Lion Air Crash, a Trail of Decisions Kept Pilots in the Dark," *The New York Times*, February 3, 2019.

17 Travis, "How the Boeing 737 MAX Disaster Looks to a Software Engineer." The example of replicating what the plane is doing by sticking one's hand out the window is his.

18 Federal Aviation Administration, Aviation Safety. Online at https://www.faa.gov/news/safety_briefing/2019/media/SE_Topic_19_04.pdf (accessed May 17, 2022).

19 Travis, "How the Boeing 737 MAX Disaster Looks to a Software Engineer."

20 Dominic Gates and Mike Baker, "The Inside Story of MCAS: How Boeing's 737 MAX System Gained Power and Lost Safeguards," *The Seattle Times*, June 19, 2019.

21 John H. Felder, "Floors, Doors, Latches, and Locks," in *The DC-10 Case: A Study in Applied Ethics, Technology, and Society*, ed. John H. Felder and Douglas Birsch (Albany: State University of New York Press, 1992), p. 71.

22 Natalie Kitroeff and Michael S. Schmidt, "Federal Prosecutors Investigating Whether Boeing Pilot Lied to F.A.A.," *The New York Times*, December 15, 2021.

23 Gates and Baker, "The Inside Story of MCAS."

24 Andew Tangel and Andy Pasztor, "Behind Boeing's Decision to Omit Details on Safety System in Lion Air Crash from Manual," *The Wall Street Journal*, December 5, 2018.

25 Natalie Kitroeff and David Gelles, "Boeing C.E.O. Knew about Pilot's Warnings before Second Crash," *The New York Times*, October 29, 2019.

26 Jack Nicas, Natalie Kitroeff, David Gelles, and James Glanz, "Boeing Built Deadly Assumptions into 737 Max, Blind to a Late Design Change," *The New York Times*, June 1, 2019.

27 DeFazio and Larsen, "Final Committee Report," p. 117.

28 Ibid., p. 20.

29 Kitroeff and Schmidt, "Federal Prosecutors Investigating."

30 Aaron Gregg, Jonathan O'Connell, Faiz Diddiqui, and Andrew Ba Tran, "At Tense Meeting with Boeing Executives, Pilots Fumed about being Left in Dark on Plane Software," *The Washington Post*, March 13, 2019.
31 Ashley Halsey III, "Pilots say they were 'in the dark' about Boeing's 737 Safety Update," *The Washington Post*, November 29, 2018.
32 Glanz, Creswell, Kaplan, and Wichter, "Behind the Lion Air Crash."
33 DeFazio and Larsen, "Final Committee Report," p. 21.
34 Summary of the FAA's Final Review, p. 7.
35 Glanz, Creswell, Kaplan, and Wichter, "Behind the Lion Air Crash."
36 Natalie Kitroeff, David Gelles, and Jack Nicas, "The Roots of Boeing's 737 Max Crisis: A Regulator Relaxes Its Oversight," *The New York Times*, July 27, 2019.
37 Nicas, Kitroeff, Gelles, and Glanz, "Boeing Built Deadly Assumptions."
38 Summary of the FAA's Final Review, p. 77.
39 Gates and Baker, "The Inside Story of MCAS."
40 Dominic Gates, "Flawed Analysis, Failed Oversight: How Boeing, FAA Certified the Suspect 737 MAX Flight Control System," March 17, 2019.
41 Summary of the FAA's Final Review, p. 8.
42 Glanz, Creswell, Kaplan, and Wichter, "Behind the Lion Air Crash."
43 DeFazio and Larsen, "Final Committee Report," p. 107.
44 Nicas, Kitroeff, Gelles, and Glanz, "Boeing Built Deadly Assumptions."
45 Ibid.
46 Glanz, Creswell, Kaplan, and Wichter, "Behind the Lion Air Crash."
47 DeFazio and Larsen, "Final Committee Report," p. 135.
48 Amanda Macias and Spencer Kimball, "Boeing waited until after Lion Air crash to tell Southwest safety alert was turned off on 737 Max," CNBC. Online at https://www.cnbc.com/2019/04/28/boeing-didnt-tell-southwest-that-safety-feature-on-737-max-was-turned-off-wsj.html (accessed May 12, 2022).
49 DeFazio and Larsen, "Final Committee Report," pp. 125–8.
50 Ibid., p. 128.
51 Ibid., pp. 13 and 15.
52 Ibid., p. 23.
53 Ibid., p. 105.
54 Gates, "Flawed Analysis, Failed Oversight."

55 DeFazio and Larsen, "Final Committee Report," p. 201, quoting Dr. Mica Endsley.
56 Ibid., p. 24.
57 David Schaper, "Pilots Criticize Boeing, Saying 737 Max 'Should Never Have Been Approved'," NPR, June 19, 2019.
58 Jamie Freed, "Boeing Considered System Redesign before Accidents: NTSB Report," *Reuters*, October 25, 2019.
59 Gates and Baker, "The Inside Story of MCAS."
60 David Gelles and Natalie Kitroeff, "Boeing and F.A.A. Faulted in Damning Report on 737 Max Certification," *New York Times*, October 11, 2019.
61 Gates and Baker, "The Inside Story of MCAS."
62 Boeing's Fatal Flaw, Frontline PBS, at 38:31-40.
63 Natasha Frost, "The 1997 Merger that Paved the Way for the Boeing 737 Max Crisis," *Quartz*, January 3, 2020. Online at https://qz.com/1776080/how-the-mcdonnell-douglas-boeing-merger-led-to-the-737-max-crisis (accessed December 5, 2022).
64 John Markoff, "Report Cites Dangers of Autonomous Weapons," *The New York Times*, February 28, 2016.

Chapter 5

1 Stephanie Saul, "Some Sleeping Pill Users Range Far Beyond Bed," *The New York Times*, March 8, 2008; "Ambien in the Driver's Seat," *The New York Time*s, March 11, 2008; Stephanie Saul, "Study Links Ambien Use to Unconscious Food Forays," *The New York Times*, March 14, 2008.
2 Steven Morris, "Devoted Husband Who Strangled Wife in His Sleep Walks Free from Court," *The Guardian*, November 20, 2009.
3 *M'Naghten's Case* (1843) 10 C & F 200.
4 Wade Robison, "In the Moral Zone," *Teaching Ethics* 8, no. 2 (Spring 2008): 57–78.
5 Rick Bragg, "New Trial Is Sought for Inmate Whose Lawyer Slept in Court," *The New York Times*, January 23, 2001.

6 Linda Greenhouse, "Inmate Whose Lawyer Slept Gets New Trial," *The New York Times*, June 4, 2002.
7 Walt Bogdanich, "At V.A. Hospital, a Rogue Cancer Unit," *The New York Times*, June 21, 2009.
8 Gilbert Ryle, *The Concept of Mind* (London: Hutchinson, 1949).
9 Aristotle, *Nicomachean Ethics*, p. 27.

Chapter 6

1 Ibid.
2 Joel Feinberg, *Harm to Others*, Vol. 1 of *Moral Limits of Criminal Law* (Oxford: Oxford University Press, 1987).
3 Don Gotterbarn, "Computer Ethics: Responsibility Regained," *National Forum: The Phi Kappa Phi Journal*, LXXI (1991): #2; Terrell Ward Bynum, and Simon Rogerson, *Computer Ethics and Professional Responsibility* (Oxford: Blackwell, 2004), p. 110; Robert Riser and Don Gotterbarn, "Ethics Activities in Computer Science Courses." Online at http://csciwww.etsu.edu/gotterbarn/ArtTE2.htm.
4 Barry Meier, "Defective Heart Devices Force Some Scary Medical Decisions," *The New York Times*, June 20, 2005.
5 Barry Meier, "Repeated Defect in Heart Devices Exposes a History of Problems," *The New York Times*, October 20, 2005.
6 Ibid.
7 *Report of the Independent Panel of Guidant Corporation*, March 20, 2006, p. 33.
8 Timothy Williams, "Citing Failures, Guidant Will Recall Thousands of Defibrillators," *The New York Times*, June 17, 2005.
9 Ibid.
10 Barry Meier, "Concern About New Design for Heart Devices," *The New York Times*, December 11, 2008.
11 Robert G. Hauser, "A Better Method for Preventing Adverse Clinical Events Caused by Implantable Cardioverter-Defibrillator Lead Fractures?," *Circulation* 118, no. 21 (2008): 2117ff.

Chapter 7

1 Jeremy W. Peters, "MOTORING; Unraveling the Mystery of Ford's Fire-Prone Switches," *The New York Times*, August 27, 2006.
2 David Barboza, "Firestone Workers Cite Lax Quality Control," *The New York Times*, September 15, 2000.
3 Andrew Martin, "Chinese Tires Are Ordered Recalled," *The New York Times*, June 26, 2007.
4 James Barron, "THE BLACKOUT OF 2003: THE OVERVIEW; POWER SURGE BLACKS OUT NORTHEAST, HITTING CITIES IN 8 STATES AND CANADA; MIDDAY SHUTDOWNS DISRUPT MILLIONS," *The New York Times*, August 15, 2003. See also http://en.wikipedia.org/wiki/Northeast_Blackout_of_2003.
5 http://wikicars.org/en/Airbag.
6 Carin M. Olson, Peter Cummings and Frederick P. Rivara, "Association of First- and Second-Generation Air Bags with Front Occupant Death in Car Crashes: A Matched Cohort Study," *American Journal of Epidemiology* 164, no. 2 (2006): 161.
7 Roger Saul et al., "DESCRIPTION AND PERFORMANCE OF THE HYBRID III THREE-YEAR-OLD, SIX-YEAR-OLD AND SMALL FEMALE TEST DUMMIES IN RESTRAINT SYSTEM AND OUT-OF-POSITION AIR BAG ENVIRONMENTS," Transportation Research Center Inc. United States Paper Number 98S7-O-01.
8 http://www.sfchronicle.us/cgi-bin/article.cgi?f=/n/a/2009/08/10/national/w160656D02.DTL&type=science#ixzz0OXFDGgXX.
9 Wade Robison, *Decisions in Doubt: The Environment and Public Policy* (Hanover: University Press of New England, 1994).
10 Daimler, Sustainability Report, 2011. Online at http://sustainability.daimler.com/reports/daimler/annual/2012/nb/English/4545/recycling.html (accessed January 21, 2015).
11 Askiner Gungor and Surendra M. Gupta, "Issues in Environmentally Conscious Manufacturing and Product Recovery: A Survey," *Computers & Industrial Engineering* 36 (1999): 823. See also S. B. Billatos and V. V. Nevrekar, "Challenges and Practical Solutions to Designing for the Environment," ASME Design for Manufacturability Conference, Chicago, IL, March 14–17, 1994, pp. 49–64.

12 John Voelcker, "Who Knew? A Car Battery Is the World's Most Recycled Product," *Green Car Reports*, March 31, 2011. Online at http://www.greencarreports.com/news/1044372_who-knew-a-car-battery-is-the-worlds-most-recycled-product (accessed January 21, 2015).
13 Feinberg, *Harm to Others*.
14 Henry Petroski, *To Engineer Is Human: The Role of Failure in Successful Design* (Vantage Books: New York, 1992), pp. 85-93.
15 See http://www.boston.com/news/specials/big_dig_ceiling_collapse/ for a list of articles from the *Boston Globe* chronicling the various problems with the Boston tunnel and, in particular, the problems with the anchoring system for the ceiling tiles, one of which fell when its anchors gave way and crushed a woman in a car.
16 Pete Carey, "Floodwalls' Collapse in New Orleans Linked to Soil Failure," *The Seattle Times,* October 8, 2005.
17 Matthew L. Wald and Kenneth Chang, "Minneapolis Bridge Had Passed Inspection," *The New York Times*, August 3, 2007.
18 Atul Gawande, "The Way We Age Now," *The New Yorker*, April 30, 2007. Online at http://www.newyorker.com/reporting/2007/04/30/070430fa_fact_gawande?currentPage=2.
19 http://clearviewhwy.com/WhatIsClearviewHwy/index.php.
20 http://clearviewhwy.com/WhatIsClearviewHwy/HowItWorks/letterformDesign.php.
21 Joshua Yaffa, "The Road to Clarity," *The New York Times Magazine,* August 12, 2007.
22 Ibid.
23 http://clearviewhwy.com/ResearchAndDesign/legibilityStudies.php.
24 Yaffa, "The Road to Clarity."
25 https://www.transportation.gov/fastlane/fonts-and-highway-safety.
26 Henry Petroski, "Easy Reading Road Signs Head to the Offramp," *The New York Times*, February 26, 2016.
27 U.S. Department of Transportation, Memorandum, March 28, 2018. Online at https://mutcd.fhwa.dot.gov/resources/interim_approval/ia5/ia5_reinstatement.pdf (accessed March 12, 2023).

Chapter 8

1 "Doctor Who Cut Off Wrong Leg Is Defended by Colleagues," *The New York Times*, September 17, 1995.
2 Paul Sisson, "Kaiser Hospital Fined for Removing Wrong Kidney," *U-T San Diego News*, December 20, 2012. Online at http://www.utsandiego.com/news/2012/dec/20/kaiser-hospital-fined-for-removing-wrong-kidney/ (accessed January 6, 2013).
3 "Florida Doctor Who Took Out Wrong Organ Fined $5000," *Insurance Journal*, June 9, 2010. Online at http://www.insurancejournal.com/news/southeast/2010/06/09/110568.htm (accessed January 3, 2013).
4 Greenhouse, "Inmate Whose Lawyer Slept Gets New Trial,"
5 Jon Nordheimer, "New Jersey Autopsy Misses Two Bullets in a Man's Head," *The New York Times*, October 20, 1993.
6 Aristotle, *Nichomachean Ethics*, p. 27.
7 http://www.typewritermuseum.org/collection/index.php3?machine=blick1&cat=ks.
8 Petroski, *To Engineer Is Human*, p. 87; see also Matthys Levy and Mario Salvadori, *Why Buildings Fall Down: How Structures Fail* (New York: W. W. Norton & Co., 1994), pp. 221–30.
9 Petroski, *To Engineer Is Human*, p. 89.
10 Ibid., p. 88.
11 Ibid., pp. 86–7.
12 Ibid., p. 89.
13 Todd Mytkowicz, Amer Diwan, Matthias Hauswirth, and Peter F. Sweeney, "Producing Wrong Data Without Doing Anything Obviously Wrong!," Fourteenth International Conference on Architectural Support for Programming Languages and Operating Systems, March 7-11, 2009, Washington, D.C.
14 NASA release 99-113, September 30, 1999.
15 http://www.reuters.com/article/idUSTRE60P50O20100126 (accessed February 1, 2010).
16 http://english.pravda.ru/society/stories/06-10-2006/84912-amputation-0 (accessed February 1, 2010).

Chapter 9

1 Petroski, *To Engineer Is Human,* p. 164; Levy and Salvadori, *Why Buildings Fall Down*, pp. 107–20.
2 Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (Chicago: University of Chicago Press, 1997), pp. 278ff.; Robison, Boisjoly, Hoeker, and Young, "Representation and Misrepresentation," pp. 1–24.
3 Vaughan, *The Challenger Launch Decision*, p. 317.
4 Ibid., p. 318.
5 Michael Davis, *Thinking Like An Engineer: Studies in the Ethics of a Profession* (New York: Oxford University Press, 1998), p. 67.
6 Report to the President by the Presidential Commission on the Space Shuttle Challenger Accident (Washington DC: Government Printing Office, June 6, 1986), p. 95.
7 Tara Parker-Hope, "A Hollywood Family Takes on Medical Mistakes," *The New York Times*, March 17, 2008. Online at http://well.blogs.nytimes.com /2008/03/17/a-hollywood-family-takes-on-medical-mistakes/. Quotations are from 60 Minutes, March 16, 2008, available online at the link to Parker-Hope.
8 For a photograph of the two bottles, see Crystal Phend, "Lower-Cost Heparin Prophylaxis in ICU?—Low-molecular weight heparin is a bargain for VTE prevention," MedPage Today, November 3, 2014. Online at https://www.medpagetoday.com/cardiology/prevention/48387; accessed March 14, 2023. I have been unable to verify the photographer, but the image has been reproduced countless times and is probably the work of a photographer at the Indianapolis Star.
9 Wade Robison, "Design Problems and Ethics," in *Philosophy and Engineering: An Emerging Agenda*, Vol. 2 of the Series Philosophy of Engineering and Technology, ed. Ibo van de Poel and David E. Goldberg (Dordrecht: Springer, 2009), pp. 205–14.

Chapter 10

1 "Doctors Fined For Fight in Operating Room," *The New York Times*, November 28, 1993.

2 Merlyn Thomas, "Two Air France Pilots Suspended After Cockpit Fight," *BBC News*, August 29, 2022. Online at https://www.bbc.com/news/world-europe-62712278 (accessed September 1, 2022).

3 The list that follows and the lists further on are the result of a project between me and two engineers, Sarah Brownell and Beth DeBartolo, at the Rochester Institute of Technology. We developed a one-page list called "Tracking Harms" for engineers to use to ensure that their design solutions at least satisfied the minimal ethical requirement not to cause unnecessary harm. The list has been vetted by its use in a large number of engineering courses at the Institute, but I have reworked some of the wording for the narrative.

4 See, e.g., Francisco Alvarado, Susan Svriuga, Falz Siddiqui, and Aaron C. Davis, "Death Toll Rises to Six after New Pedestrian Bridge Collapses Near Miami, Crushing Cars Underneath," *The Washington Post,* March 16, 2018.

5 Pam Belluck, "Woman Killed as Slab Falls From Big Dig Tunnel," *The New York Times*, July 11, 2006. Online at http://www.nytimes.com/2006/07/11/us/11cnd-boston.html?mcubz=1 (accessed August 18, 2017).

6 Wade Robison, "Nano-Technology, Ethics, and Risks," *Nanoethics* 5, Issue 1 (2011): 1–13.

7 "Lead in Toys," Center for Disease Control. Online at https://www.cdc.gov/nceh/features/leadintoys/index.html (Accessed August 7, 2022).

8 "Small Parts for Toys and Children's Products Business Guidance." Online at https://www.cpsc.gov/Business--Manufacturing/Business-Education/Business-Guidance/Small-Parts-for-Toys-and-Childrens-Products (accessed August 7, 2022).

9 "CPSC Proposes Guidelines For Sharp Points And Edges On Toys." Online at https://www.cpsc.gov/Newsroom/News-Releases/1977/CPSC-Proposes-Guidelines-For-Sharp-Points-And-Edges-On-Toys (accessed August 7, 2022).

10 Taylor Synclair Goethe, "Bigotry Encoded: Racial Bias in Technology," *Rochester Institute of Technology Reporter*, March 2, 2019.

11 "Operational and Maintenance Costs for Wind Turbines." Wind Measurement International. Online at http://www.windmeasurementinternational.com/wind-turbines/om-turbines.php (accessed August 9, 2022).
12 Ray Sanchez, Sara Ganim, and Linh Tran, "Flint Water Crisis: Who's been Charged, Who Hasn't," CNN, April 22, 2016. Online at https://www.cnn.com/2016/04/21/us/flint-crisis-who-was-charged/index.html (accessed September 16, 2022).
13 Center for Auto Safety, "History of the GM Side Saddle Gas Tank Defect," *The Washington Post*, February 5, 1993. Online at https://www.autosafety.org/history-gm-side-saddle-gas-tank-defect/ (accessed September 22, 2022).
14 Ibid.
15 Ibid.
16 Itamar Shatz, "Brooks' Law: Adding Manpower to a Late Project Makes It Later." Online at https://effectiviology.com/brooks-law/ (accessed October 2, 2022).
17 These sorts of problems are nicely laid out in Robert Block, *The Politics of Projects* (New York: Yourdon Press, 1983), p. 5.
18 Natasha Frost, "The 1997 Merger that Paved the Way for the Boeing 737 Max Crisis," *Quartz*, January 3, 2020; reprinted by Yahoo! Finance. Online at https://finance.yahoo.com/news/1997-merger-paved-way-boeing-090042193.html (accessed December 14, 2022).

Chapter 11

1 Joseph W. Walton, *Essentials of Engineering Design* (St. Paul: West Publishing Co., 1991), p. xv.

Bibliography

Alvarado, Francisco, Susan Svriuga, Falz Siddiqui, and Aaron C. Davis. "Death Toll Rises to Six After New Pedestrian Bridge Collapses Near Miami, Crushing Cars Underneath," *The Washington Post*, March 16, 2018.

Aristotle. *Nicomachean Ethics*. Translated by W. D. Ross. Kitchener: Batoche Books, 1999.

Auto Dismantlers Guide to Recycling Mercury Switches and Mercury Lamps, Environmental Protection Agency, Maine.

Barboza, David. "Firestone Workers Cite Lax Quality Control," *The New York Times*, September 15, 2000.

Barnett, Edward. "Periodontal and Dental Cleanser and Periodontal Stimulator," U.S. Patent No. 3,775,848, December 4, 1973.

Barron, James. "THE BLACKOUT OF 2003: THE OVERVIEW; POWER SURGE BLACKS OUT NORTHEAST, HITTING CITIES IN 8 STATES AND CANADA; MIDDAY SHUTDOWNS DISRUPT MILLIONS," *The New York Times*, August 15, 2003.

Belluck, Pam. "Woman Killed as Slab Falls from Big Dig Tunnel," *The New York Times*, July 11, 2006. Online at http://www.nytimes.com/2006/07/11/us/11cnd-boston.html?mcubz=1.

Billatos, S. B. and V. V. Nevrekar. "Challenges and Practical Solutions to Designing for the Environment," ASME Design for Manufacturability Conference, Chicago, March 14–17, 1994, 49–64.

Billinghurst, Thomas. "Airbus Aircraft to Reduce Fuel Consumption by 15% by 2015," *Gulfnews*, November 13, 2013. Online at https://gulfnews.com/business/aviation/airbus-aircraft-to-reduce-fuel-consumption-by-15-by-2015-1.1254747.

Block, Melissa. "What Went Wrong On The Day The Music Died?" *All Things Considered*, National Public Radio, February 2, 2009.

Block, Robert. *The Politics of Projects*. New York: Yourdon Press, 1983.

Boeing's Fatal Flaw, Frontline PBS. Online at https://www.youtube.com/watch?v=wXMO0bhPhCw.

Bogdanich, Walt. "At V.A. Hospital, a Rogue Cancer Unit," *The New York Times*, June 21, 2009.

Bragg, Rick. "New Trial Is Sought for Inmate Whose Lawyer Slept in Court," *The New York Times*, January 23, 2001.

Bynum, Terrell Ward and Simon Rogerson. *Computer Ethics and Professional Responsibility*. Oxford: Blackwell, 2004.

Carey, Pete. "Floodwalls' Collapse in New Orleans Linked to Soil Failure," *The Seattle Times*, October 8, 2005.

Center for Auto Safety. "History of the GM Side Saddle Gas Tank Defect," *The Washington Post*, February 5, 1993. Online at https://www.autosafety.org/history-gm-side-saddle-gas-tank-defect/.

Clover, Juli. "Apple's Butterfly Keyboards vs. Scissor Switch Keyboards," *MacRumors*, June 3, 2020.

"CPSC Proposes Guidelines For Sharp Points And Edges On Toys." Online at https://www.cpsc.gov/Newsroom/News-Releases/1977/CPSC-Proposes-Guidelines-For-Sharp-Points-And-Edges-On-Toys.

Daimler Sustainability Report. 2011. Online at http://sustainability.daimler.com/reports/daimler/annual/2012/nb/English/4545/recycling.html.

Davies, Alex. "Blame a Catastrophic Blindspot for the Fatal Virgin Galactic Crash," *Wired*, July 28, 2015.

Davis, Michael. *Thinking Like An Engineer: Studies in the Ethics of a Profession*. New York: Oxford University Press, 1998.

DeFazio, Peter A. and Rick Larsen. *Final Committee Report: The Design, Development & Certification of the Boeing 737 MAX*, September 16, 2020.

"Doctor Who Cut Off Wrong Leg Is Defended by Colleagues," *The New York Times*, September 17, 1995.

"Doctors Fined For Fight in Operating Room," *The New York Times*, November 28, 1993.

Federal Aviation Administration. "Aviation Safety." Online at https://www.faa.gov/news/safety_briefing/2019/media/SE_Topic_19_04.pdf.

Feinberg, Joel. *Harm to Others,* Vol. 1 *of Moral Limits of Criminal Law*. Oxford: Oxford University Press, 1987.

Felder, John H. "Floors, Doors, Latches, and Locks," in *The DC-10 Case: A Study in Applied Ethics, Technology, and Society*, edited by John H. Felder and Douglas Birsch. Albany: State University of New York Press, 1992.

"Florida Doctor Who Took Out Wrong Organ Fined $5000," *Insurance Journal*, June 9, 2010.

Freed, Jamie. "Boeing Considered System Redesign before Accidents: NTSB Report," *Reuters*, October 25, 2019.

Frost, Natasha. "The 1997 Merger that Paved the Way for the Boeing 737 Max Crisis," *Quartz*, January 3, 2020. Online at https://qz.com/1776080/how-the-mcdonnell-douglas-boeing-merger-led-to-the-737-max-crisis.

Gates, Dominic. "Flawed Analysis, Failed Oversight: How Boeing, FAA Certified the Suspect 737 MAX Flight Control System," *The Seattle Times*, March 17, 2019.

Gates, Dominic and Mike Baker. "The Inside Story of MCAS: How Boeing's 737 MAX System Gained Power and Lost Safeguards," *The Seattle Times*, June 19, 2019.

Gawande, Atul. "The Way We Age Now," *The New Yorker*, April 30, 2007.

Gelles, David and Natalie Kitroeff. "Boeing and F.A.A. Faulted in Damning Report on 737 Max Certification," *The New York Times*, October 11, 2019.

Glanz, James, Julie Creswell, Thomas Kaplan, and Zach Wichter. "Behind the Lion Air Crash, a Trail of Decisions Kept Pilots in the Dark," *The New York Times*, February 3, 2019.

Goethe, Taylor Synclair. "Bigotry Encoded: Racial Bias in Technology," *Rochester Institute of Technology Reporter*, March 2, 2019.

Gotterbarn, Don. "Computer Ethics: Responsibility Regained," *National Forum: The Phi Kappa Phi Journal* LXXI, no. 2 (1991): 26.

Greenhouse, Linda. "Inmate Whose Lawyer Slept Gets New Trial," *The New York Times*, June 4, 2002.

Gregg, Aaron, Jonathan O'Connell, Faiz Diddiqui, and Andrew Ba Tran. "At Tense Meeting with Boeing Executives, Pilots Fumed about Being Left in Dark on Plane Software," *The Washington Post*, March 13, 2019.

Gungor, Askiner and Surendra M. Gupta, "Issues in Environmentally Conscious Manufacturing and Product Recovery: A Survey," *Computers & Industrial Engineering* 36 (1999): 823.

Halsey III, Ashley. "Pilots Say They were "in the dark" about Boeing's 737 Safety Update," *The Washington Post*, November 29, 2018.

Hauser, Robert G. "A Better Method for Preventing Adverse Clinical Events Caused by Implantable Cardioverter-Defibrillator Lead Fractures?," *Circulation* 118, no. 21 (November 8, 2008): 2117ff.

Helander, Martin. *A Guide to Human Factors and Ergonomics*, 2nd ed. New York: Taylor & Francis, 2005.

Hume, Tim. "Captain of TransAsia Flight 235 Shut Off Working Engine after Other Failed: Report," CNN, July 2, 2015.

Isbell, Douglas, Mary Hardin, and Joan Underwood. "Mars Climate Orbiter Team Finds Likely Cause of Loss," NASA Release 99–113, September 30, 1999.

Kaplan, Thomas. "Boeing, FAA Face Scrutiny after Deadly Lion Air Crash," *The Seattle Times*, February 3, 2019.

Kitroeff, Natalie and David Gelles. "Boeing C.E.O. Knew about Pilot's Warnings before Second Crash," *The New York Times*, October 29, 2019.

Kitroeff, Natalie, David Gelles, and Jack Nicas. "The Roots of Boeing's 737 Max Crisis: A Regulator Relaxes Its Oversight," *The New York Times*, July 27, 2019.

Kitroeff, Natalie and Michael S. Schmidt. "Federal Prosecutors Investigating Whether Boeing Pilot Lied to F.A.A.," *The New York Times*, December 15, 2021.

"Lead in Toys," Center for Disease Control. Online at https://www.cdc.gov/nceh/features/leadintoys/index.html.

Levy, Matthys and Mario Salvadori. *Why Buildings Fall Down: How Structures Fail*. New York: W. W. Norton & Co., 1994.

Macias, Amanda and Spencer Kimball. "Boeing Waited until after Lion Air Crash to Tell Southwest Safety Alert was Turned Off on 737 Max," CNBC. Online at https://www.cnbc.com/2019/04/28/boeing-didnt-tell-southwest-that-safety-feature-on-737-max-was-turned-off-wsj.html.

Manes, Stephen. "When Trust in "Data" Is Misplaced," *The New York Times*, September 17, 1996.

Markoff, John. "Report Cites Dangers of Autonomous Weapons," *The New York Times*, February 28, 2016.

Martin, Andrew. "Chinese Tires Are Ordered Recalled," *The New York Times*, June 26, 2007.

Maynard, Micheline and Matthew L. Wald, "Experts Puzzle Over How Flight Overshot Airport," *The New York Times*, October 23, 2009.

Mazzetti, Mark and Matt Apuzzojan. "C.I.A. Officers Are Cleared in Senate Computer Search," *The New York Times*, January 14, 2015.

Meier, Barry. "Concern about New Design for Heart Devices," *The New York Times*, December 11, 2008.

Meier, Barry. "Defective Heart Devices Force Some Scary Medical Decisions," *The New York Times*, June 20, 2005.

Meier, Barry. "Repeated Defect in Heart Devices Exposes a History of Problems," *The New York Times*, October 20, 2005.

Milbank, Dana. "After two faulty Boeing jets crash, the Trump administration blames foreign pilots," *The Washington Post*, May 16, 2019.

Miller, Richard K. "Why the Hard Science of Engineering Is No Longer Enough to Meet the 21st Century Challenges," 8ff. Online at http://www.olin.edu/sites/default/files/rebalancing_engineering_education_may_15.pdf.

M'Naghten's Case, see *Queen v. M'Naghten*.

Morgenstern, Joe. "The Fifty-Nine-Story Crisis," *The New Yorker*, May 29, 1995.

Morris, Steven. "Devoted Husband Who Strangled Wife in His Sleep Walks Free from Court," *The Guardian*, November 20, 2009.

Motavalli, Jim. "Runaway Toyotas? Investigation of Sudden Acceleration Eerily Recalls Deadly Ford Transmission Issue 25 Years Ago," Mother Nature Network. Online at http://www.mnn.com/transportation/cars/blogs/runaway-toyotas-investigation-of-sudden-acceleration-eerily-recalls-deadly.

Mytkowicz, Todd, Amer Diwan, Matthias Hauswirth, and Peter F. Sweeney. "Producing Wrong Data Without Doing Anything Obviously Wrong!," Fourteenth International Conference on Architectural Support for Programming Languages and Operating Systems, March 7–11, 2009.

Naylor, Brian. "Toyota Recall Shines Harsh Light on Safety Agency," Modern Edition, National Public Radio, February 4, 2010.

Nicas, Jack, Natalie Kitroeff, David Gelles, and James Glanz. "Boeing Built Deadly Assumptions into 737 Max, Blind to a Late Design Change," *The New York Times*, June 1, 2019.

Nordheimer, Jon. "New Jersey Autopsy Misses Two Bullets in a Man's Head," *The New York Times*, October 20, 1993.

Olson, Carin Met, Peter Cummings, and Frederick P. Rivara. "Association of First- and Second-Generation Air Bags with Front Occupant Death in Car Crashes: A Matched Cohort Study," *American Journal of Epidemiology* 164, no. 2 (June 14, 2006): 161.

"Operational and Maintenance Costs for Wind Turbines." Wind Measurement International. Online at http://www.windmeasurementinternational.com/wind-turbines/om-turbines.php.

Park, Gene. "FAA Probes Whether Go! Pilots Fell Asleep," *Honolulu Star Bulletin* 13, no. 51 (February 20, 2008). Online at https://archives.starbulletin.com/2008/02/20/news/story08.html.

Parker, Mark. *Humble Pie: A Comedy of Maths Errors*. New York: Penguin, 2020.

Parker-Hope, Tara. "A Hollywood Family Takes on Medical Mistakes," *The New York Times*, March 17, 2008.

Perkins, Lucy. "Human Error Caused Virgin Galactic Crash, Investigators Say," National Public Radio, July 28, 2015.

Peters, Jeremy W. "MOTORING; Unraveling the Mystery of Ford's Fire-Prone Switches," *The New York Times*, August 27, 2006.

Petroski, Henry. *The Evolution of Useful Things*. New York: Alfred A. Knopf, 1995.

Petroski, Henry. *The Toothpick: Technology and Culture*. New York: Alfred A. Knopf, 2007.

Petroski, Henry. *To Engineer Is Human: The Role of Failure in Successful Design*. Vantage Books: New York, 1992.

Phillips, Don. "Putting the Pilot Back in Autopilot," *The Washington Post National Weekly Edition*, April 29–May 5, 1996.

"Pilot's Wrong Keystroke Led To Crash, Airline Says," *The New York Times*, August 24, 1996.

Queen v. M'Naghten, 10 Clark & F.200, 2 Eng. Rep. 718 (H.L. 1843).

Report of the Independent Panel of Guidant Corporation, March 20, 2006.

Report of the Presidential Commission on the Space Shuttle Challenger Accident. Washington, D.C.: United States Government Printing Office, 1986.

Riser, Robert and Don Gotterbarn. "Ethics Activities in Computer Science Courses." Online at http://csciwww.etsu.edu/gotterbarn/ArtTE2.htm.

Robison, Wade. *Decisions in Doubt: The Environment and Public Policy*. Hanover: University Press of New England, 1994.

Robison, Wade. "Design Problems and Ethics," in *Philosophy and Engineering: An Emerging Agenda*, Vol. 2 of the Series Philosophy of Engineering and Technology, edited by David E. Goldberg and Ibo van de Poel. Dordrecht: Springer, 2009.

Robison, Wade. "Ethical Presentations of Data: Tufte and the Morton-Thiokol Engineers," in *Philosophy and Engineering: Exploring Boundaries, Expanding Connections*, edited by Diane P. Michelfelder, Brian Newberry, and Qin Zhu. Dordrecht: Springer, 2016.

Robison, Wade. "In the Moral Zone," *Teaching Ethics* 8, no. 2 (Spring 2008): 57–78.

Robison, Wade, Roger Boisjoly, David Hoeker, and Stefan Young. "Representation and Misrepresentation: Tufte and the Morton-Thikol Engineers on the Challenger," *Science and Engineering Ethics* 8 (2002): 59–81.

Ryle, Gilbert. *The Concept of Mind*. London: Hutchinson, 1949.

Sanchez, Ray, Sara Ganim, and Linh Tran. "Flint Water Crisis: Who's been Charged, Who Hasn't," CNN, April 22, 2016. Online at https://www.cnn.com/2016/04/21/us/flint-crisis-who-was-charged/index.html.

Saul, Roger et al. "DESCRIPTION AND PERFORMANCE OF THE HYBRID III THREE YEAR OLD, SIX-YEAR- OLD AND SMALL FEMALE TEST DUMMIES IN RESTRAINT SYSTEM AND OUT-OF- POSITION AIR BAG ENVIRONMENTS," Transportation Research Center Inc. United States Paper Number 98S7-O-01.

Saul, Stephanie. "Ambien in the Driver's Seat," *The New York Times*, March 11 2008.

Saul, Stephanie. "Some Sleeping Pill Users Range Far Beyond Bed," *The New York Times*, March 8, 2008.

Saul, Stephanie. "Study Links Ambien Use to Unconscious Food Forays," *The New York Times*, March 14, 2008.

Schaper, David. "Pilots Criticize Boeing, Saying 737 Max 'Should Never Have Been Approved'," NPR, June 19, 2019.

Shatz, Itamar. "Brooks' Law: Adding Manpower to a Late Project Makes It Later." Online at https://effectiviology.com/brooks-law/.

Silberner, Joanne. "Study: Common Heart Drug Combo Raises Risk," *All Things Considered*, March 3, 2009.

Sisson, Paul. "Kaiser Hospital Fined for Removing Wrong Kidney," *U-T San Diego News*, December 20, 2012.

"Small Parts for Toys and Children's Products Business Guidance." Online at https://www.cpsc.gov/Business--Manufacturing/Business-Education/Business-Guidance/Small-Parts-for-Toys-and-Childrens-Products (accessed August 7, 2022).

Stewart, Will. "Russian Roulette Shock as Wedding Guest Shoots Himself in Party Trick Gone Wrong," *Daily Mail*, March 23, 2010.

Summary of the FAA's Review of the Boeing 737 MAX, November 18, 2020. Online at https://www.faa.gov/foia/electronic_reading_room/boeing_reading_room/media/737_RTS_Summary.pdf.

Tangel, Andrew and Andy Pasztor. "Behind Boeing's Decision to Omit Details on Safety System in Lion Air Crash from Manual," *Wall Street Journal*, December 5, 2018.

Thomas, Merlyn. "Two Air France Pilots Suspended after Cockpit Fight," *BBC News*, August 29, 2022. Online at https://www.bbc.com/news/world-europe-62712278.

Travis, Gregory. "How the Boeing 737 MAX Disaster Looks to a Software Engineer," *IEEE Spectrum*, April 18, 2019. Online at https://spectrum.ieee.org/how-the-boeing-737-max-disaster-looks-to-a-software-developer.

van de Poel, Ibo and David E. Goldberg, eds. *Philosophy and Engineering: An Emerging Agenda*, Vol. 2 of the Series Philosophy of Engineering and Technology, 205–14. Dordrecht: Springer, 2009.

Vaughan, Diane. *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. Chicago: University of Chicago Press, 1997.

Vlasic, Bill. "G.M. Enquiry Cites Years of Neglect Over Fatal Defect," *The New York Times*, June 5, 2014.

Volcker, John. "Who Knew? A Car Battery Is the World's Most Recycled Product," *Green Car Reports*, March 31, 2011.

Wald, Matthew L. "Expert Says Engineer Sent Text Messages Before Deadly Train Crash," *The New York Times*, January 22, 2010.

Wald, Matthew L. and Kenneth Chang. "Minneapolis Bridge Had Passed Inspection," *The New York Times*, August 3, 2007.

Wald, Matthew L. and Jess McKinley. "California Bans Texting by Operators of Trains," *The New York Times*, September 19, 2008.

Walton, Joseph W. *Essentials of Engineering Design*. St. Paul: West Publishing Co., 1991.

Williams, Timothy. "Citing Failures, Guidant Will Recall Thousands of Defibrillators," *The New York Times*, June 17, 2005.

Yaffa, Joshua. "The Road to Clarity," *The New York Times Magazine*, August 12, 2007.

Index

ABS brakes 141
accidents
  due to artifact (*see* error-provocative design)
  due to operator error (*see* operator error)
  intellectual ability 21–2, 24–5, 31
  off in some way 21–3
  relevance of circumstances 3, 21, 25–9, 57, 60, 174–5, 202
  training 22–5, 31, 60, 67–8, 74, 76, 84–5, 112, 159
Aciphex 99
airbags 54, 109–11
Airbus 64
Air France 180
air stream 65
Ambien 80–1
ambiguous information 115–16
anesthesiologist 179–80
angle of attack 65–6, 69–70, 72
argument from design 11, 201
argument from effects 11, 201
Aristotle 9, 36, 88, 95, 139
artifact
  embodying ethical considerations 1–2, 55–6, 88, 156, 175
  realizing design solutions 105, 146
aspirational 133
autopilot 57–9, 61–2, 86–90, 107, 202, 207

backup program 114–15
badly designed artifact 1, 29–30, 62, 174
balancing risk against benefit 163
bathroom door 48–9
batteries 120, 122–3
Baxter 167–72
benign by design 201–2, 208
big dig in Boston 125, 155
Big Ten university 158
biology 134
blackout 107
Blickensderfer 142
Boeing 55, 63–75, 177, 194–5, 197
Boeing 737 MAX 55, 63–8, 73–7, 194–5
Bogota 57–61, 80, 87–8
Boston 125, 155, 186
brain death 130
bridge 1, 15, 93, 125, 155, 159, 165, 185, 200
Brooks' law 196

Cadillac trunk 95–7, 104–5, 109, 119, 143, 190, 207
Cali 57–61, 69, 80, 87
California 27, 116, 186
care 11, 28, 59, 85, 129, 136–7, 149–51, 153–4, 169–70, 175, 179–80, 204
causal effects 11, 53, 145, 177, 187, 201
causal stream 11, 177, 187, 201
Center for Auto Safety 44
certification 135, 151
Challenger 147–8, 160–4, 196
changing hats 164
Chapanis and Lindenbaum 37–8
character 54, 82, 169–72, 174
Chinese tires 107
Chrysler 193–4
circumcision 152, 157
Citicorp Center 28

Clearview 128–33
clutch pedal 108–9
Colombia airliner crash 57–8, 76–7, 202
competence 54, 83–4, 86, 88, 90, 93–4, 133, 153, 174, 192, 202
complexity in design solutions 29
Congress 132, 192
consequences 13, 16, 81–2, 97, 125, 145–7, 150, 165
corporate character 171–2, 174
cost benefit analysis 193
counterproductive 23–4
creativity 5, 8, 50, 200, 210

decision-procedures 154, 165
defibrillator 100–5, 132
dementia 80
design history 40, 119, 142–4, 210
design problems 4–9, 11–12, 17–19, 27, 36, 40, 50, 51, 78, 87, 90–2, 94–5, 97, 105, 119–20, 122, 124, 136, 141–4, 159, 183–5, 193, 200, 202, 208
  a complex of decisions 51
  underdetermine solutions 9, 89, 105
design solutions. *See also* error-provocative design
  execution of 15
  faulty 43, 98, 124, 207
  foolproof 26, 42, 53, 94, 109
  involve ethical choices 2–5, 8, 11–12, 17, 50–2, 54–5, 76–7, 89, 92–3, 113, 124–6, 132–3, 142, 150, 177, 208
  involves value 5–6, 11–12, 14, 51–4, 89, 91, 133, 141, 201–2, 204–5
Ditlow, Clarence 44
DNA 134
Dodge Caravan 33
door handle 41, 49, 75, 87
door latches 41
double doors 113
downstream 11, 124–5, 177, 187, 190
due care 150, 170, 175, 204

effects, causal. *See* causal effects
Elwell, Daniel 64
engineering intellectual core 4, 7, 9, 17–18, 40, 50, 52, 89, 177, 200–2
ergonomics 35–7
error-provocative design 29–30, 31–5, 41, 43–4, 48–55, 89–94, 97, 108, 112, 124–5, 173, 206
Essentials of Engineering Design 199
ethical red flag 12–13, 35, 89, 138–40, 174, 177–8
ethical theory 13, 36, 208–9
Ethiopian Airlines 63–4, 67, 72
European Union 123, 188
evil genius of an engineer 90–2, 201–2, 207
Excedrin 83
external morality 191–8

F-22 fighter jets 76
failure rate 104, 125, 172–3, 189
faucets 113, 118
FDA 103
Federal Aviation Administration (FAA) 63–4, 67, 71, 74, 195
Federal Highway Administration 129
Firestone tires 107
Flint 192, 194
flipping a coin 165–6
flood walls 125, 155
Florida International 185
Ford 44, 107
Forkner, Mark 67
form of life 157–75
forms of knowledge
  knowing how 35, 85, 140, 144–9
  knowing that 25, 59, 70–1, 73, 81, 101–2, 140–4
free-riding 177

gallbladder 139
Galloping Gertie 159
Glasgow, Michael 192
GM 53, 120–1, 123, 193–6
GM's former entity 121, 123
Go! airlines 22, 25
gold standard 81
Guidant 100–4, 132, 170–2
guillotine 158, 160, 164, 204

habit 2, 14, 22, 34–5, 38–41, 46–8, 60, 73, 75, 96–7, 112, 119, 143–4, 210
harm
  setback to an interest 97, 123
  unnecessary 2, 4, 11–13, 17, 19, 49, 53–4, 77, 85, 90–4, 97, 100, 105, 118, 123–5, 133, 140, 144, 180, 187–8, 190–1, 194, 201–2, 209
  unprovoked 107–13
"head in the game". *See* accidents, off in some way
helmets 17, 144
heparin 167–8
Hep-Lock 167–8
Highway Gothic 129–31
Holly, Buddy 23
Hyatt-Regency 16, 125, 145–6, 187

ignition switch 53
"I'm so stupid!" 42, 44
Indianapolis 168, 172
inner morality 166–7, 172, 175
insanity 80
instructions 14, 22–3, 38, 46, 60–2, 115
intellectual core of engineering. *See* engineering intellectual core
intention
  not necessary for moral responsibility 55, 77, 82, 84, 86–8, 153, 201
  to produce harm 59, 63, 81, 89
  relevance 79
internal morality 172
irresistible impulse 80
Ivey, Edward 193

joystick 75

Kansas City 16, 125, 145
Kant 36, 208
Kao, Dr. Gary D. 83–4
keeping up 133
knowledge. *See* forms of knowledge

land mine 173–4, 182
Landsberg, Bruce 24
lawyer 15, 83–6, 93, 136–7, 139, 151–2, 157–8, 165, 167, 169–70, 174–5, 178
  falling asleep 82–3
  Japanese 204–5
left-hander 39
legacy problem 75, 96, 143, 195
life cycle 187–8, 191, 208
Lion Air 63–4, 67, 70, 72, 197
Lund, Bob 161–6

Macbeth, Bill 162
McDonnell Douglas 74, 197
Maneuvering Characteristics Augmentation System (MCAS) 66–74, 195
Mars Climate Orbiter 150, 175
Mason, Mr. 162–3, 166
Mazda RX-8 108–9, 113
Medical Humanities Fellow 139
Medtronic 104
Meeker, Don 130–1
Mercedes 122–3, 188
mercury switch 11–13, 93, 120–1, 207
Microsoft 75, 114
Mill 36
Minneapolis 22, 125, 155
mitigate harm 6
Montalbano, James 130–1

moral
accountability 91
failure 15–16, 53, 77, 89, 138, 192, 197, 203
judgments 18, 88–91, 139, 168–9
obligations 16, 138, 154–5, 171, 179, 192–4, 197–8, 204
principle: cause no unnecessary harm 4, 13, 113, 140, 201, 208–9
red flag 12–13, 35, 89, 138–40, 174, 177–8
relations 16–17, 19, 21, 137–8, 140, 151–5, 169, 191–2, 196–8, 203
morality v. engineering 18–19, 199–205
Morton-Thiokol 148, 161–2, 194–5
motivation 25, 31–2

narcolepsy 83
NASA 147, 161–2
National Highway Traffic Safety Administration (NHTSA) 44
"natural and obvious" 38–9, 41
New Orleans 125, 155
Nixon 116
no information 113
normative judgment 15, 35–6
norms 136, 175
nose dive 68, 73

operator error 21, 26–7, 29–30, 43–4, 46, 50, 58, 62–3, 91, 93, 125, 167–8, 206
O-rings 28, 147–8, 161, 164
Oukrop, Joshua 100

Petroski, Henry 6, 8, 145
physiology 142
pickup truck 193
Plavix 99
poet 8–9, 54–5
Presidential Commission 164
Prilosec 99
professionals 14, 16, 82–3, 85–6, 93, 126, 133, 135–8, 144, 152–3, 155, 160, 163, 165, 167, 170, 178, 193–4, 197–8, 204–5
projective history 146
psychology 40, 141

Quaid 167–70
qualitative 18, 199–205, 122–3
quantitative 4, 9, 15–16, 18, 50, 52, 159, 199–200, 210
QWERTY 40, 143

recycling 11, 53, 119, 188
redesign 62, 69, 77, 88, 141–2, 168, 172, 188, 198
relations. *See* moral, relations
remanufacturing 11, 53, 119–24
responsibility 45, 52, 60, 63, 87, 108, 121, 163, 173, 200, 203, 207
with intent 80–1
without intent 77, 79, 82–6
right-handed 42
risk management 167–8, 194
road stripes 126–8
Rochester NY 127, 131
Rogers, Chairman 147, 164
role morality 16–17, 19, 89, 135–40, 154–5, 157, 166, 169, 191–2, 208
Romeo 58
Rozo 57–9
rules of skill 13–16, 53, 84, 89, 136–7, 140, 203
runaway trim 71, 74

safety 35, 44, 52, 54, 74, 91, 98, 112, 117, 155, 193, 207–8
seeing reverberations 146–9
Selectric typewriter 142
servants 191–2

"severe head trauma" 117
shirking their duties 121, 178–9
shoulder harness 117
60 Minutes Report 167
sleepwalker 80
social position 135
space shuttle 28, 147, 160. *See also* Challenger
special knowledge 84, 89, 136, 140, 158, 203
special skills 84, 136, 158, 166, 203
stabilizers 66, 68, 74–5, 195
stalling 65–6, 72
stove top 33, 38, 46, 50
Subaru SVX 117–18
Sullenberger, Sully 72
sustainability 119–21, 184

Tacoma Narrows Bridge 159
team 4, 135, 150, 155, 177–90, 195–7, 204
terrorist 80
Texas 83, 139
thinking like a manager 163
thinking like an engineer 92, 157–60, 204, 210
throwaways 121–2
toaster 2–4, 13, 32, 35, 96, 121, 141, 191
toddler 4, 80, 82, 189
toothpick 4–11, 13, 50–1, 105, 200–1
The Toothpick: *Technology and Culture* 6
Toyota 44
tracking consequences 145, 150
train operator in California 27
Transportation Institute 130
Tulua 61

University of Tennessee Medical School 139
unnecessary harm. *See* harms, unnecessary
U.S. Appeals Court 83
U.S. Department of Transportation 132
useless information 113, 115

VA hospital 83–4
Virgin Galactic SpaceShipTwo 1
virtue theory 208
Viton 161
VW rabbit 117

Walton, Joseph 199
warning device 39, 62, 70
Wasatch Operations 162
water heater 90, 144
wind-tunnel 66
wind-up turn 66
wrong kidney 139
wrong leg 139, 152–3

X-ray machine 29, 98–100, 104–5, 107, 139

Y2K failure 76