CHARLES E. HARRIS, JR.

Explaining Disasters:
The Case for Preventive Ethics

NASA

Crewmembers of the January 8, 1986, Challenger mission, leaving to board the space shuttle. All seven lost their lives following the launch-phase explosion. From front to back: Francis R. Scobee, Judith A. Resnik, Ronald E. McNair, Michael J. Smith, Christa McAuliffe, Ellison Onizuka, and Gregory B. Jarvis.

In 1986, the space shuttle Challenger exploded during launch, taking the lives of six astronauts and one teacher, Christa McAuliffe. The disaster virtually stopped U.S. space exploration for two years. How should this disaster be explained?

Most disasters have multiple explanations. One type of explanation in the Challenger case focuses on the flaws in the design of the field joints in the boosters, or on other engineering failures. Another type locates the problem in improper management practices, either at the National Aeronautics and Space Administration (NASA) or with Morton Thiokol, the manufacturer of the boosters. Another type finds the fault in unethical conduct on the part of NASA or the private contractors. Still other types of explanation might attribute the disaster to an unanticipated convergence of events, or just plain bad luck. I shall confine myself, however, to the first

The author is with the Department of Philosophy, Texas A&M University, 510 Blocker Building, College Station, TX 77843-4237.

0278-0079/95/$4.00©1995IEEE

three types of explanation: bad engineering, bad management, and bad ethics.

Even though we may know that it is insufficient, there seems to be a natural tendency to focus on a single type of explanation. The result is that these three types of explanation compete with one another in the minds of many people. If an event can be explained in terms of engineering failures, for example, we may think there is no need to look for evidence of improper management or unethical conduct. If there is evidence of incompetent management, why look for engineering problems or ethical improprieties? One reason for this tendency may be that people tend to look for explanations most congruent with their own areas of expertise. Engineers usually look for the explanation of a disaster in bad engineering, most often in faulty design. Managers or management consultants tend to find the explanation in bad management. Ethicists are more likely to look for explanations in terms of ethically improper behavior.

Contrary to this approach, there are good reasons to believe that these three types of explanation are not mutually exclusive. The same disaster can be explained in terms of bad engineering, bad management and bad ethics. One consequence of taking this more pluralistic approach to explaining disasters is that the place of ethical considerations in explaining disasters is not neglected. An appreciation of the importance of ethical failures can, in turn, serve to underscore the importance of avoiding these failures in the future. I shall refer to this effort to isolate the ethical failures involved in engineering disasters and to use this knowledge to prevent such failures in the future as *preventive ethics*.

Before proceeding further, it is important to point out that there is a distinction between an engineering disaster and an ethically improper use of engineering. The Challenger explosion was an engineering disaster: it involved a technical malfunction that had catastrophic consequences. The employment of German engineers to design the gas valves used at Auschwitz was not an engineering disaster. The valves evidently worked all too well. The problem was that the end to which engineering design was directed was unethical. Few people would question the relevance of ethical categories in explaining the tragedy of Auschwitz: the ends toward which engineering design was directed were unethical. For most of us, however, the goals of engineering work in the Challenger project were not unethical. If ethical categories are relevant, they must be relevant in a different way. I am concerned with this second type of situation, not the first.

Three Types of Explanation

What do we mean by an explanation of a disaster? In explaining a disaster, at least two conditions must be met. First, there must be a failure or impropriety of some sort. Since we are limiting ourselves to three types of explanation, we shall be concerned with three types of failure: in engineering, in management, and in ethics. When we say there has been a failure of some sort, we mean that the rules, standards, or canons appropriate to that area have been violated. Thus, to say that a disaster exhibited improper engineering means that engineering standards were violated. To say that a disaster exhibited improper management means that the canons of good management practice were violated. Similarly, to say that a disaster exhibited unethical conduct means that the canons of proper ethical conduct were violated.

A second condition is that the impropriety must have been a contributing cause of the disaster. While there may be times when a single cause is sufficient to explain a disaster, it is more common to find that there are several contributing causes. I shall offer the following as a working account (not a formal definition) of a contributing cause: Event A is a contributing cause of Event B, when Event A is prior to Event B and when the existence of Event A makes Event B more likely to occur. Using these two conditions as tests, we can make a case that the Challenger disaster can be explained in all three ways: it was bad engineering, bad management and bad ethics.

The case for explanation in terms of bad engineering is based on the design flaws in the seal between the sections of the boosters. One of the canons of good engineering design is that static and dynamic situations must be carefully distinguished, and the design must fit the situation. Yet in the case of the Challenger, this canon was violated. The O-ring seal between the sections of the boosters was designed for a static situation, but the flexing to which the seal was subjected in flight meant that it should have been designed for a dynamic situation. This design flaw, along with the unusually cold weather that caused the O-rings to lose some of their resiliency, was perhaps the most obvious engineering explanation of the disaster.[1]

Furthermore, the design flaw was a contributing cause to the disaster. The design flaw made the disaster much more probable. Indeed, apart from this design flaw, the disaster might never

[1] I have used two written sources for my account of the Challenger disaster. One source is the commission chaired by William P. Rogers in 1986 [1]. I shall refer to this as the Rogers Commission Report. The other is Roger Boisjoly's, "The Challenger disaster: Moral responsibility and the working engineer" [2].

have occurred. So both of the conditions of explanation in terms of an engineering failure are fulfilled. There were violations of engineering principles, and these violations made the disaster much more likely to happen.

There is a natural tendency to focus on a single type of explanation.

There is also a case for an explanation of the Challenger disaster in terms of bad management. To say that an event exhibits bad management is to say that it violates the standards of good management.[2] One of the standards of good management is that managers should establish and maintain effective communication with their employees. The reason for this is that good communication not only enhances employee morale, but also furnishes managers with information that is essential in making sound management decisions. In order to enhance communication, managers must do at least two things. First, they must create an atmosphere in which employees can bring up problems without fear of reprisal. Second, they must respond positively to employees when they utilize this freedom to bring up problems. This does not mean that managers must always follow employees' advice, but they must consider and evaluate it carefully.

These requirements of good management practice, which are especially important with regard to professional employees, were evidently violated by Morton Thiokol managers. Roger Boisjoly reports that he alerted Thiokol managers to the problems with the O-ring seal a year or more before the Challenger disaster. He even asked for funding to look for solutions. Not only was his request ignored, but there was evidently an atmosphere of intimidation that inhibited engineers from communicating their concerns freely. On the night before the disastrous launch, Boisjoly and other engineers made their case for a no-launch recommendation to NASA, primarily on the basis of anticipated difficulties with the O-ring seals at the low launch temperatures. After first being accepted by Thiokol managers, this recommendation was later reversed, partially at least as a result of protests from NASA. According to Boisjoly's account, when he objected to the reversal of the original recommendation, his manager (Gerald Mason) looked at him in a way that indicated he was about to be fired.[3]

Improper management was also a contributing cause of the disaster. If Thiokol managers had been more responsive to Boisjoly's early warnings, they might have ordered research aimed at improving the O-ring seal, and an improved seal might well have averted the disaster. If Thiokol and NASA managers had listened to the engineers on the night before the launch, they might have recommended against the launch and the launch might not have taken place. So bad management was also an explanation of the disaster, in that management principles were violated, and the violations made it more likely that a disaster would occur.

Finally, a case can be made that ethically improper conduct was part of the explanation of the disaster. To say that something is unethical is to say that it violates ethical standards. One such standard is the Golden Rule: "Do unto others as you would have them do unto you." One wonders if Thiokol or NASA managers would have been willing to fly in the Challenger themselves, knowing what they did about the problems with the O-rings. I am inclined to say that they would not, and that their action violated the Golden Rule.

Perhaps even more telling is the violation of the standard of free and informed consent. People should be informed about unusual dangers to which they might be subjected and given the chance to consent or not consent to the dangers. According to the Rogers Commission, this canon was not fully honored with respect to the problem created by ice formation on the Challenger, due to the sub-freezing temperatures the night before launch. Although they had been consulted about the ice problem, the crew was not fully apprised of its seriousness [1, p. 118]. There is also no record of the crew's having been adequately informed of the O-ring problem, even though it was known to be potentially life-threatening. These deficiencies can only be considered serious violations of the principle of informed consent. Even though the astronauts knew that they were engaged in a high-risk mission, the principle of informed consent was not thereby rendered irrelevant. The astronauts should have been informed of the unusual problems.

In addition to the violation of widely-accepted ethical precepts, the events preceding the Challenger disaster exhibit other types of ethical deficiencies. The Rogers Commission concluded that Thiokol management reversed its original decision "contrary to the views of its

[2]For further discussion of the engineer/manager relationship, see [3].

[3]Reported in [4].

engineers in order to accommodate a major customer" [1, p. 104]. What explains this reversal? NASA managers expressed extreme displeasure with the original Thiokol decision not to launch, probably due to pressures on them for a quick success.[4] The testimony of Robert Lund, the vice president of engineering at Morton Thiokol, centers around a shift in the burden of proof. Whereas NASA originally adopted a policy that a launch recommendation bore the burden of proof, it had shifted to the position that a no-launch recommendation bore the burden of proof [1, p. 93]. After first agreeing with his engineers, Lund changed is mind, perhaps in response to pressure from Mason. The testimony of Jerry Mason, a senior vice president at Morton Thiokol, centers around the claim that the engineering evidence was inconclusive and that a management decision had to be made [1, p. 773]. There is evidence, then, that both NASA and Thiokol managers may have exhibited ethical deficiencies. One thinks of weakness of will (lack of courage to do what one knows is right), self-deception, and self-interest as likely candidates for these deficiencies.

A good case can also be made that ethical failures were a contributing cause to the disaster. If the managers at NASA and Thiokol had put themselves in the place of the astronauts and had never been affected by weakness of will, self-deception, or self-interest, they would almost certainly have taken the O-ring problems more seriously. The managers would probably have paid attention to Boisjoly's early warnings and ordered further testing, which might have led to the correction of the problem. If managers had held consistently to the canon of free and informed consent, they would have fully informed the astronauts of the O-ring problem. We do not know, of course, whether the astronauts would have decided to fly if they had been informed about the O-ring problem. There is, however, a significant chance that they would have decided not to fly, especially if the information about the O-ring problem had been added to the information about the danger due to ice. Even if they had decided to fly, the managers and engineers might have been more likely to try to correct the O-ring problem, knowing that they must inform the astronauts about it.

One wonders if Thoikol or NASA managers would have been willing to fly in the Challenger themselves, given their knowledge of the O-ring problems.

Thus, if managers and engineers had avoided unethical conduct, they would have been more likely to have made different decisions. This means that ethical failings were present and could be considered contributing causes of the disaster.

Primacy of the Engineering Explanation

If this analysis is correct, there is nothing wrong with saying that bad engineering, bad management and faulty ethics all play a part in explaining the Challenger disaster. Principles of sound engineering, sound management and sound ethics were violated, and these violations could all be considered contributing causes to the disaster. These three types of explanation are not mutually exclusive. One cannot show that one type of explanation is inapplicable merely by showing that another type of explanation is applicable. One cannot show, for example, that an explanation in terms of ethical failings is irrelevant by showing that an explanation in terms of engineering ineptitude is relevant.

But isn't the engineering explanation more fundamental than the others? Even if all three types of explanation are relevant, doesn't the engineering explanation occupy pride of place? The simple answer to this question is, "Yes." The engineering deficiencies seem to be the most crucial, in the sense that the disaster almost certainly would not have occurred if there had been no problem with the O-rings. This cannot be said of the management and ethical failures. Even if management practices and ethical conduct had been exemplary, the disaster might still have occurred. Suppose Thiokol managers had listened to Boisjoly's early warnings about the O-ring deficiencies and ordered further testing and research to resolve the problems. A bad design might still have resulted. Even if NASA and Thiokol managers had listened with an open mind and in a non-intimidating way to the engineers on the night before the launch, they might still have concluded in good faith that the engineer-

[4] According to Roger Boisjoly, George Hardy of NASA said he was appalled by Thiokol's no-launch recommendation. See [2, p. 8].

ing evidence was not compelling. While the managers might have made a mistake, they might not have violated principles of sound management.

The situation is similar with regard to the ethical improprieties. Suppose Thiokol managers had attempted to follow the Golden Rule, so that they ordered further research and development on the O-rings. This research and development could still have issued in a bad design. They might even in good faith have been willing to fly themselves. Furthermore, if the astronauts had been fully informed about the problems with ice and the O-rings, so that the requirement of free and informed consent was met, they might have decided to fly anyway. And if engineers and managers had resisted unethical influences on the night before the launch, they still might have made a decision to launch.

Of course following sound engineering principles does not guarantee that there will be no design mistakes, but it is still true that the disaster probably would not have occurred if the design mistakes had been corrected. By contrast, the disaster might still have occurred, even if the management and ethical failures *had* been corrected. In this sense, then, the engineering failure can be considered the most fundamental or at least the most direct explanation of the Challenger disaster.

Preventive Ethics

It does not follow, however, that management and ethical considerations are irrelevant in explaining the disaster. There is good reason to believe that there were management and ethical failures, and that these were contributing causes to the disaster. We cannot say for certain that eliminating these failures would have kept the Challenger disaster from happening, but it would have made the disaster less likely. This is because eliminating the management and ethical failures would have made the engineering failures themselves less likely to have happened. Of course there are other reasons besides preventing disasters for engaging in sound ethical and management practices, but I am concerned here only with this reason.

Thus, understanding why a disaster happened puts us in a better position to *prevent* similar disasters in the future. This is one of the reasons engineers want to look for the engineering explanation of a disaster. Engineers, like the rest of us, learn from experience. If they can isolate the engineering factors that explain a disaster, they can do something to prevent similar mistakes in the future. Perhaps we could call this *preventive engineering*.[5]

The same thing could be said about management failures. If managers at NASA, Morton Thiokol, and perhaps other private contractors had established a more open and non-intimidating atmosphere for their engineers and had been more adept at listening to the engineers' concerns, remedial measures might have been taken regarding the O-rings and the disaster might not have happened. Perhaps we can call this *preventive management*.

People should be informed about unusual dangers to which they might be subjected, and given the chance to consent or not consent to the dangers.

By similar reasoning we can say that discovering and attempting to eliminate ethical failures can also aid in preventing similar disasters in the future. As we have seen, if managers had been more attentive to ethical considerations such as the Golden Rule and the principle of informed consent and had not succumbed to self-interest or excessive external pressures, they might have taken stronger measures to correct the O-ring problems. Similarly, greater ethical concern and strength of will might have led more engineers to insist that either the O-ring problem be remedied or the Challenger should not fly. Exposing these problems and attempting to eliminate them can make an important contribution to preventing similar disasters in the future. I have already referred to this as part of preventive ethics.

The idea of preventive ethics is not wholly new. Some large health-care organizations employ medical ethicists on the corporate level in order to aid in the formulation of ethically acceptable policies. Management in these organizations apparently believes that operating by ethically acceptable policies may prevent legal and public-image problems and serve as a defense if such problems arise. Promoting codes of ethics and installing ethics officers and procedures for promoting ethical awareness may be a

[5]Steven B. Young and Willem H. Vanderburg develop the concept of "preventive engineering" in [5].

part of this same philosophy.

So far I have focused exclusively on the Challenger case in order to illustrate the ethical dimension of explaining disasters and the concept of preventive ethics. But many other famous cases in engineering ethics also exemplify ethical failures and suggest that the elimination of those failures might have prevented the disasters, or at least made them less probable. Engineers and managers were aware, for example, of the problems with the cargo hatch door of the McDonnell Douglas DC-10, but only one engineer appears to have made any concerted effort to remedy the problem. If managers and engineers had resisted unethical influences or imaginatively placed themselves in the position of passengers in the DC-10, would they have acted differently? If they had, the crash near Paris, France, which killed all 346 passengers, might have been avoided. Ford engineers and managers were aware of the susceptibility of the Ford Pinto to explosion from even low-impact rear-end collisions. Would they have been more inclined to remedy the design defect if they had taken seriously the possibility that they or a family member might have driven the car, or if they had considered informing the public of the danger from rear-end collisions? Similar arguments might be made about the Chevrolet Corvair, the Union Carbide disaster in Bhopal, India, and many other cases not so well known.

A good case can be made that ethical failures were a contributing cause to the disaster.

There is no way of knowing whether greater ethical sensitivity and the absence of impediments to ethically responsible action would have prevented these particular disasters, but it seems almost certain that the presence of these factors can prevent *some* unfortunate and tragic engineering disasters. This is enough to make preventive ethics worthwhile.

References

[1] William P. Rogers, "Report to the President by the Presidential Commission on the Space Shuttle Challenger Accident," Washington, DC, June 6, 1986.

[2] Roger Boisjoly, "The Challenger disaster: Moral responsibility and the working engineer," in *Ethical Issues in Engineering*, Deborah C. Johnson, Ed. Englewood Cliffs, NJ: Prentice Hall, 1991, pp. 6-14.

[3] Charles E. Harris, Jr., Michael S. Pritchard, and Michael J. Rabins, *Engineering Ethics*. Belmont, CA: Wadsworth, 1995, pp. 273-277.

[4] Roger Boisjoly, Massachusetts Institute of Technology, Cambridge, MA, Jan. 7, 1987, videotape record of remarks to audience.

[5] Steven B. Young and Willem H. Vanderburg, "A materials life cycle framework for preventive engineering," *IEEE Technol. & Soc. Mag.*, vol. 11, pp. 26-31, Fall 1992. T&S