cantilevered balcony had been attached to a ledger board that was nailed to the structure by the framing subcontractor instead of bolted as specified by the architect. The ledger board separated from the structure under dead load plus a very light live load (the two visitors). The architect designed the structure, including the balconies, and oversaw the construction but did not inspect the finished balcony closely enough to detect the deviation from his plans and specifications.

The architect's contract required that he sign off on the contractor's pay applications as assurance that "the quality of workmanship and materials used conforms with the contract documents." But the contract also said that, "The architect shall not be required to make exhaustive or continuous on-site inspections to check the quality or quantity of the work."

The legal argument centered on whether the architect should have done more to inspect the structure, with the plaintiffs arguing that he was contracted to "observe construction" and "endeavor to guard the owner against defects and deficiencies" in addition to providing his design services. The defendant architect argued that his inspection could not be detailed for that fee and that he had properly discharged his responsibility for construction observation.

A general counsel for the Texas Society of Architects wrote, "unless the project's owner retains the architect to provide more extensive services, the architect's on-site duties are limited and do not include exhaustive or continuous on-site inspections to check the quality of the construction work performed by the contractor. … The architect cannot be expected to guarantee the quality of the contractor's work, however, unless the architect has agreed to provide the additional services that would be necessary to enable the architect to provide that assurance."

In our assessment, the construction error that occurred was egregious, and because of the criticality of the cantilevered balcony components, this construction error should not have gone undetected by any reasonable inspection by a professional architect or engineer with ANY responsibility for oversight of structural construction.

The original design has not been questioned, but it called for joist hangers that were not used by the framing subcontractor to secure the joists to the ledger board and bolts to secure the ledger board to the structure. Instead, nails were used. But even the original design was likely inadequate. Joist hangers are not designed to carry a moment as in this cantilevered application. Had the joist hangers been used and had the ledger board been more securely fastened to the structure with the bolts originally specified, the failure would likely have occurred between joist and ledger, rather than between ledger and structure, and perhaps with more than two people on the structure. A more reasonable design would involve joists that penetrate into the structure and are secured to parallel floor/ceiling joists that allow them to develop the required moment capacity at the wall, and it is not clear whether this design was an alternative that was also rejected by the general or framing contractor.

The lesson here is that the professional engineer (or architect) has a moral responsibility, even where there is no clear legal responsibility, to prevent problems like this from developing in projects in which he or she has a significant role. In engineered projects, there must be a contractual arrangement allowing appropriate construction inspection engineering efforts, and the most critical design details such as the one in question here should have the highest priority for the construction inspector.

CASE 33

Computer Programs and Moral Responsibility—the Therac-25 Case

Medical linear accelerators (linacs) create high-energy beams that can destroy tumors with minimal damage to surrounding healthy tissue. For relatively shallow tissue, accelerated electrons are used; for deeper tissue, the electron beam is converted into X-ray photons.[110] In the mid-1970s, Atomic Energy of Canada Limited (AECL) developed a radical new "double-pass" accelerator that needs much less space to develop the required energy levels because it folds the long physical mechanism required to accelerate

electrons. Using this double-pass mechanism, AECL designed the Therac-25, which also had the economic advantage over the Therac-20 and other predecessor machines of combining electron and photon acceleration in one machine. The Therac-25 was also different in another way: The software had more responsibility for insuring patient safety than in previous machines. The earlier Therac-20, for example, had independent protective circuits for monitoring electron-beam scanning, plus mechanical interlocks for ensuring safe operation.

Eleven Therac-25 machines were installed in the United States and Canada between 1985 and 1987, and six accidents involving massive overdoses occurred. The first overdose occurred at the Kennestone Regional Oncology Center in 1985. When the machine turned on, the patient felt a "tremendous force of heat … this red-hot sensation." When the technician came in, the patient said, "You burned me." The technician said this was not possible. Later, the patient's shoulder (the area of treatment) "froze," and she experienced spasms. The doctors could provide no satisfactory explanation for an obvious radiation burn. Eventually, the patient's breast had to be removed because of radiation burns, and she was in constant pain. The manufacturer and operators of the machine refused to believe that it could have been caused by the Therac-25. A lawsuit was settled out of court, and other Therac-25 users were not informed that anything untoward had happened.

The second accident occurred at the Ontario Cancer Foundation in Hamilton, Ontario. When the machine shut down on the command to deliver the dose, the operator was not concerned, having become accustomed to frequent malfunctions with no harmful consequences. After the treatment was finally administered, however, the patient described a burning sensation in the treatment area. The patient died four months later of an extremely virulent cancer, but an autopsy revealed that a total hip replacement would have been necessary because of the radiation overexposure. AECL could not reproduce the malfunction that occurred at the Hamilton facility, but it altered the software, claiming an improvement over the old system by five orders of magnitude—a claim that was probably exaggerated.

The third accident occurred at Yakima Valley Memorial Hospital in 1985 in Yakima, Washington. After treatment, the patient developed an excessive reddening of the skin, which the hospital staff eventually attributed to "cause unknown." The patient was in constant pain, which was relieved by surgery, and did not die from the radiation. The fact that three similar incidents had occurred with this equipment did not trigger investigation by the manufacturer or government agencies.

The fourth accident occurred in 1986 at the East Texas Cancer Center (ETCC) in Tyler, Texas. Upon attempting to administer the dose, the machine shut down with a "Malfunction 54" error message. The patient said he felt like he had received an electric shock or that someone had poured hot coffee on his back. He began to get up from the treatment table to ask for help, but at that moment the operator hit the "P" key to proceed with treatment. The patient said he felt like his arm was being shocked by electricity and that his hand was leaving his body. He went to the treatment room door and pounded on it. The operator was shocked and immediately opened the door for the patient, who appeared shaken and upset. Unknown to anyone at the time, the patient had received a massive overdose. He died from complications of the overdose five months after the accident.

One local AECL engineer and one from the home office in Canada came to investigate. They were unable to reproduce Malfunction 54. One local AECL engineer explained that it was not possible to overdose a patient. AECL engineers also said that AECL knew of no accidents involving radiation overexposure by Therac-25, even though AECL must surely have been aware of the Hamilton and Yakima incidents. The AECL engineers suggested that an electrical problem might be to blame, but further investigation by ETCC ruled out this possibility.

The fifth incident also occurred at ETCC, this time on April 11, 1986. Upon being given the command to administer the dose, the Therac-25 again registered the Malfunction 54 message, made some loud noises, and shut down. The patient said he heard a sizzling sound, felt "fire" on the side of his face and saw a flash of light. Agitated, he asked, "What happened to me, what happened to me?" He died from the overdose on May 1, 1986.

If not for the efforts of Fritz Hager, the Tyler hospital physicist, the understanding of the software

problems might have come much later. Mr. Hager was eventually able to elicit the Malfunction 54 message, determining that the speed of the data entry was the key factor in producing the error condition. After explaining this to AECL, the firm was finally able to produce the condition on its own. This seemed to suggest that the particular coding error was not as important as the fact that there was an unsafe design of the software and the lack of any backup hardware safety mechanisms.

The sixth accident also occurred at Yakima Valley Hospital in January 1987. The patient reported "feeling a burning sensation" in the chest and died in April from complications related to the overdose. After the second Yakima accident, the U.S. Food and Drug Administration concluded that the software alone could not be relied upon to ensure the safe operation of the machine. The initiatives for identifying the problems with the Therac-25 came from users, not the manufacturer, which was slow to respond. The medical staff on the user side were also slow to recognize the problem.

Blame-Responsibility: Corporate Responsibility

This tragic story illustrates irresponsible actions on both the corporate and individual levels. Yet, the investigators of the accidents did not wish "to criticize the manufacturer of the equipment or anyone else."[111] Philosopher Helen Nissenbaum believes that this reluctance to assign blame, either to organizations or groups, is not unusual. Rather, "accountability is systematically undetermined in our computerized society—which, given the value of accountability to society, is a disturbing loss."[112] She believes further that "if not addressed, this erosion of accountability will mean that computers are 'out of control' in an important and disturbing way."[113] Even if Nissenbaum's claims are extreme, it is probably true that the increased usage of computers have raised in an especially urgent way the problem of responsibility or accountability, and that the issue must be addressed.

Let us first consider the issue of blame-responsibility, on the corporate level. What is the blame-responsibility (if any) that can be assigned to such corporate entities as AECL, Yakima Valley Memorial Hospital, and the East Texas Cancer Center?

We saw in Chapter 4 that corporations can be causes of harm by way of specific corporate policies (or the absence of corporate policies), corporate decisions, management decisions, and a corporate culture. We noted that there are some relatively strong arguments that organizations such as corporations can be morally responsible agents like people. Whether or not they can be morally responsible agents, they can still be

1. criticized for harms,
2. asked to make reparations for harms, and
3. assessed as in need of reform.

Let us look at specific issues in the Therac-25 case that might lead to blame-responsibility on the corporate level.

1. One design flaw in the Therac-25 was the absence of hardware safety backups. Earlier versions of the machine had such backups, and if they had been present in the later version, some (or all) of the accidents might not have occurred. Although this design flaw may have been simply the fault of the individual engineers, it may have resulted from the fact that some of the engineers at AECL apparently did not have proper training in systems engineering. This, in turn, may have been the result of a failure of AECL management and company policy with respect to the training of AECL engineers.
2. AECL evidently did not have adequate testing and an adequate quality assurance program. This deficiency may also have been a major factor in producing the accidents, and these failures should probably be attributed to management and perhaps to corporate policies and a corporate culture that did not sufficiently value both testing and quality assurance.
3. AECL made exaggerated claims for the safety of the Therac-25. Technicians were led to believe that the machines could not possibly administer an overdose, and this was probably one reason the technicians were also insufficiently responsive to patient complaints. The exaggerated claims for safety may have also been partially responsible for

the fact that physicians were slow to recognize the radiation burns. These problems could well be attributable to a corporate culture that was excessively concerned for sales.

4. AECL was slow in responding to reports of accidents and in informing other users of the malfunctions of the Therac-25. Bad management decisions and, again, a corporate culture that was overly concerned with sales and insufficiently concerned with safety were probably at least partly to blame.
5. The monitoring equipment in at least one of the medical facilities (the East Texas Cancer Center) was not properly functioning, and this may have played a part in the injuries to patients. There may have been a deficiency with management and perhaps with a corporate culture that was not sufficiently oriented toward the highest standards of safety.

These examples strongly suggest that at least AECL deserves moral criticism for the injuries and deaths to patients. AECL could be asked to make reparations for harms (and may be legally liable for such reparations) and is in need of internal reform. The East Texas Cancer Center may also be open to criticisms, although on a far more limited basis.

Blame-Responsibility: Individual Responsibility

The Therac-25 accidents were not caused by any single individual. In Chapter 3, however, we saw that in situations involving collective action and inaction, there are principles that give direction for assigning blame-responsibility. The principle of responsibility for action in groups states: In a situation in which harm has been produced by collective action, the degree of responsibility of each member of the group depends on the extent to which the member caused the action by some action reasonably avoidable on his part. The principles of responsibility for inaction in a group states: In a situation in which harm has been produced by collective inaction, the degree or responsibility of each member of the group depends on the extent to which the member could reasonably be expected to have tried to prevent the action.

We have also seen that blame-responsibility can be the result of malicious intent, recklessness, or negligence. The following enumeration is probably best understood as a list of various types of negligence and therefore as types of inaction for which those who are involved bear some degree of blame-responsibility, depending on the causal importance of their inaction in the harms.

We also saw that negligence involves the following four factors:

1. the existence of a standard of conduct,
2. a failure of conformity to these standards,
3. a reasonably close causal connection between the conduct and resulting harm, and
4. a resulting actual loss or damage to the interests of another person.

One of the problems with attributing negligence in computer-related incidents is that the standards of conduct (or "due care") are sometimes insufficiently developed and made public. Nevertheless, we believe that there are implicit standards that warrant the attribution of blame-responsibility with respect to the following groups of individuals.

1. As we have noted, one of the design flaws in the Therac-25 was the absence of the hardware safety backups that the earlier machines had. If the backups had been present, some (or all) of the accidents might not have occurred. Although this design flaw may have been partly attributable to management and company policies that did not place enough emphasis on systems engineering, it may also be attributable to professional negligence that was the fault of the individual engineers involved. The accidents might not have occurred if the hardware backups had been present. Insofar as the professional negligence is the fault of the individual engineers, they bear considerable responsibility for the accidents. The negligence here was the failure of engineers to investigate more fully the dangers associated with a system with no hardware backups and the resulting failure to incorporate these backups into their design.
2. The manufacturing personnel who built the faulty microswitch that controlled the position of the

turntable on which the patients were placed were important causal agents in some of the accidents, especially the one at the Ontario Cancer Foundation. The standard account gives little information about the reasons for this fault, but perhaps we can best attribute it to negligence involved in the building of the faulty equipment. If the patients had been properly positioned, they might not have suffered radiation burns, but we shall see that there were other causal factors present. So we can say that the manufacturing personnel should be held partially responsible.

3. The programmers were also partially responsible for harm to patients. There were errors in programming and obscure error messages. There appeared to be considerable negligence on the part of the programmers, and their errors apparently were directly causally responsible in part for the harms. It should be said on behalf of the programmers, however, that there are usually "bugs" in programs, and the programmers may not have had sufficient training to be aware of the dangers of leaving all of the responsibility for safety to the computer programs.
4. Evidently, the user manuals were inadequately written. There was no explanation, for example, of the Malfunction 54 error message. The absence of proper instructions was clearly a factor in the accidents. Had the operators known how to respond to error messages, they might have been able to avoid some of the accidents. Here again, there appeared to be negligence that was causally related to the accidents. Manual writers can only write what they are given, however, and we do not know what information they were given. So we cannot, without further information, know just how much blame-responsibility the manual writers should bear.
5. In some of the accidents, technicians may not have been sufficiently aware of the possibility of radiation burns, and they sometimes seemed shockingly insensitive to patient distress. This again is a type of negligence that may have played some part in the harm done to patients. In defense of the technicians, however, two considerations are relevant. First, both of these faults can probably be attributed in part to the AECL claims that radiation burns were not possible and to the limited knowledge that was at the disposal of the technicians. Second, technician negligence probably was a minor factor in the actual harm done. Therefore, the causal relationship of technician negligence to actual harm done was probably minimal.
6. In several cases, physicians seemed slow to recognize that overexposure had occurred. This is also a type of professional negligence. Again, however, two considerations in defense of the physicians are relevant. First, whether lives would have been saved if treatments for radiation burns have been more prompt is not clear. Second, one reason for the physicians' tardiness might have been the excessive claims of AECL that overexposure was not possible. Still, physicians in radiation-treatment facilities should be alert to the possibility of radiation burns.

As this analysis shows, the major blame-responsibility for the injuries and deaths from the Therac-25 lies with AECL on both the individual and corporate levels. There was probably negligence on the part of both management and individuals at AECL. Furthermore, there was also probably a corporate culture that encouraged irresponsible action. Finally, the negligence had a strong causal relationship to the injuries and deaths.

It would be interesting to speculate on the impediments to responsibility that explain the problems at AECL. AECL was apparently plagued by a corporate culture in which managers focused excessively on profit and sales to the exclusion of other considerations such as safety. This may have been a type of microscopic vision. Managers may have also engaged in self-deception, convincing themselves that the reports of injuries and malfunctions of the Therac-25 were not significant, would not be repeated, and were not the result of any fundamental faults of the machine itself.

Individual negligence on the part of engineers and programmers may have been partly the result of self-interest because any insistence on greater attention to safety considerations might have resulted in disfavor by managers. We have already pointed out that engineers may have been affected by ignorance because of their insufficient training in systems engineering.

Finally, group-think may have played a part in the behavior of engineers and programmers. Perhaps, a "can-do" mentality and an emphasis on avoiding delays in getting the product on the market inhibited individuals from making objections based on safety considerations.

Maintain Accountability in a Computerized Society

Helen Nissenbaum has made several suggestions about ways to maintain accountability in a computerized society, two of which seem especially valuable.[114] One suggestion is that standards of care should be promoted in computer science and computer engineering. Guidelines for producing safer and more reliable computer systems should be widely promulgated and adhered to by computer professionals. Not only should such standards result in greater safety and reliability but also the existence of such standards should make it easier to identify those who should be held responsible and liable for failures. We have already mentioned one such standard, namely, that computer programs should not bear the sole responsibility for safety.

A second suggestion is that strict liability should be imposed for defective customer-oriented software and for software that has a considerable impact on society. Strict liability implies the manufacturer is responsible for any harm caused by a defective product, regardless of whether the fault can be assigned to the producer of the product. Strict liability would help to ensure that victims are properly compensated, and it would send a strong message to the producers of software that they should be vitally concerned with the safety of the public. As an example of the current situation in which the producers of software assume no responsibility for the safety of their product, according to Nissenbaum, Apple Computer makes the following statement:

> Apple makes no warranty or representation, either expressed or implied, with respect to software, its quality, performance, merchantability, or fitness for a particular purpose. As a result, this software is sold "as is," and you, the purchaser, are assuming the entire risk as to its quality and performance.

These evasions are problematic from an ethical standpoint. As the Therac-25 case illustrates, people can be harmed and even killed by computer mishaps.

Some people have objected to Nissenbaum's suggestions. One objection is that, although software engineering has standards for software-development processes, there are few standards for software products. Furthermore, setting product standards has turned out to be difficult. So Nissenbaum's first suggestion may be hard to implement. Nissenbaum's second suggestion is also somewhat impractical, according to some critics. Software may not be sufficiently mature to qualify for strict liability, they argue. Nevertheless, some computer scientists are sympathetic with Nissenbaum's suggestions, believing that they point the way to necessary reforms.

CASE 34

Roundabouts[115]

Roadway intersections present several engineering challenges. Consider, for instance, that in 2009, 20.8 percent of roadway fatalities in the United States occurred at intersections, or were in some way intersection related.[116] Signaled intersections are problematic for drivers, since a good deal of attention and thought may be required to traverse a busy intersection. Drivers must decide quickly when and how to proceed, especially when facing a changing light, or when navigating multiple traffic lanes. Consider as well that stop-and-go traffic, such as traffic at a busy intersection, increases automobile emissions significantly and results in traffic congestion. Both of these issues raise significant problems for engineers, since safety and efficiency are primary engineering concerns.

Roundabouts provide an elegant solution to many of these problems. Roundabouts are circular intersections designed to allow vehicles to traverse in any direction, often without ever coming to a complete