



This copy is for your personal, non-commercial use only. This article may not be reprinted for commercial purposes without the written permission of Mechanical Engineering magazine and ASME. © 2008 Mechanical Engineering magazine

Safety First?

FOCUS ON: DESIGN

There is no excuse for manufacturers that let defective products reach the market.

By Peter R. Lewis

BAD HEADLINES DUE TO DEFECTIVE PRODUCTS CAN ALMOST GUT A COMPANY. Earlier this year, when the accelerator problems in many Toyota cars become widely known, the company's reputation—and sales—took a nosedive. And no company associated with the disaster aboard the *Deepwater Horizon* has escaped public rebuke.

Out of the headlines, there is a much larger number of product failures which are not always given the publicity they deserve, but which may be just as damaging. Poor product design lies at the heart of these problems, usually coupled with a failure to test products under realistic conditions.

Sometimes these mistakes are made out of misguided sense of frugality. For instance, it has been estimated that executives managing the drilling aboard the ill-fated *Deepwater Horizon* had hoped to save about \$5 million by speeding through some of the steps to seal the well. The resulting accident has accounted for untold billions of dollars in damage. Even in less high profile instances, the cost of solving the problems arising from faulty product design usually far exceeds the cost of correcting the design problems in the first place.

In my experience as a forensic engineer, I have seen countless examples of poor product and industrial design that have led to damage, injury, sometimes death—and almost in every case, large expenses for the company in question. It is a subject that gets far too little attention in the engineering community.

SMALL FAILURES, MULTIPLIED BY THE MILLION, CAN MAKE FOR AN ENORMOUS FINANCIAL HIT. For instance, one of the largest class-action lawsuits ever filed in the U.S. involved the failure of domestic plastic piping installed for hot water heating systems in the late 1980s.

I became involved in the initial lawsuit as an expert reporting on the failure of a plastic joint, which caused a flood into rooms below and destroyed computers and other equipment. The plaintiffs argued that the plumber had not tightened the joint correctly. In fact, the fault was not in the plumber, but in the joint, which had not been made correctly. A report I found from Texas courts, showed that U.S. Brass, Shell, DuPont, and Hoechst had admitted they supplied faulty plastic pipe and fittings to domestic water systems, which degraded in service and finally fractured.

A key point that emerged was that the manufacturers knew from tests they had performed that the plastics were sensitive to oxidation from the low levels of chlorine present in the water supply. The acetal resin fittings tended to fail first, followed by the polybutene pipe, and the verdict resolved our own dispute. However, owing to the very large numbers of such systems installed across North America, the manufacturers are still dealing with their liability. A billion dollars has been pledged by the companies involved to settle the remaining claims, making it one of the largest class actions ever resolved.



This polybutene pipe was damaged by a reaction between the plastic and chlorine in the water.

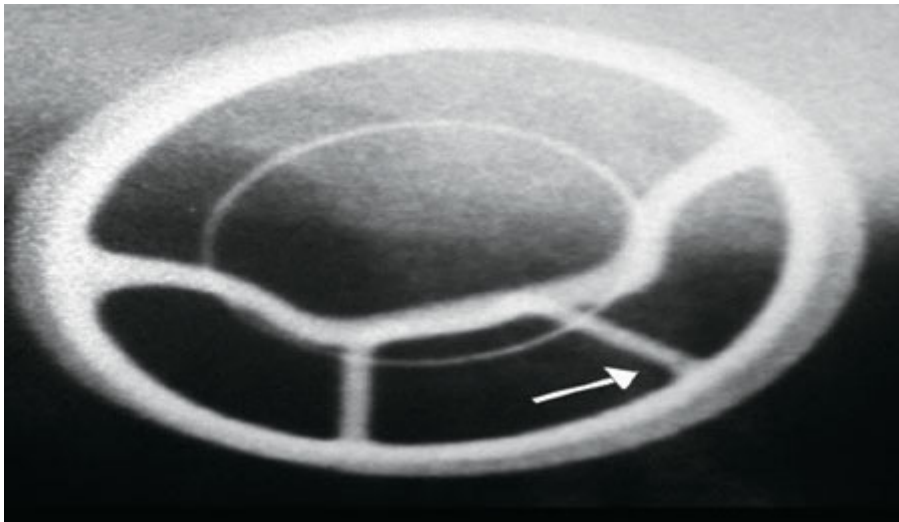
The case shows how companies ignore their own tests at their peril. Why they did so is still something of a mystery. It is possible to protect polybutene piping and acetal fittings against the known risks of oxidation, and this is done in Europe, where such plumbing is used extensively.

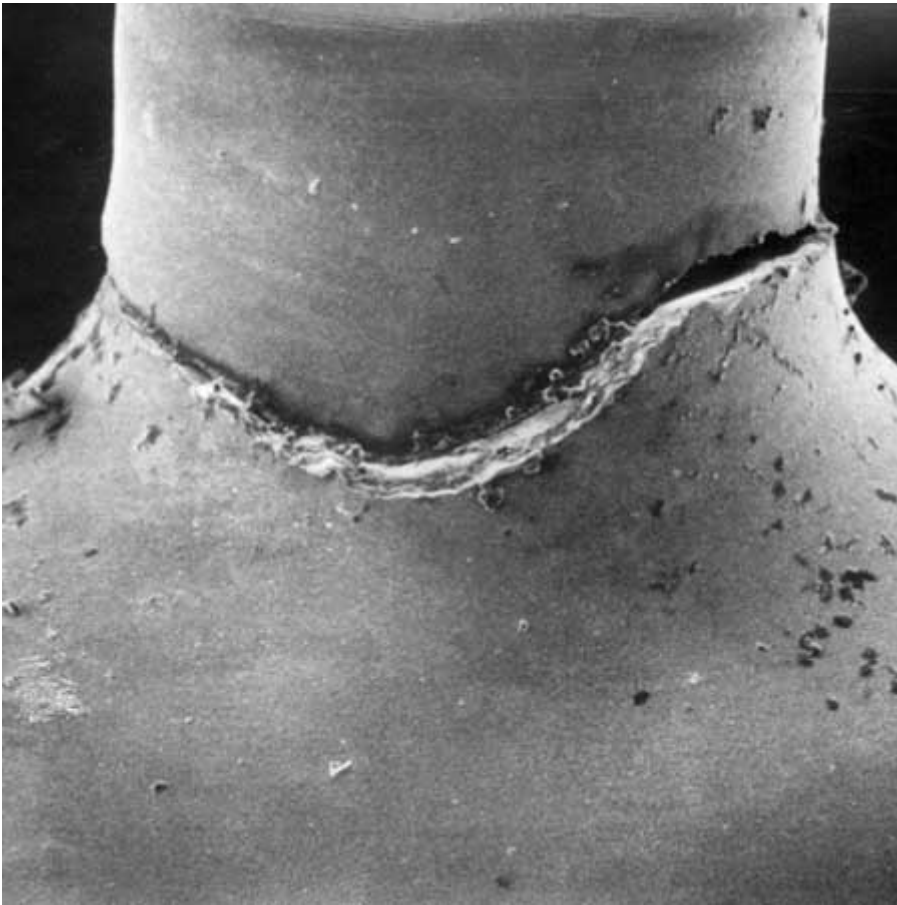
Ignoring early warnings of failure of a product in use can lead to disastrous consequences as well. One notable example is the failure of the joint in a catheter. (I investigated a catheter failure in 1990, when the tip of an epidural catheter broke away and was left in the patient's spine. The sample was a maverick, but should not have been supplied and the manufacturer paid out substantial damages.) When a new catheter design started cracking in the mid-1990s, the failure was not discovered until catastrophic fluid leakages were detected by nurses.

This was simply the final stage of failure. The cracks often connected the bore with the outer surface without much leakage. The danger of this is that bacteria living on the outer walls of the catheters can infect the fluids via the hairline cracks, an insidious and deadly problem, given the lethal nature of many bacteria in a hospital environment. A premature baby was infected in this way and suffered meningitis, which nearly killed him and led to brain damage discovered later as he grew up. The case was settled in 2008 with damages awarded to the injured child, the problem probably being caused by faulty molding of the polycarbonate joints.

Although the problem is now fixed, one can well ask why the manufacturer didn't make the product correctly in the first place. The company also failed to test in environments found in hospitals, where cleaning agents, organic liquids, and other agents that can attack this plastic are commonplace. Designers have a responsibility to test their prototypes in realistic conditions before supplying a product to hospitals.

Catheters play a part in one of the greatest advances in recent decades: the minimally invasive method of treating heart conditions. One treatment involves inserting a catheter into the major artery via the groin, threading the catheter to a blockage and inflating a polymer balloon to crush the fatty deposits and opening the artery to a better flow of blood, a method known as angioplasty. If a metal stent is placed over the balloon, it deforms and remains in place after deflation, helping to support the artery walls from collapse.





Makers of the Bjork-Shiley synthetic heart valve (top) discovered early on that stresses led to the failure of the joints holding the disk to the struts (center). The image just above shows a damaged strut under high magnification.

For all their curative power, there have been many product failures involving the equipment used in these techniques. To be sure, it is a difficult environment to design for. Fatigue fractures can be caused by the beating of the heart, and the blood itself is corrosive. But the design and manufacture of some of the devices can be questioned.

One of the worst examples of device failure remains the Bjork-Shiley synthetic heart valve. The original design tended to become clogged over time by fatty deposits so the device was redesigned to remove the problem. However, the redesign relied upon tantalum welded joints, which failed due to fatigue. Early signs of problems with the product were ignored, and the result was several hundred unnecessary deaths.

Because it involved a medical device, the manufacturer can share the blame with the primary regulatory agency. The U.S. Food and Drug Administration failed at first to investigate the cause of heart valve failure. Indeed, it could be argued that the agency should have banned the device as early as 1979, but it did not act until 1986. This episode is considered to be one of the agency's worst regulatory failures because use of the valve could have been halted almost immediately rather than years later.

SOMETIMES PRODUCTS CAN BE USED LONG AFTER THEY HAVE BEEN RULED DANGEROUS. A case I examined in the 1970s involved cars suddenly catching fire; I traced the cause to ozone cracks and wear in the rubber and plastic fuel lines of the Fiat Mirafiori (which was sold in the U.S. as the Brava). The car was recalled in many markets, but not the Republic of Ireland, where unwitting owners were still driving very dangerous vehicles.

In one horrendous accident, two young children were severely injured when a Fiat car burst into flames just after the mother had left the car to enter her house. Investigators suspected the fuel pipes running through the car's interior. The family sued the company for the injuries to the children. Rather than settle, the company went to court, where the research I had performed decades before was produced.

Needless to say, the company paid substantial damages.

That is not all, however. The publicity engendered by the case in the *Irish Times*, a leading newspaper in Ireland, led to old cases involving serious accidents with the car being reopened and reinvestigated. In one particularly grisly instance, the resulting car fire was so intense that the remains of a priest could only be identified from his sandal fittings. There were many car fires in the U.S. with similar results.

None of the accidents had to happen. If the fuel line had been well designed from the beginning using armored ozone-resistant rubber, there would have been no problem.

The way Fiat handled this case was echoed recently by Toyota, which denied its accelerator problems for several years until pressures of litigation finally led to admission of a serious design flaw. Both the Fiat and Toyota cases show that design faults are replicated endlessly and needlessly. Such problems should have been discovered by rigorous testing *before* those models ever went to the dealer showroom.



The Fiat Mirafiori was built with defective fuel lines, which led to some horrific and sometimes fatal car fires.

I have analyzed components for companies that test new models fitted with new parts, and whenever those components fail, there is immediate remedial action. In one case, a new design of radiator header tank in the cooling system experienced cracking that led to loss of fluid and engine seizure. It turned out the problem was the result of a faulty tank rather than a flawed design, so the supplier was at fault for sending the product to the car company. Such “mavericks” do occur from time to time, but the onus is on the manufacturers to inspect and test before shipping their goods.

People often say that “lessons have been learned” after major disasters, but it is often untrue. Fuel pipes, for example, continue to fail. In September 2006, a Nimrod reconnaissance aircraft suffered a fuel leak that resulted in a fire during a mission over Afghanistan; the plane crashed, killing 14 British military personnel on board. A report on the crash determined that, due to the design flaw, the aircraft had “never been airworthy from the first time it was released to the service” nearly 40 years earlier.

I recently examined a leaking fuel pipe involved in an aircraft tractor fire at London’s Heathrow Airport. Although the pipe was armored, it was not ozone resistant, and the cracks penetrated the armor to cause

sudden failure and fuel leak. There have been several other similar fires, and not just at Heathrow, showing the problem to be a design fault by the manufacturer.

THERE ARE OFTEN WARNING SIGNS IN MANY FAILURE CASES, WARNINGS THAT ARE IGNORED AT PERIL. The accident aboard the *Deepwater Horizon*, for instance, appears to have been caused in part by faults in critical components of the blowout preventer, and tests which may have uncovered these faults had not apparently been performed just before the fatal blowout.

Light regulation may have contributed to that problem, as in many other recent failures (and not just in engineering). But companies are certainly able to address such problems themselves: There are many independent forensic engineers who can analyze warning signs of safety-critical products and advise remedial action well before any catastrophic failures. Products should be designed with ample failsafe features and redundant parts in the case of failure so a device continues to function. And product testing must be conducted in realistic conditions.



A poorly designed fuel line led to the crash of a Nimrod reconnaissance aircraft over Afghanistan.

The report by the National Transportation Safety Board on the collapse of the I-35W bridge in Minneapolis in 2008 concluded that the span was faulty from its inception. The bridge was opened to traffic a few months before the Silver Bridge disaster of December 1967, when a suspension bridge collapsed suddenly and 46 drivers and occupants of cars on the bridge fell into the Ohio River below.

That accident should have been a flashing red light to everyone involved with the bridge in Minneapolis. The Silver Bridge fell because it was under-designed and lacked any redundancy in its hangers. The I-35W bridge was also under-designed, with gusset plates at the joints of the support girders too thin for the design loads on the bridge. Then concrete was added to the roadway, and just before the collapse, materials and equipment for a new surface were added just above one of the weakest points of the structure. Regular inspections—introduced after the Silver Bridge disaster—showed defects such as fatigue cracks and corrosion as well as signs of premature deformation of the plates, but the warnings were ignored.

Warnings of early failure must be heeded if future disasters are to be prevented, especially for large structures where inspection is mandatory. Otherwise what is the point of inspection?

One way to try to prevent future disasters is to publicize such accidents much more widely. Rather than be embarrassed by engineering failures, we should study them to understand why things went so wrong.

Engineering Failure Analysis is an engineering journal published in the United Kingdom that is dedicated to case studies of failure in engineering products and processes. With the power of current search engines, even obscure and detailed case studies are available on every engineer's personal computer.

Product failures must be analyzed by unbiased investigators, individuals who cannot be pressured by over-zealous managers or finance officers. But all engineers should be aware of their basic responsibility to design safe and reliable products.

Peter R. Lewis is a professor of forensic engineering at The Open University in Milton Keynes, England. Lewis is the author of Forensic Materials Engineering, published by CRC Press Inc. in 2004, and Forensic Polymer Engineering, published this year by Woodhead Publishing Ltd.