PROFESSIONAL ETHICS

Notes

Risk, Safety, and Liability in Engineering

Naveen is employed as a chemical engineer at Hindustan Manufacturing. Although he does not work with hot metals himself, he supervises workers who are exposed to hot metals 8 hours a day five day a week Naveen becomes concerned when several workers develop respirator problems and complain about “those bad smelling fumes from the hot metals”. When Naveen asks his superior, about air quality in the workplace, the reply is that the workplace is in full compliance with OSHA guidelines. Naveen also learns that OSHA guidelines do not apply to chemicals that have not been tested and that a relatively small percentage of chemical in the workplace have actually been tested. This is also the case with the vast majority of chemicals that workers are exposed to at Hindustan.

Naveen goes to Hindustan’s science library, talks to the reference librarian about his concerns, and does a literature search to see if he can find anything that might be helpful in determining why the workers have developed respiratory problems. He finds the title of an article that looks promising and asks the reference librarian to send for a copy. The librarian tells Naveen that the formal request must have signed approval of superior, so Naveen fills out the request form and sends it to superior’s office for approval.

One month later the article has still not arrived. Naveen asks call about the request. Call replies that he doesn’t recall ever seeing it. He tells Naveen it must have gotten “lost in the shuffele”. Naveen feels out another form and this time personally hands it to Superior. Superior says he will send it to the reference librarian right away.

Another month passes and the article has not arrived. Naveen mentions his frustration to the reference librarian, who replies that he never received a request from Superior to order the paper. What should Naveen do now?

1.1 Introduction

Naveen's concern for safety in the workplace is a common one for engineers. How should engineers deal with issues of risk and safety, especially when they involve possible liability for harm? In the Hindustan case, the risk arises from a manufacturing process. Other risks arise from products, structures, and substances created by engineers.

Engineering necessarily involves risk. Even if engineers did not innovate, but rather designed things in the same way year after year, the chance of producing chemicals that were once thought to be safe. But the element of risk is greatly increased because engineers are constantly involved in innovation. A bridge or building is constructed with new materials or with a new design. New machines are created and new compounds synthesized, always without full knowledge of their long–term effects on humans or the environment.

Dealing with risk posses many perils for the engineer. In this chapter, we shall consider some of these perils, especially as they relate to the engineer's ethical and professional responsibilities. First, we shall look at some reasons why accidents are hard to anticipate and risk is often difficult to estimate. Some studies of accidents in technology-related areas have even suggested that accidents are inevitable and that there is such a thing as the "normal accident."

Next, we shall examine some reasons why it is easy for engineers to accept incrementally increasing risk, almost without realizing it. Using the events leading up to the challenger explosion as an illustration, we shall show how engineers can increase the chance of accidents by a process, which may not be fully realized until an accident occurs.

Then, we shall look at several different approaches to the definition of acceptable risk. Engineers should be aware of the fact that different social groups have different definitions of acceptable risk and different agendas regarding proper management of risk. One approach is that of the risk expert, who wants to balance risk and benefit in a way that optimizes overall public well-being. The layperson, on the other hand, wants to protect himself or herself from risk involves certain dreaded events, such as cancer or nuclear catastrophe. This approach leads to a definition of acceptable risk that differs from the risk expert’s. The government regulator wants as much assurance as possible that the public is not being exposed to unexpected harm. This approach is different from either of the other two.

To manager risk responsibly, engineers should also be aware of some of the issues posed by legal liability for risk. One of these issues is that the standards of proof are very different in science and tort law. This fact poses ethical problems, because the standards of tort law give more protection to the victims of technologically imposed risk, and the standard of science give more protections to the creators of technologically imposed risk, and the standards of science give more protection to the creator of technologically imposed risk. Another issue is the legal liabilities incurred by engineers in attempting to protect the public from unnecessary risk.

Before discussing any of this, however, we should consider what the engineering codes have to say about risk and safety.

1.2 Codes and Engineering Practice Regarding Risk and Safety

Virtually all engineering codes give a prominent place to safety, stating that engineers must hold paramount the safety, health, and welfare of the public. The relationship of risk to safety is very close. If products, structures, processes, and substances are unsafe, they subject humans and the environment to undue risk. Therefore, the statements in the codes having to do with safety are relevant to the topic of risk.

The NSPE code, in sections II.1.b and III.2.b, requires engineers to design safely, defining this in terms of “accepted engineering standards.” For example, item III.2.b instructs engineers not to “complete, sign or seal plans and / or specifications that are not of a design safe to the public health and welfare and in conformity with accepted engineering standards.” Items II.1.a instructs engineers that if their professional judgment is overruled in “circumstances where the safety, health, property or welfare of the public are endangered,” they are obligated to “notify their employer or client and such other authority as may be appropriate.”

Many other engineers’ codes give similar instructions to engineers. For example, the IEEE Code of Ethics emphasizes member’s responsibility for the public’s health and safety in three ways. First electrical engineer agree “to accept responsibility in making engineering decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment”. Second, they agree “to improve the understanding of technology, its appropriate application, and potential consequences.” Third, they agree “to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations.” These last two items emphasize the importance of informed consent.

Engineering practice is suffused with concern with safety. One of the most pervasive concepts in engineering practice is the notion of “factors of safety.” If the largest load a walkway will have to carry at any one time is 1000 pounds, for example, a prudent engineer might design the walkway geometry to carry 3000 pounds. The walkway dimensions for normal usage would then be designed with a factor of safety of three.

Accepted engineering practice goes still further. In choosing materials to build the walkway, an engineer might begin with a material that has an advertised yield stress of a given number of pounds per square inch, and then treat this material as if it had only half of that capacity in determining how much materials to include in the walkway construction. This introduces an additional factor of safety of two. The final overall factor of safety at the walkway would be the product of the two separate factors, or six in this example.

Thus, a prudent engineer would design the walkway to be six times as strong as required for normal everyday use to account for unpredictably high loads or unaccountably weak construction material. This approach is taught to all engineers early in their training, and factors of safety of six or higher are the norm rather than the exception.

Accidents, however, are often difficult to predict, and so the degree of risk is often hard to estimate, as we shall see in the next section.

1.3 Difficulties in Estimating Risk

Estimating risk has been described by one writer as looking “through a glass darkly.” If we could accurately predict the harm resulting from engineering work, there would be no risk. We would know precisely the harm to expect. Instead, we can only estimate the magnitude and probability of harm. To make matters worse, often we cannot even make our estimate with accuracy. In actual practice, therefore, estimating risk (or “risk assessment”) is an uncertain prediction of the probability of harm. In this section, we shall consider some of the methods of estimating risk, the uncertainties in these methods, and the value judgments that these uncertainties necessitate.

Detecting Failure Modes

With respect to new technologies, engineers and scientists must have some way of estimating the risks that they impose on those affected by it. One of the methods for assessing risk involves the use of a fault tree. A fault tree is a diagram of the possible ways in which a malfunction or accident can occur. Fault trees are most often used to anticipate hazard for which there is little or no direct experience, such as nuclear meltdowns. It enables an engineer to analyze in a systematic fashion the various failure modes attends to an engineering project. A failure mode is a way in which a structure, mechanism, or process can malfunction. For example, a structure can rip apart in tension, crumble to pieces in compression, crack and break in bending, lose its integrity due to corrosion (rusting), explode due to excessive internal pressure, or burn due to excessive temperature. Figure 1.1 illustrates how a fault tree analysis can be used to discover why an automobile will not start.

Another approach to a systematic examination of failure modes is the events tree analysis. In a fault-tree analysis we begin with an undesirable event, such as a car not starting or the loss of electrical power to a nuclear power plant safety system. Then, we reason backward to determine what might have led to the event. By contrast, in an event-tree analysis, we begin with an initial event and reason forward to the state of the system to which the event can lead. Figure 1.2 illustrates in schematic form an event-tree analysis.

This simplified event tree for an accident involving a loss of coolant in a typical nuclear power plant begins with a failure and enumerates the various events to which this failure could lead. This event tree shows the logical relationships.

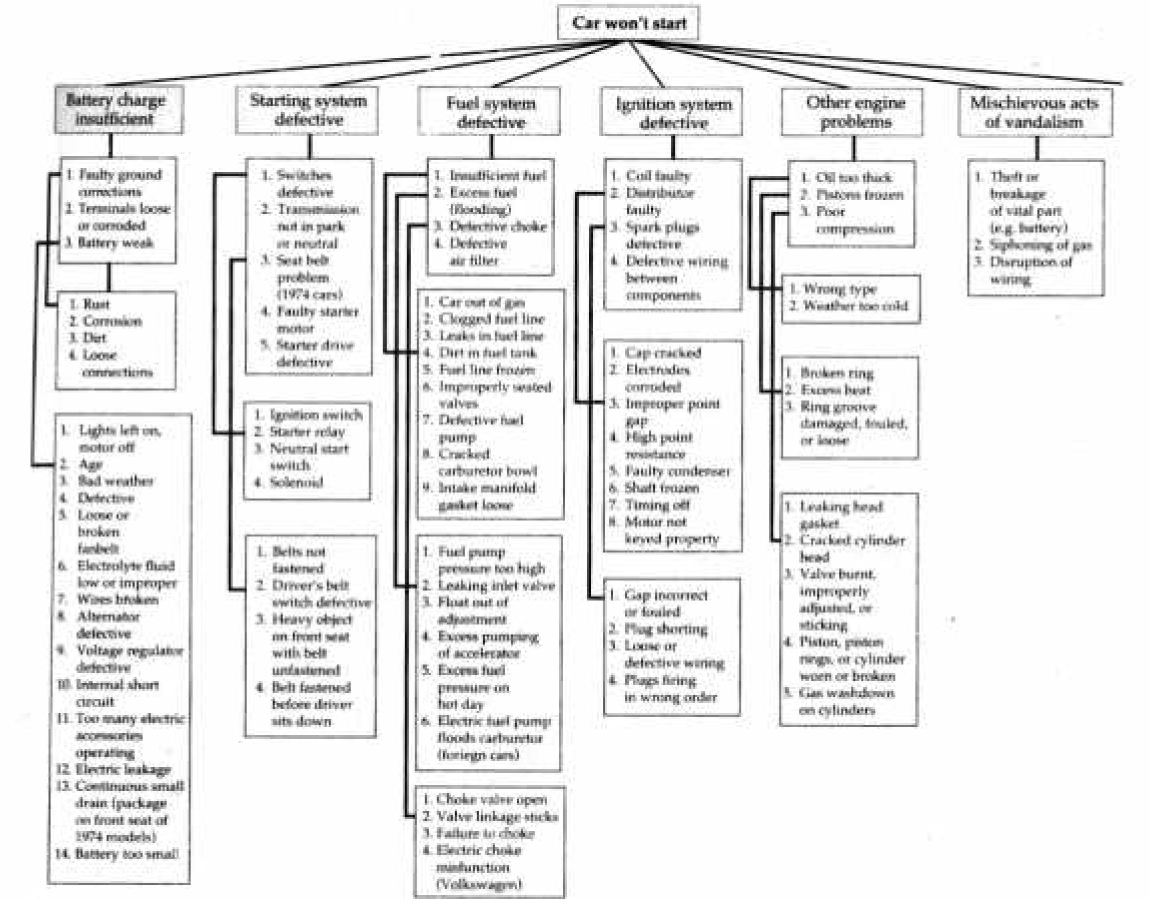
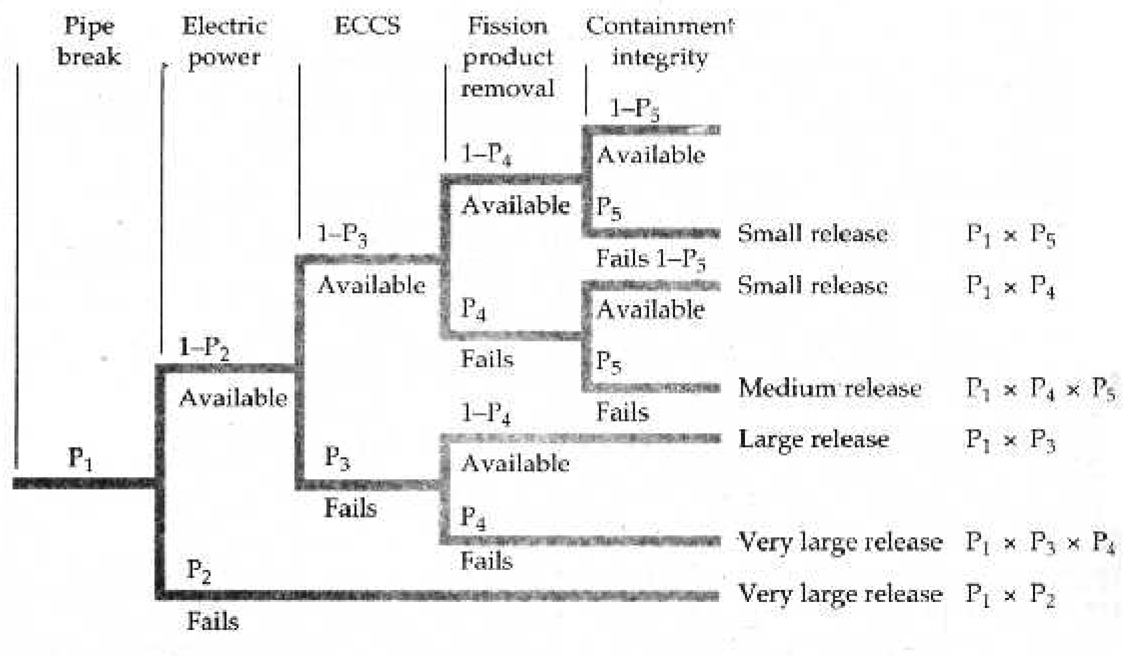

Car won't start
Battery charge insufficient
Starting system defective
Fuel system defective
Ignition system defective
Other engine problems
Mischievous acts of vandalism
1. Faulty ground connections
2. Terminals loose or corroded
3. Battery weak
1. Rust
2. Corrosion
3. Dirt
4. Loose connections
1. Lights left on, motor off
2. Age
3. Bad weather
4. Defective
5. Loose or broken fanbelt
6. Electrolyte fluid low or improper
7. Wires broken
8. Alternator defective
9. Voltage regulator defective
10. Internal short circuit
11. Too many electric accessories operating
12. Electric leakage
13. Continuous small drain (package on front seat of 1974 models)
14. Battery too small
1. Switches defective
2. Transmission not in park or neutral
3. Seat belt problem (1974 cars)
4. Faulty starter motor
5. Starter drive defective
1. Ignition switch
2. Starter relay
3. Neutral start switch
4. Solenoid
1. Belts not fastened
2. Driver's belt switch defective
3. Heavy object on front seat with belt unfastened
4. Belt fastened before driver sits down
1. Insufficient fuel
2. Excess fuel (flooding)
3. Defective choke
4. Defective air filter
1. Car out of gas
2. Clogged fuel line
3. Leaks in fuel line
4. Dirt in fuel tank
5. Fuel line frozen
6. Improperly seated valves
7. Defective fuel pump
8. Cracked carburetor bowl
9. Intake manifold gasket loose
1. Fuel pump pressure too high
2. Leaking inlet valve
3. Float out of adjustment
4. Excess pumping of accelerator
5. Excess fuel pressure on hot day
6. Electric fuel pump floods carburetor (foriegn cars)
1. Choke valve open
2. Valve linkage sticks
3. Failure to choke
4. Electric choke malfunction (Volkswagen)
1. Coil faulty
2. Distributor faulty
3. Spark plugs defective
4. Defective wiring between components
1. Cap cracked
2. Electrodes corroded
3. Improper point gap
4. High point resistance
5. Faulty condenser
6. Shaft frozen
7. Timing off
8. Motor not keyed properly
1. Gap incorrect or fouled
2. Plug shorting
3. Loose or defective wiring
4. Plugs firing in wrong order
1. Oil too thick
2. Pistons frozen
3. Poor compression
1. Wrong type
2. Weather too cold
1. Broken ring
2. Excess heat
3. Ring groove damaged, fouled, or loose
1. Leaking head gasket
2. Cracked cylinder head
3. Valve burnt, improperly adjusted, or sticking
4. Piston, piston rings, or cylinder worn or broken
5. Gas washdown on cylinders
1. Theft or breakage of vital part (e.g. battery)
2. Siphoning of gas
3. Disruption of wiring

Figure 1.1 Fault – analysis of failure of an automobile to start the failure appears at the top of the fault tree, and the possible causes of the failure appear as “branches” of the fault tree.

Between the possible ways that a pipe break can affect the safety systems in a nuclear plant. If both a pipe and on-site power fail simultaneously, the outcome will be a very large release of radioactive coolant. If these two systems are independent, the probability of this happening is the product of the two probabilities taken separately. For example, if there is one chance in 10^{-4} (P_1 = 0.0001) that the pipe will break and one chance in 10^{-5} (P_2 = 0.00001) that the on-site power will fail, then the chance of a loss of a very large release is one in 10^{-9} ($P = P_1 P_2$).



Reproduced, with permission, from the *Annual Review of Energy*, Volume 6, © 1981 by Annual Reviews, Inc. Courtesy N. C. Rasmussen.

Figure 1.2 An event tree analysis of a pipe break in a nuclear plant

Although it is necessary to go through such analyses to ensure that we have taken into account as many failure modes as possible, they have severe limitations. First, we cannot anticipate all of the mechanical, physical, electrical, and chemical problems that might lead to failure. Second, we cannot anticipate all of the points of human error that could lead to failure. Third, the probabilities assigned to the failure modes are largely conjectural and based on analyses that cannot be corroborated by experimental testing. We are not, for example, going to melt down a nuclear reactor to determine the probability of such an occurrence leading to a chain reaction fission explosion. In many cases we do not know the probability of material behavior at extremely elevated temperatures. Fourth, we can never be sure we have all of the possible initiating events (even ones we know exist in different contexts) included on the event tree or placed in the right order.

Are There “Normal Accidents”?

Sociologist Charles Perrow confirms some of these problems by arguing that there are two characteristics of high-risk technologies that make them especially susceptible to accidents, so that we can speak of “normal accidents”. These two characteristics are the “tight coupling” and the “complex interactions” of the parts of a technological system. These two factors not only make accidents likely but also difficult to predict and control. This, in turn, makes risk difficult to estimate.

Processes are tightly coupled if they are connected in such a way that one process is known to affect another and will usually do so within a short time. In tight coupling there is usually little time to correct a failure and little likelihood of confining a failure to one part of the system, so that the whole system is damaged. A chemical plant is tightly coupled, because a failure in one part of the plant can quickly affect other parts of the plant. A university, by contrast, is loosely coupled, because if one department ceases to function, the operation of the whole university is usually not threatened.

Processes can also be complexly interactive, in that the parts of the system can interact in unanticipated ways. No one dreamed that when X failed, it would affect Y. chemical plants are also complexly interactive, in that parts affect one another in feedback patterns that cannot always be anticipated. A post office, by contrast, is not so complexly interactive. The parts of the system are related to one another for the most part in a linear way and do not usually interact in unanticipated ways to cause the post office to cease functioning. If a post office ceases to function, it is usually because of a well-understood failure.

Examples of complexly interactive and tightly coupled technical systems include not only chemical plants but also nuclear power plants, space missions, and nuclear weapons systems. Being tightly coupled and complexly interactive, they can have unanticipated failures, and there is little time to correct the problems or keep them from affecting the entire system. This makes accidents difficult to predict and disasters difficult to avoid, once a malfunction appears.

Unfortunately, it is difficult to change tightly coupled and complexly interactive systems to make accidents less likely. To reduce complexity, decentralization is required, enabling operators to have the ability to react independently and creatively to unanticipated events. To deal with tight coupling, however, centralization is required, in which operators follow orders quickly and without question to avoid a failure or limit its effects. It may not be possible, furthermore, to make a system both loosely coupled and noncomplex. According to Perrow, therefore, accidents in complex, tightly coupled systems are inevitable and, in this sense, “normal”. Engineers know that, to some extent, one can include localized and autonomous automatic controls to protect against complexity failures, coupled with manual overrides to protect against tight coupling failures.

Here is an example of an accident in a system that was complexly interactive and tightly coupled and that could have been prevented by the type of good engineering just described. In the summer of 1962 the New York Telephone Company completed heating system additions to a new accounting building in Yonkers, New York. The three-story, square-block building was a paradigm of safe design, using the latest technology.

In October 1962, after the building was occupied and the workers were in place, final adjustments were being made on the building’s new, expanded heating system locate in the basement. This system consisted of three side-by-side, oil-fired boilers. The boilers were designed for low pressure of less than 6.0 psi and so were not covered by ASME boiler and pressure vessel codes. Each boiler was equipped with a spring-loaded safety relief valve designed to open and release steam into the atmosphere if the boiler pressure got too high. Each boiler was also equipped with a pressure-actuated cutoff valve designed to cut off oil flow to the boiler burners in the event of excessive pressure. The steam pressure from the boilers was delivered to the steam radiators, each of which had its own local relief valve. Finally, in the event that all else failed, a one-foot diameter pressure gauge with a red danger zone painted on the face sat on the top of each boiler. If the pressure got too high, the gauge was supposed to alert a janitor who operated the boilers, so he could turn off the burners.

On October, 2, 1962, the following events transpired.

1. The building custodian decided to fire up boiler 1 in the heating system for the first time that fall. The electricians had just wired the control system for the new companion boiler (boiler3) and successfully tested the electrical signal flows.
2. The custodian did not know that the electricians had left the fuel cutoff control system disconnected. The electricians had disconnected the system because they were planning to do additional work on boiler 3 the following week. They intended to wire the fuel cutoffs for the two boilers in series (that is, high pressure in either would stop both).
3. The custodian mechanically closed the header valve, because it was a warm, Indian summer day, and he did not want to send steam into the radiators on the floors above. Thus, the boilers was delivering steam pressure against a blocked valve, and the individual steam radiator valves were thus out of the control loop.
4. As subsequent testing showed, the relief valve had rusted shut after some tests the previous spring in which the boilers had last been fired up. (Later, laws were enacted in New York state that require relief valves for low-pressure boiler systems to be operated by hand once every 24 hours to ensure that they are not rusted shut. At the time, low-pressure boiler systems were not subject to this requirement).
5. This was on Thursday before payday, and the custodian made a short walk to his bank at the lunch hour to cash a check, shortly after turning on the boiler 1.

6. The cafeteria was on the other side of the wall against which the boiler end abutted. Employees were in line against that wall awaiting their turn at the cafeteria serving tables. There were more people in line than there would have been on Friday, because on payday many workers went out to cash their paychecks and have lunch at local restaurants.
7. Boiler exploded. The end of the boiler that was the most removed from the wall next to the cafeteria blew off, making the boiler into a rocketlike projectile. The boiler lifted off its stanchions and crashed into the cafeteria, after which it continued to rise at great velocity through all three stories of the building. Twenty-five people were killed and almost one hundred were seriously injured.

The events that led to this disaster were complexly interrelated. There is no possible way that fault-tree or event-tree analyses could have predicated this chain of events. If the outside temperature had been cooler, the custodian would not have closed the header valve and the individual steam radiator valves in each upstairs room would have opened. If the relief valve had been hand-operated every day, its malfunction would have been discovered and probably corrected. If the time had not been noon and the day before payday, the custodian might have stayed in the basement and seen the high pressure gauge reading and turned off the burners. If it had not been lunch time, unfortunate victims would not have been in the cafeteria line on the other side of the wall from the boiler.

The events were also tightly coupled. There was not much time to correct the problem once the pressure started to rise and no way to isolate the boiler failure from a catastrophe in the rest of the building.

1.4 Normalizing Deviance

The complexity and tight coupling of technical system are not the only factors that make accidents more likely. Engineers can also increase the risk to the public by allowing increase number of deviancies from proper standards of safety and acceptable risk. Sociologist Diane Vaughn refers to this phenomenon as the *normalization of deviance.*

Every design carries with it certain predictions about how the designed object should perform in use. Sometimes these predications are not fulfilled, producing what are commonly referred to as *anomalies*. Rather than correcting the design or the operating conditions that led to the anomalies, engineers or managers too often do something less desirable. They may simply accept the anomaly or even increase the boundaries of acceptable risk. Sometimes this process leads to disasters.

This process is dramatically and tragically illustrated by the events leading to the challenger disaster. Neither the contractor, Morton Thiokol, nor NASA expected the rubber O-ring sealing the joints in the Solid Rocket Booster (SRB) to be touched by the hot gases of motor ignition, much less to be partially burned. However, as flights confirmed damage to the sealing ring, the reaction by both NASA and Thiokol was to accept the anomalies without attempting to remedy the problems that caused the anomalies.

Here are several examples of normalizing device:

1. In 1977, test result showed that the SRB joints would rotate open at ignition, creating a larger gap between the tang and clevis. According to NASA engineers, the gap was large enough to prevent the secondary seal from sealing if the primary O-ring failed late in the ignition cycle. Nevertheless, after some modifications, such as adding sealing putty behind the O-rings, the joint was officially certified as an acceptable risk, even though the joint’s behavior deviated from design predictions.
2. Another anomaly was discovered in November 1981 in flight STS-2, where there was “Impingement erosion” of the primary O-ring in the right SRB’s aft field joints. The hot propellant gasses had moved through the “blow holes” in the zinc chromate putty in the joints. The blowholes were caused by entrapped air introduced at time the putty was installed. Even though this troubling

phenomenon was not predicated, the joints were again certified as an acceptable risk.

3. A third anomaly occurred in 1984 with the launch of STS 41-B, when, for the first time, two primary O-rings on two different joints were eroded. Again, the erosion on two joints was termed an acceptable risk.
4. Another anomaly occurred in 1985, when “blowby” of hot gases had reached the secondary seal on a nozzle joints. The nozzle joints were considered safe because, unlike the field joints, they contained a different and very safe secondary seal, a “face seal”. The problem was that a similar malfunction could happen with the field joint, where the danger was much more serious, and these problems were not deal with.
5. Perhaps the most dramatic example of expanding the boundaries of acceptable risk was in the area of the acceptable temperature for launch. Prior to the challenger launch, the lowest temperature of the seals at launch time was 53 degrees. (At that time, the ambient temperature was in the high 60s.) On the night before the launch of challenger, however, the temperature of the seals was expected to be 29 degrees. Thus, the boundaries for acceptable risk were expanded by 24 degrees.

The result of accepting these anomalies without making any adequate attempt to remedy the basic problem (poor seal design), and of lowering the temperature considered acceptable for launch, led to the tragic destruction of the challenger and the loss of its crew.

Vaughn argues that these kinds of problems cannot be eliminated from technological systems and that, as a result, accidents are inevitable. Whether or not this is the case, there is no question that technology imposes risk on the public and that these risks often difficult to detect, and eliminate. Now let us examine some of the controversies surrounding the concept of acceptable risk.

1.5 The Expert's Approach to Acceptable Risk: Identifying and Defining Acceptable Risk

Identifying Risk

To assess a risk, an engineer must first identify it. To identify a risk, an engineer must first know what a risk is. Most people would agree that the concept of risk involves the notion of adverse effect or harm. We might define a harm as an invasion or limitation of a person's freedom or well-being. Some of the most important types of well-being are physical well-being, psychological well-being, and economic well-being.

For the most part, engineering risks have to do with physical and economic well-being. Engineering work can subject us to risks of health and accident or physical injury. This affects our economic well-being. Faulty design of a building can cause it to collapse, resulting in economic loss to the owner and perhaps death for the inhabitants. Faulty design of a chemical plant can cause accidents and economic disaster.

This account of risk is in accord with the thought of many risk experts. William W. Lowrance, for example, defines risk as "a compound measure of the probability and magnitude of adverse effect." Risk, according to Lowrance, is composed of two elements: the likelihood of an adverse effect or harm and the magnitude of that adverse effect or harm. By "compound," Lowrance means "the product". Risk, for the risk expert, is thus the product of the likelihood and the magnitude of the harm. A relatively slight harm that is highly likely might constitute a greater risk than a relatively large harm that is far less likely.

A 1992 National Public Radio story on the Environmental Protection Agency began with a quotation from EPA official Linda Fisher illustrating the risk expert's conception of risk:

A lot of our priorities are set by pubic opinion, and the public quite often is more worried about things that they perceive to cause greater risks than things that really cause