CHAPTER 3

FIVE CASES AND THE MODEL

3.1 Introduction

In this chapter I will use five cases to build the theoretical model and hypotheses to be tested in the remaining sections of the paper. Because the existing literature is limited and there is a lack of strong theory in this area (as noted in chapter two), I will use grounded theory (Glaser & Strauss, 1967), to build hypotheses from case material. The five cases that I will use are the Chernobyl nuclear plant explosion, the grounding of the Exxon Valdez, the Bhopal chemical plant gas leak, the mis-grinding of the mirror for the Hubble space telescope, and the explosion of the space shuttle Challenger.

The case material will be drawn from reports that were intended to provide factual accounts of the catastrophes. These reports were generally not intended to generate theory beyond that of the incident itself. Even in Vaughan's account of the Challenger disaster (1990), she points out that, "This case study does not generate the sort of comparative information on which definitive policy statements can be made".

In each of the cases, I relied upon a main source for much of my information. However, I crossed checked each source against other sources to ensure that my primary source of "facts" was not noticeably biased.

A summary of each case will be provided and then I will analyze the key

factors which seem to have contributed to the catastrophe. At the end of the chapter, I will look across cases to see if there is a set of similarities or common factors that appears to stand out.

I will also refer back to the existing literature and theories (Roberts, 1992; Turner, 1978) to see how the common factors that I have found link to previous work. Finally, based on the common factors derived by my grounded theory case analyses, and supported by the theoretical literature, I will present a set of hypotheses to be tested.

3.2 Chernobyl

The Chernobyl disaster occured in the Ukraine, then a part of the Soviet Union, on April 26, 1986. At 1:24 a.m. on that day, the No. 4 nuclear power reactor at Chernobyl exploded sending radiation high into the atmosphere and spreading it far onto the surrounding countryside. Large areas of farmland in the Ukraine, the "breadbasket" of the former Soviet Union will remain poisoned by radioactivity for years to come. Many individuals were also exposed to radiation. Some died outright; others will face increased risk of cancer in the years to come.

Below, I will try to summarize the events that led to this organizational failure. In doing so, I will rely heavily on the account of Grigori Medvedev (1991) who was a high-ranking nuclear scientist within the Soviet nuclear industry at the time of the accident. I will also use several backup sources, including Hamman & Parrott (1987).

THE PLAYERS:

In the former Soviet Union, it was considered prestigious to work in the nuclear power industry as compared to the conventional power industry. As a result, assignments within the industry and career advancement were based on political criteria rather than qualifications. Many of the engineers in the nuclear power industry had no training in nuclear energy; they came from a wide range of other engineeering or scientific backgrounds. This was the case at Chernobyl.

The list of characters in the chain of command (who are all associated with the disaster) at Chernobyl includes Scherbina, the deputy chairman of the council of ministers, " who automatically transposed to matters of energy the management methods he had used (for years) in the gas industry". Below him was Mayorets, Minister of Energy and Electrification "who was quite incompetent in energy matters generally, and in nuclear energy in particular", (Medvedev, p. 21). Mayorets' first act upon his appointment was to abolish the directorate which handled research and development. He also cut back on maintenance and reserve power at the country's power stations, which raised the rate of utilization of installed capacity, but "the risk of a major disaster increased", (Medvedev, p. 21).

Mayorets also was in favor of maintaining a previously established "tradition of silence" (Medvedev, p. 20). Soon after his appointment, he signed an order which said:

> "Information about the unfavorable ecological impact of energy-related facilities (the effect of electromagnetic fields, irradiation, contamination of air, water, and soil) on operational personnel, the population and the environment shall not be reported openly in the press or broadcast on radio or television." (Medvedev, p. 20)

It was not only the public which was subject to this tradition of silence. Most of the individuals working within the nuclear industry also had no access to information about accidents that happened at other Soviet plants or other plants worldwide. Knowledge about the Three-Mile Island disaster was classified and available only to the top echelon of the industry.

Below Mayorets was Bryukhanov who was the director of the Chernobyl plant. His background was as a turbine engineer, "but unfortunately he was not a nuclear power expert... People who work at nuclear power stations just have to be experts in nuclear power." (Medvedev, p. 42)

Reporting to Bryukhanov was Fomin who was the chief engineer of the Chernobyl plant. Fomin had trained as an electrical engineer and had previously worked in a thermal power station. Fomin designed the tests that were being run at the time the reactor exploded. The final character I must introduce is Dyatlov, who was trained as a pure physicist. Dyatlov was the deputy chief engineer for operations for the No. 3 and No. 4 reactor (the one which exploded). He was in charge of the control room at the time of the explosion.

THE TEST PROGRAM:

Below I will try to summarize the events of the accident drawing heavily

from Medvedev's account (1991), but omitting as much of the technical details as possible. The seeds of the disaster were laid when a test plan for the reactor was drawn up.

The test was designed to help engineers solve a problem that they were grappling with involving a basic design flaw in the Chernobyl type of reactor (an RBMK -- I will comment more on this type of reactor design later) Specifically,

> "there are some essential safety systems of the RBMK reactor which cannot tolerate an interruption in power supply... and for which power supply is absolutely essential after an emergency shutdown of the reactor and a second group of systems that can do without electricity for periods of time no longer than tenths of a minute and which are also essential to safety. (Hamman & Parrott)"

Now, the plants had back-up diesel generators to provide this needed electricity after an emergency shutdown. Unfortunately, the generators took about 50 seconds to come to full power--too long. So, the engineers felt that they could devise a way to draw power from the reactor's turbines which would still be spinning (although slowing down) after an emergency shutdown. This would give them enough power to operate safely until the generators came to full power. Previous attempts to get enough power from the still spinning turbines had failed in tests at other plants and at Chernobyl. Recently, the engineers had come up with a new device designed to solve the problem, and they needed to test it. Thus, Fomin, the chief engineer of the plant wrote up a test program to carry out such a test.

The test plan involved allowing an interial rundown of the rotor blades of the generator, which was to supply its own needs at a power level of 700-1000 megawatts.

> "...such a rundown should really have taken place when the reactor was being shut down because in a maximum design-basis accident the reactor's emergency power reduction system, on the basis of the five emergency parameters, is supposed to be triggered and to shut down the reactor. Yet, a different disasterously hazardous course was followed: the generator was allowed to run down while the reactor was still functioning. Why such a dangerous regime was chosen remains a mystery. One can only assume that Fomin wanted a totally pure experiment". (Medvedev, p. 50).

In other words, the test should have been designed so that it mimicked the conditions under which the generator was supposed to keep working--a situation in which low power signalled that the reactor should be shut down. Instead, the test was designed to run when the reactor was fully functional--a very dangerous test if something went wrong.

Furthermore, as Medvedev points out, there was an additional major flaw in the test design.

> "...in keeping with the experimental program, the emergency core cooling system was disconnected from the multiple forced circulation loop. This was one of Fomin's most severe and fatal mistakes. And it was done deliberately, so as to prevent the cold water from the ECCS tanks from entering the hot reactor causing a heat shock. When the prompt neutron power surge later started and the main circulation pumps were disconnected, thus leaving the reactor without cooling water, ...emergency water from the ECCS tanks might just have saved the day, by suppressing the reactivity void coefficient. " (Medvedev, p. 47).

THE TEST BEGINS: April 25, 1986:

Once the test began, things began to go wrong. Present in the control

room at the time were Dyatlov, the deputy chief engineer for operations, Akimov and Toptunov, operators who had just come on the shift, and Tregub, the foreman from the previous shift.

As the test began, the local automatic control system (LAR) was switched off. Toptunov was then unable to keep the reactor power at 1,500 megawatts and it fell to 30 megawatts.

> "...At such a low power level, the reactor begins to be intensively poisoned by products of decay such as xenon and iodine. It becomes difficult or even impossible to restore the parameters. All of this meant that the inertial rundown experiment had to be halted. This was clearly understood by all the nuclear operators, including the senior reactor control engineer, Toptunov and the shift foreman, Akimov, and even by Dyatlov" (Medevedev, p. 54).

Dyatlov began cursing at the operators, blaming them for the reactor poisoning that was occuring. At this point, he had two options: increasing the power immediately, or waiting twenty-four hours for the poisons to dissipate. However, Dyatlov was unwilling to wait (the safe option) and ran about the control room ranting and raving.

Toptunov and Akimov were now in a bind. Before falling to low levels, the reactor had been operating at 50 percent of its rated power.

> "It was still possible to restore the parameters. The safety rules prohibited an increase of power if it had fallen from 80 percent...because in such circumstances the reactor becomes poisoned more quickly. But these figures--50 percent and 80 percent--were painfully close...Therefore, Toptunov made the only correct decision. 'I'm not going to raise the power! he said firmly.'" (Medvedev, p. 55).

Akimov supported Toptunov's decision, but Dyatlov did not agree. He

shouted at Toptunov, telling him that increasing power was within the rules, and that if Toptunov did not do it, that Tregub (the foreman from the previous shift) would do it. Toptunov, an inexperienced twenty-six year old, was intimidated. Later, he recounted his thoughts at the moment he made his decision:

> "The operational reactivity reserve is twenty-eight rods. In order to offset the poisoning, we're going to have to remove five to seven rods from the reserve group. I might cause a power surge, but if I don't do what I'm told, I'll be fired." (Medvedev, p. 55).
>
> (Unfortunately, his punishment was worse than being fired, he later died of radiation poisoning).

Medvedev maintains that Toptunov and Akimov as well as the operators on preceding shifts "failed to show the proper sense of responsibility and blithely proceeded to commit serious breaches of the nuclear safety regulations." (Medvedev, p. 57) He says that they were concerned mainly with finishing the tests as quickly as possible and were particularly careless in controlling the reactor. He cites eight serious violations that were either written into the program (test) or were commited during the preparation and conduct of the tests:

"

> * In an attempt to climb out of the "iodine well", the operational reactivity reserve was reduced to below the permissible level,...making useless the reactor's AZ or emergency power reduction system.
>
> * The LAR was erroneously switched off, thus reducing the power of the reactor to below the level prescribed in the program; the reactor became difficult to control.
>
> * All eight main circulation pumps were connected to the reactor, with discharge levels on some of them at excessively high emergency levels; as a result, the coolant was close to saturation temperature (this was

done in keeping with the program).

* For the purpose of repeating the experiment without electrical current, the reactor protection systems relying on the shutdown signal from two turbogenerators were neutralized.

* The protection systems triggered by preset water levels and steam pressure in the drum-separators were blocked, in an attempt to proceed with the test despite the unstable condition of the reactor; the reactor protection system based on heat parameters was cut off.

* The MPA protection system, for the maximum design-basis accident, was switched off, in an attempt to avoid spurious triggering of the ECCS during the test, thereby making it impossible to limit the scope of the probable accident.

* Both emergency diesel-generators were blocked, together with the operating and start-up standby transformers, thus disconnecting the unit from the grid; though intended to ensure a 'pure experiment' this actually completed the chain of conditions necessary for an extreme nuclear disaster." (Medvedev, p. 58).

As the test program continued, warning signs began to appear to the operators. Medvedev maintains that there were several key points in time along the way at which the experiment could have been scraped, the reactor manually shut down and disaster averted. The last of these chances occured just one and one-half minutes before the explosion.

However, that chance was not taken and the experiments were begun. About 20 seconds before the reactor blew up, Akimov, realizing that disaster was imminent, pressed the emergency AZ button. This button causes all the control rods to drop into the core and stop the nuclear reactor instantaneously. The AZ button is to be used only in case of the most extreme emergency. However, in this case, the rods did not drop into the reactor fast enough (they

take about 20 seconds to fall into place in the RBMK reactor versus as little as 1 second in a similar Canadian designed reactor). The rods froze into place as the reactor blew up. Highly radioactive chunks of graphite from the core were hurled into the area surrounding the plant and the plant itself caught on fire.

THE DENIAL:

After the plant blew up, the officials in the plant immediately began to deny the extent of the damage that had been suffered. Dyatlov, for one, kept insisting that the reactor was intact, despite touring the central turbine hall and seeing graphite and fuel rods on the ground and feeling the intense radiation (so intense that their instruments could not measure it). Akimov and Toptunov were also "utterly unwilling to believe that the reactor was no more" (Medvedev, p. 117).

Based on these assumptions, Bryukhanov and Fomin reported to Moscow that the reactor was intact. It was only several days later, when officials from Moscow arrived and the plant was surveyed from the air, did they realize that the core had blown up. In the meantime, the evacuation of nearby villages was delayed causing needless radiation exposure to thousands of people.

REACTOR DESIGN AND RISK PERCEPTION:

Finally, some comments about the reactor design are appropriate here. The reactor, as noted before, was a graphite reactor known as the RBMK type. In general, these types of reactors are considered by nuclear experts in the West to be more dangerous than pressurized water reactors (the most commonly used

design), (see Hamman & Parrott, p. 113 for technical details). According to Medvedev (p. 62), this type of reactor design was chosen because of assertions by some academicians that it was the safest and most economical. Protests by Medvedev and others went ignored.

Furthermore, the Soviets were not at all concerned with dispersing the risk posed by nuclear plants by siting them at large distances. Rather, the plans for the Chernobyl site involved ultimately the building of 12 nuclear reactors, thus concentrating the risk. (In the explosion of the No. 4 reactor, it was only truly heroic efforts of the firefighters that prevented the fire from spreading to the No. 3 reactor and possibly to No. 1 and 2 as well).

Finally, the containment vessel on the plant was flimsy by Western standards. The Chernobyl plant did not have the huge concrete domed structure that we see covering all of the nuclear plants in the United States. However, it must be admitted that the explosion at Chernobyl was of such a magnitude that it is not known whether a domed containment vessel would have mitigated the situation at all.

SUMMARY AND ANALYSIS:

There are obviously numerous factors that contributed directly to the disaster at Chernobyl. Below, I will try to compress and summarize those factors into several key points:

* Testing and drills should be part of accident prevention. In this case the testing procedure caused the accident.

* The reward system was politically based rather than meritorious. Engineers with no training in nuclear science populated the Soviet nuclear industry from the plant level to the very top.

* The standards for operating the plants were considerably below those of plants in the West. The RBMK type reactor in particular was considered too dangerous by Western designers. (Hamman & Parrott, p. 114).

* The risk factors involved in building plants, operating plants and in the final test of the Chernobyl plant seem to have been largely ignored by virtually everyone except a few nuclear scientists who occasionally spoke up. Ignorance of risk was compounded by the "tradition of silence" about accidents that took place in the Soviet Union and other places.

* The command and control system appears to have been highly deficient. For example, at a fateful moment, Teptunov's decision not to proceed with the experiment was overruled by Dyatlov. This violated Roberts' rule for migrating decision making--Teptunov had the most expertise to make the decision at the moment and could have averted the tragedy.

3.3 Exxon Valdez

On Friday morning, March 24, 1989 at 12:04 a.m. the Exxon Valdez grounded on Bligh Reef inside the Prince William Sound, an area of pristine beauty and delicate ecological makeup. The tanker ended up spilling about 240,000 barrels of oil into the ocean. However, the spill could have been worse; 1,000,000 additional barrels were on board the ship and were later off-loaded in mid-ocean.

The grounding and spillage of the oil were only the beginning of the catastrophic disaster, as I will explain here. The disaster was really a compound one; the first part (Part A) involved the grounding, and the second

part (Part B) involved the inability of many organizational "actors" in the catastrophe to act in ways which would have lessened the severity of the spill's impact.

THE PLAYERS, Part A:

Hazelwood: Captain Hazelwood and other crew members of the tanker Valdez were important, but not the only characters involved in the first phase (Part A) of the disaster. However, Captain Hazelwood bears most of the responsibility for the grounding because he was the commander of the ship. It will never be known whether or not Hazelwood was legally drunk when the ship went aground, however it is known that he had been drinking that night prior to boarding the vessel. Moreover,

> "...at the time of the accident Hazelwood's driver's license had been invalid, revoked as a result of a drunk-driving incident the previous Fall. In all, the license had been suspended for drunk-driving violations three times since 1984.
>
> One piece of the accident puzzle had to do with the renewal of Hazelwood's master's certification. Why had the Coast Guard made the renewal without checking Hazelwood's motor vehicle driving record for driving-while-intoxicated citations? Exxon... was well aware of Hazelwood's past drinking problem. In April 1985, Captain Hazelwood had voluntarily entered a private alcohol treatment program." (Davidson, p. 67-68).

The Coast Guard: Inadequate radar coverage was also a factor that probably contributed to the disaster. On the night of the accident the radar trackers at the Coast Guard Station had trouble tracking the Valdez as it reached Bligh Reef.

In 1981, James Woodle, Coast Guard commander at the time, recommended that the radar system be improved. He wanted much better coverage between Bligh Island and the edge of the Columbia Glacier (which dumped big chunks of ice into the water that were dangerous to ships). The Coast Guard felt that the additional radar station sites were "cost prohibitive" (Davidson, p. 12) at $100,000 per year. Even worse,

> "...Commander Steve McCall who took over as the Coast Guard's ranking officer in Valdez favored a downgraded system. 'It's been twelve years since the tankers began operating, and nothing major has gone wrong,' McCall commented....'We started downgrading in 1984...We changed the radars in '82 and made manpower cuts... How much do you really need to watch a ship that is going in and out, all by itself with nobody around it?'" (Davidson, p. 12)

Furthermore, at the time of the grounding, tanker crews believed that the Coast Guard plotted their progress at six-minute intervals out to Bligh Reef, since this was a requirement of the Coast Guard manuals. However, " The Coast Guard had stopped plotting vessels as far as Bligh Reef without informing the tanker crews" (Davidson, p. 74). Had the course of the Exxon Valdez been plotted on March 23, the radar man in Valdez could have provided a warning prior to the grounding on the reef. Furthermore, as Davidson tells us,

> "Since the quality of radar coverage used to track tankers varies with weather conditions a Coast Guard directive had been issued earlier to improve radar coverage. At the time of the accident, the equipment necessary to make this radar improvement had been sitting in Valdez for more than a year and a half without being used. No one had bothered putting it into operation." (Davidson, p. 74)

Another potential hazard created by the Coast Guard involved harbor

pilotage requirements for the tankers. Federal statute required that when tankers were moving between the open sea and a port they had to be commanded by someone with a "pilotage endorsement" (Davidson, p. 72). Ship's officers often lacked this endorsement, so harbor pilots were used.

> "When the tankers first came to Prince William Sound, these pilotage regulations were active between Hinchinbrook Island (very far south of where the accident occured) and the port of Valdez. However, pilot boats that return harbor pilots to Valdez struggled on the rough seas, especially in winter...One pilot boat sank; its crew narrowly escaped.
>
> In such cases, the Valdez Coast Guard might either have required tankers to hold offshore until weather conditions improved or required oil companies to upgrade the pilotage certification of their crews. Instead the Coast Guard acquiesced to reductions of pilotage requirements in the sound...Beginning in 1986, the Coast Guard issued a series of temporary and conditional directives that made pilotage requirements so complicated that at the time of the accident many people were uncertain as to just what those requirements were." (Davidson, p. 72).

THE ACCIDENT, Part A:

At 9:12 p.m. on March 23, 1989, the Exxon Valdez departed from Valdez Harbor. On the bridge were harbor pilot Ed Murphy and Captain Hazelwood. Murphy smelled alcohol on Hazelwood's breath but said nothing. Monitoring of alcohol use or abuse by crew members of the tankers appears to have been minimal.

> "According to Ed Kiml, head of security at the Alyeska terminal, tanker crew members who have been drinking can pass through security 'as long as they've got their faculties to walk and get back on the ship'" (Davidson, p. 68).

At 11:20 p.m. on March 23, 1989, after guiding the ship through the Valdez Narrows to Rocky Point, the harbor pilot handed control of the Valdez

over Captain Joseph Hazelwood. As the ship proceeded through the Prince William Sound, Hazelwood and Third Mate Gregory Cousins noted an extensive ice floe about two miles dead ahead. They had several choices:

> "They could wait until the ice moved or reduce speed and work their way through the ice. Captain Hazelwood chose another option: turn and enter the gap between the ice and the reef. The ship was still accelerating.
>
> Hazelwood ordered the helmsman to alter their course...A well timed right turn would be necessary to avoid Bligh Reef which lay six miles ahead ...There would be little room for error. The vessel needed at least six-tenths of a mile to make the turn and the gap between the ice and Bligh Reef was only nine-tenths of a mile wide. The tanker itself was nearly two-tenths of a mile long." (Davidson, p. 15-16).

Hazelwood then gave two last orders to the helmsman--to increase speed and to put the vessel on automatic pilot. Both orders were unusual given the dangerous conditions up ahead. Hazelwood then left the bridge, leaving Third Mate Cousins in charge. This was in violation of Coast Guard policy requiring two oficers to be on the bridge in the presence of danger.

Cousins noticed that the automatic pilot was on, and shifted the vessel back to manual mode. However, he did not slow down the vessel. As he watched the radar, concentrating on the ice, he may have lost track of time. In any event, he did not start his turn on time. As he began to realize his error, he ordered a hard right, but it was too late; the ship shuddered with impact and then ground to a halt on Bligh Reef. (Davidson, p. 17).

THE PLAYERS, Part B:

Part B refers to the clean-up efforts after the tanker hit the reef.

Roughly 240,000 barrels of oil were spilled out into the sound. The players involved in the cleanup include Alyeska (the oil company consortium), Exxon (represented by executive Frank Iarossi), the Coast Guard, and the State of Alaska (Department of Environmental Conservation or "DEC").

Alyeska: Alyeska was a consortium formed by seven oil companies to build the Trans-Alaska Pipeline. British Petroleum had a 50.01 percent share, Exxon and ARCO each had about 20 percent and Mobil, Amerada Hess, Unocal and Phillips Petroleum had minor shares. In order to obtain the permit in 1973 to build the pipeline, Alyeska had agreed with the United States federal government that it would take responsibility for any and all spills associated with tanker operations at Valdez. A contingency plan for spills was drawn up that was:

> "a document that spelled out precisely how Alyeska would respond to a spill: the oil spill equipment that would be available, the names and backgrounds of cleanup personnel, response times, lists of subcontractors and so on. In an attempt to eliminate confusion, the pipeline permit called for one plan to cover all Alyeska's parent companies". (Davidson, p. 81).

Very early on, there were serious doubts expressed that Alyeska would be able to contain and effectively clean up a medium or large-sized spill. Former Coast Guard commander Woodle became Alyeska's marine superintendent and resigned in 1984, warning of:

> "reductions in manning, age of equipment, limited training opportunities, and lack of experienced coordination personnel...efforts to cut cost have limited purchase of new oil spill recovery equipment". (Davidson, p. 86)

State inspectors were also dissatisfied with Alyeska's severe personnel cuts and also questionned the reliability of the cleanup equipment. Then, in 1986, at the insistence of Alaska's DEC, Alyeska finally provided a contingency plan involving a scenario for a 200,000 barrel spill. But, in doing so, it protested that such a spill would "happen only once in 241 years", (Davidson, p. 87).

Exxon: Exxon Shipping was not as confident as Alyeska about the ability of the consortium to respond to a spill. According to their representative, Frank Iarossi, Exxon had alway wanted more spill equipment in Valdez.

> "'We specifically asked that dispersant-spraying equipment be stationed in Alaska, that prior dispersant application arrangements be made with C-130s in Alaska, and that there be bigger barges for unloading skimmers. Our last official plea was made on September of 1987. I don't know which companies voted against our request. But to get to the scene of this spill and not have that equipment was a real bitter pill'". (Davidson, p. 88)

> "Although Alyeska guards the secrey of votes within its owners committee, it is clear the British Petroleum with 50.01 percent ownership and a controlling vote, vetoed the purchase of the much-needed oil spill equipment". (Davidson, p. 88)

Exxon's concern about Alyeska's ability to respond was also reflected in a letter it sent to the Alaska DEC in 1982 stating that in the event of a major spill by an Exxon vessel that Exxon's oil response team would be activated.

The Coast Guard: The Coast Guard's authority after the spill was limited, although advisory services were provided. The Coast Guard could do

little because:

> "...Under both state and federal law, a spiller has the right to initiate a spill response, to clean up its mess. The government is not allowed to intervene unless the spiller either refuses to take responsibility or its response is obviously inadequate". (Davidson, p. 58).

The DEC: The DEC was the Alaska state agency charged with monitoring Alyeska. However, despite huge state revenue from the oil industry, the DEC was severely lacking in funds and personnel.

Its ability to regulate Alyeska and the oil companies during simple daily operations was severely restricted. The oil companies consistently spilled oil in the port and dumped oily ballast water into the bay. With respect to making sure that Alyeska was prepared to deal with a major spill, the DEC also appears to have been highly deficient,

> "A review of DEC files and Alyeska's track record reveals an overall pattern of denial marked by both the oil industry's tight-fisted resistance to making good on its promises and the state's lack of perseverance in requiring it to do so", (Davidson, p. 86).

COORDINATING THE CLEANUP, Part B:

The story of the cleanup is just as much a part of the disaster as was the initial grounding of the tanker on Bligh Reef. Most of the problem was that there were multiple parties involved, all fighting over jurisdictions and precious hours and days were lost in the meantime.

In the first few hours after the spill, Alyeska attempted to put its oil recovery equipment into the water. However, when workers arrived at the dock, they found the barge in dry-dock. The necessary large skimmers and

deep-sea boom were buried under tons of equipment. A forklift and a crane were required to sort the skimmers and sections of boom and load them onto the barge. As a result, precious hours were lost before any equipment reached the spill out on the reef.

It is relatively clear now that the most expedient way of dealing with the spill would have been the spraying of dispersants and the use of controlled burning. Both of these options were available during the first 72 hours after the spill because of calm weather conditions; after that a severe storm came in and those options disappeared.

However, neither option was used because of fighting for jurisdiction among the parties. As soon as Exxon declared that it would assume responsibility for the spill, Alyeska quietly faded away (despite the State's insistence that Alyeska still needed to be held accountable). Exxon wanted to implement controlled burning and dispersant spraying immediately (even though they were faced with certain limitations, such as insufficient quantities of dispersant on hand, etc). However, Exxon was prohibited from doing so by the Coast Guard and the DEC. Both agencies feared the effects of pollution from the burning and the dispersants (which had not been tried on a spill this large), not realizing that the effects of not treating the oil (even if it caused pollution) were far worse than allowing it to remain untreated. Thus, Exxon was largely limited in the first 72 hours to using booms and skimmers owned by Alyeska.

As the days and hours passed, it became increasingly evident that

Exxon's ability to handle the spill on its own was being hampered by many things including jurisdictional conflicts. Eventually, both the state and Exxon called upon the Coast Guard to federalize the spill. However, the Coast Guard refused to do so, and clean up efforts continued to be disorganized and haphazard in the weeks and months to come.

SUMMARY AND ANALYSIS:

PART A:

* The screening methods used by Exxon or the Coast Guard in detecting substance abuse on the part of crew members, especially captains, were inadequate.

* Inadequate radar coverage existed for two reasons: (1) The Coast Guard decided not to build additional radar stations and instead downgraded its radar operations, while denying that tanker operations in the sound were risky, and (2) the Coast Guard had failed to install the new equipment that was already on hand designed to improve radar coverage.

* At the time of the grounding, the Coast Guard had was no longer plotting vessels as far out as Bligh Reef. However, the tanker crews did not know this.

* The Coast Guard had eased up on harbor pilotage requirements, requiring ships to be piloted only through the Valdez Narrows. This was despite relatively dangerous conditions in the Prince William Sound all the way to Hinchinbrook Island.

PART B:

* Alyeska had established an unrealistic contingency plan for containing oil spills. Moreover, it refused to purchase modern equipment and take seriously the probability of a spill. In its 200,000 barrel scenario, it claimed that such a spill had a probability of only once in every 241 years.

* Alyeska was concerned only with keeping costs to a minimum and not with protecting the environment or complying with the contingency plan.

* The DEC was completely unable to monitor Alyeska and make it conform to the contingency plan. Operations at Valdez involved small spills daily and Alyeska behaved with impunity.

* Exxon was prevented from using dispersants and controlled burning during the critical first 72 hours. This was because there were major jurisdictional disputes that continued through the cleanup efforts.

3.4 Bhopal

At about 12:40 a.m. on December 3, 1984, at the Union Carbide plant in Bhopal, India a tank of methyl isocyante gas (MIC) ruptured. The gas escaped into the nearby residential slum area killing and injuring people and animals. Roughly 3,000 people died within a week after the incident and about 300,000 others were affected by exposure to the gas (Shrivastava, p. 12).

THE PLAYERS:

Union Carbide and UCIL: The Bhopal chemical plant was owned by Union Carbide India Ltd. (UCIL). That company was in turn owned just over fifty percent by Union Carbide Corp. and it also had about 24,000 individual shareholders. (Shrivastava, p. 44).

UCIL was primarily a company that manufactured and sold electric batteries. However, over time it diversifed and sought out new markets. In the 1960s, it entered into chemical and pesticide production. In the late 1970's and early 1980's, competition in the pesticide industry increased for a number of reasons. During this time UCIL decided to backward integrate and manufacture MIC, (a key component of some pesticides) domestically instead of importing it from the parent company. This move would save money.

In 1979, the company expanded the Bhopal plant so that it could manufacture five pesticide components including MIC. However, this made the plant one which was much more potentially dangerous than before due to the toxicity of the chemicals and the special conditions under which they had to be handled.

It is also important to note that UCIL was small relative to Union Carbide, "it represented less than 2 percent of the parent company's worldwide sales and less than 3 percent of its profits" (Shrivastava, p. 59).

The Bhopal plant: The Bhopal plant had operated below 40-percent capacity for several years and was part of the money losing Agricultural Products Division at UCIL. At the time of the accident, the plant was for sale.

Low employee morale and lack of regard for safety permeated the plant:

> "...basic rules were being ignored. For example, maintenance workers were signing permits they could not read and leaving particular work tasks without signing off. Employees were working in prohibited areas without the premits required by plant rules. And the fire-watch attendant was sometimes called away to perform other duties.
>
> ...In this environment, unsafe practices and decisions involving breaches of policy were common. Several of these contributed to the accident including the following:
> 1. the number of operators manning the MIC unit was cut in half between 1980 and 1984. ....
> 2. Operators had inadequate safety training. ...
> 3. Managers and plant workers had little information on the hazard potential of the plant and there were no emergency plans. ....
> 4. When storage tank E610 (the one that eventually ruptured) failed to pressurize on October 21, 1984, managers did not investigate causes of the failure.
> 5. Operators failed to put in the slip blind to prevent water from entering the storage tank during the flushing operation (the chemical

reaction between the water and the MIC contributed to the explosion later). (Shrivastava, p. 57-58)

Another problem at the plant was lack of management continuity. In the last fifteen years prior to the accident, there were eight different managers. "Many of them came from nonchemical-industry backgrounds and had little or no experience in dealing with hazardous technologies" (Shrivastava p. 60) This compounded the problems of running the plant because all policies and procedures at the Bhopal plant covering everything from safety to maintenance had to be adapted from the parent company's documents. Day-to-day management was left in the hands of these usually unqualified local managers.

However, the parent company did attempt to cover itself by conducting periodic operational safety surveys in which staff from the parent company conducted a safety audit. The last survey of the Bhopal plant prior to the accident was in May of 1982. The survey team identified ten areas of major concern and ordered them corrected by the local manager. According to Shrivastava, five of these problems eventually contributed to the accident:

1. The potential for release of toxic materials in the phosgene/MIC unit and storage areas because of equipment failure, operating problems, or maintenance problems.
2. A lack of fixed water-spray protection in several areas of the plant.
3. The potential for contamination, excess pressure, or overfilling of the MIC storage tank.
4. Deficiencies in safety valves and instrument maintenance programs.
5. Problems created by high personnel turnover at the plant, particularly in operations.

Local management did try to deal with these problems and developed an

action plan to solve some. However, most of the problems were chronic, needing continuous monitoring. "Descriptions of the physically rundown condition of the plant at the time of the accident suggests that these chronic problems still existed" (Shrivastava, p. 61).

Finally, risk perception in general seems to have been incredibly low at all levels of the organizaton, as underscored by Shrivastava's comments:

> "The plant had no contingency plans for dealing with major accidents. The need for such plans was not identified, either by the local mangement or by the experts from headquarters who conducted the periodic operation safety surveys. This, in turn, contributed to the general lack of understanding, both in the plant, and in the community, about the lethal nature of MIC."

Governmental Authorities: Governmental authorities at various levels contributed to the disaster. When the plan for backward integration was proposed, the municipal authorities in Bhopal objected because the plant's location was not well suited for the production of hazardous chemicals. However, due to UCIL's influence as a powerful company in India, the central and state government authorities overruled the objections of the city.

Moreover, Shrivastava (p. 39) maintains that safety inspections on the part of the Department of the Environment were cursory, if they were done at all. In 1983, the annual budget for the Department, covering all of India, was only $650,000.

The city authorities also contributed to the disaster. By 1984, two slum colonies of squatters in mud huts were located across the road from the plant.

Hoping to improve slum conditions, the city granted ownership rights to each family on the land where they were living (up to 500 square feet). Thus, the city made permanent a group of residents that would ultimately lie directly in harm's way, despite knowledge of the hazardous nature of the plant.

THE ACCIDENT:

MIC is a highly toxic chemical used in making the pesticide Sevin. It is very unstable and must be kept at low temperatures. UCIL manufactured it in small batches, keeping it in underground tanks until needed for processing. (Shrivastava, p. 50).

The plant had several safety features:

> "The vent-gas scrubber was a safety device designed to neutralize toxic exhausts from the MIC plant and the storage system...The gases could also be routed directly to the flare without going through the scrubber...However the flare was not designed to handle large quantities of MIC vapors. A few weeks before the accident the scrubber was turned off to a standby position.
>
> Two additional features of the plant were relevant... The first was a refrigeration system used to keep MIC at low temperatures, particularly in the summer...However, the refrigeration system was shut down in June of 1984 and its coolant drained for use in another part of the plant, thus making it impossible to switch on the refrigeration system during an emergency. The second important feature was a set of water-spray pipes that could be used to control escaping gases, overheated equipment or fires." (Shrivastava, p. 53).

For about two months prior to the accident, tank E610 (the one which ruptured) was not under positive nitrogen pressure. Because of this, small amounts of contaminants such as metal impurities entered the tank through the nitrogen line (Shrivastava, p. 62). These metal impurities later acted as a

catalyst in contributing to the gas leak.

About two weeks prior to the accident, tank E610 failed to pressurize; managers failed to investigate the causes for this failure and allowed the tank to store MIC without positive pressure.

> "This permitted small quantities of water and contaminants to react with MIC and form trimer (a plastic substance in the pipe lines. It was this trimer buildup that necessitated the flushing of pipes on the night of December 2." (Shrivastava, p. 58).

The work crew that was manning the MIC unit had been cut from twelve to six, with the maintenance crew reduced from three to one. The maintenance supervisor position had been eliminated on the second and third shifts; this was a move that contributed directly to the accident according to Shrivastava (p. 57). This was because,

> "the maintenance supervisor was responsible for ensuring that there was adequate preparation for the pipe flushing operation, and that the slip blind was installed to prevent water from entering the tank." (Shrivastava, p. 57)

On the night of December 2, operators began flushing the tank's pipes to remove the trimer that had built up previously due to lack of pressurization in the tank for the last two weeks. However,

> "Operators failed to put in the slip blind to prevent water from entering the storage tank during the flushing operation. When no water was coming out the other end of the pipe, the production supervisor ordered the worker who was washing the pipes to resume the flushing operation and did not investigate where the water was going. This supervisor had been transferred to his job just one month before from a UCIL battery plant and had little experience in MIC technology and little knowledge of hazards in this plant." (Shrivastava, p. 58).

When the water entered the tank, it reacted with the MIC that had been contaminated with metallic impurities. This caused the temperature and pressure in the storage tank to rise rapidly. The temperature rise could not be controlled because the refrigeration system had been shut off.

As the toxic gases began to escape from the ruptured tank, they could not be neutralized. The scrubber failed to work because it was designed to deal with gases only, not a mixture of liquid and gases. The flare tower was down for repair, and finally the water sprinklers could not throw the water high enough to neutralize the escaping gases (Shrivastava, p. 65).

As the gas escaped, the workers at the plant realized that there was an emergency. However, inexplicably, the plant operators turned off the alarm that would have warned the neighboring community about the accident. As the gas escaped, thousands died and hundreds of thousands were seriously injured, many for life.

SUMMARY AND ANALYSIS:

* Safety monitoring and drills were inadequate or nonexistent. The previous corporate safety audit revealed fatal flaws which were not corrected.

* The plant was losing money, so the focus was on cutting staff to save money rather than on safety.

* Safety standards at the Bhopal plant were not enforced by govermental authorities; in fact those same authorities exacerbated the situation in some respects. Certainly, as revealed by the corporate audit, the Bhopal plant was allowed to operate in a way that would not have been acceptable in the U.S.

* The risk perceptions of the plant managers, personnel and Indian authorities appear to have been low with respect to operating the plant. Apparently Union Carbide did not see the plant as a significant source of risk potential either.

* At Bhopal we saw a continuous breakdown of the command and control system. Rules and procedures were systemtically broken. Many rules and procedures were not standardized but were ad hoc, being adapted from master manuals from the parent company. The personnel at the plant were often untrained in MIC production and hazardous chemical handling.

3.5 Hubble Telescope

The story of the Hubble Telescope fiasco is not terribly complex. It involves funding problems, managment problems, intense time pressures, and simple, but highly significant, errors that had numerous opportunities to be caught but which were not.

The Players:

Perkin-Elmer was the contractor on the project. It significantly under-bid the project, bidding well below the price of its rival Eastman-Kodak. In fact, from the beginning, the company "was operating without any flexibility because (it) had underbid the telescope contract" (Capers & Lipton, p. 43). Perkin-Elmer bid the job at $70 million which was $35.5 million less than Kodak. However, in Kodak's bid was a proposal to build two main mirrors using different equipment, test each mirror with the instruments used to make the other and choose the better of the two for the telescope. (Such a procedure would have undoubtedly prevented the Hubble disaster, as we will see). "Kodak also proposed testing the telescope's main mirror and its smaller

secondary mirror before launch. Perkin Elmer proposed no such testing" (Capers & Lipton, p. 43).

Supposedly, Perkin-Elmer and NASA both knew that the telescope was being underbid (Capers & Lipton, p. 43). Essentially, NASA reassured Perkin-Elmer that once the project was underway, the company could demand more money for "unforseen" technical changes. "Yet by the time work began on the space telescope, Congress no longer was willing to give NASA extra money. In turn, the space agency's top managers became unsympathetic to Perkin-Elmer's pleas, threatening to cancel the project if it didn't stay within budget." (Capers & Lipton, p. 43).

Bud Rigby was the manager in charge of grinding the mirror. He was under intense pressure. Because of an unrealistic NASA schedule, when the mirror arrived at the Danbury plant where the fine polishing would take place, things were already nine months behind schedule, "and the hard stuff hadn't even begun". (Capers & Lipton, p. 43.). And, Rigby was well aware that any delays in finishing the mirror would escalate the cost of the whole NASA project since it would create a bottleneck affecting thousands of employees in dozens of companies all building parts of the space telescope.

Wilhelm Geissler was the the master optician on the project. Unlike the "Old World" opticians in the industry, Geissler had full faith in the computers to tell him exactly how to polish the mirror. One morning, however,

"Geissler punched the wrong numbers into the computer, hitting "1.0"

> instead of "0.1" To everyone's horror, the whirring polishing tool began digging a groove near the inside edge of the mirror. It could have been much worse. A technician watched the mirror constantly during the hours it was polished, keeping his finger on a kill switch...the technician on duty acted instantly when the polishing tool ran amok. The motor cut off, preventing the arm from leaving a deep scar. The groove was smoothed over somewhat in later polishing runs, but Geissler's mark would never go away completely." (Capers and Lipton, p. 44)

Lucian Montagnino, was responsible for seeing that the retooling of the null corrector was done right. The null corrector was an instrument that was to be used continuously through the grinding process to measure the surface smoothness of the mirror to within a few millionths of an inch.

Roderic Scott, was a consultant who had retired from the company but had been brought back in to work on the telescope project. Scott was an optical designer whose job was to function as a trouble shooter (Capers & Lipton, p. 46).

Senior Management: In the 1980's the organization converted to matrix management. Prior to that, scientists would form task forces to work on contracts. Now, under the new regime,

> "managers decided who worked on what, shifting employees from job to job, depending on which project had the most pressing schedule problem or the most commercial promise. In effect, people now had two bosses. Many of those working on the Hubble mirror, for example, were employed by the Optical Operations division, but they reported to Bud Rigby, who was in the Electro-Optical division. And Rigby reported on the mirror to the director of yet another division, Optical Technology." (Capers & Lipton, p. 48).

WHAT WENT WRONG:

While numerous factors contributed to the Hubble fiasco, the single most

important factor was the improper assembly of the null corrector (the precise measurement instrument). This mistake indeed provided the fatal flaw.

The null corrector, costing about $1 million, was designed by Abe Offner, who was not consulted during the assembly operation. The crew assembling the null corrector reported to Montagnino. They were under intense time pressures.

> "They had only a few days left for the final adjustment: the distance between the lower of the mirrors and the lens. Special rods had been manufactured to measure the spaces (made of Invar a material that doesn't expand or contract with temperature changes)...They had been measured and cut, then shipped to an independent laboratory that certified their lengths. Because an error of even the width of a human hair would make the mirror the wrong shape, a special microscope and laser were used to make the measurements. And the harried technicians made a mistake. To set the distance between the lens and the mirror the technicians eased a measuring rod into place and looked through the microscope at the end of the rod. They had to bounce the laser beam precisely off the tip, through a hole in a tiny cap on the rod. The cap was coated with special paint so there would be no reflection unless the laser were aimed at the right spot. But one little spot of paint had worn off. Unknown to the technicians, the laser was set to bounce off that worn spot." (Capers & Lipton, p. 45).

Unfortunately, because the technicians were so rushed, they failed to recognize the problem. When they tried to set the lens for the null corrector where the laser said to put it, something was obviously wrong.

> "The way the null corrector was built, the lens wouldn't go down far enough without adding something to the bracket that held the lens in place. Under normal circumstances, this design anomaly might have triggered an engineering inquiry; but the deadline was upon them. There was no time for an inquiry. There wasn't even time to ask the machine shop to custom-make spacers for the bracket. The technicians grabbed three household washers, the kind you could find in any hardware store for twenty cents. They flattened the washers and put them into the $1

> million null correcter. The technicians moved the lens 1.3 millimeters lower than it was supposed to go." (Capers & Lipton, p. 45).

After the null corrector was assembled, it was placed atop the measuring tower, where it was "handled like the crown jewels" (Capers & Lipton, p. 46). Over the next 11 months, Rigby and his crew would rely

> "entirely on the null corrector to tell them whether the mirror was getting closer to the desired shape. It was as if they were cutting and measuring with a thirteen-inch ruler they thought was a foot long" (Capers & Lipton, p. 45).

Although the flaw in the null corrector was fundamental to the ultimate telescope fiasco, there were opportunities to discover that a flaw existed; those oppportunities were bypassed for numerous reasons (not unlike the Chernobyl disaster). Scott, the consultant on the project kept urging Montagnino to buy "fire insurance" by getting an independent test of the mirror. In fact, he recommended that they use Kodak's null corrector for such a test, but was branded a "traitor" because Kodak was the competition.

Then, as the grinding proceeded, evidence of an abberation appeared. "Measurements had been made from a second, much less accurate null corrector that had been brought in for another purpose" (Capers & Lipton, p. 51). The measurements from the second null corrector showed that there was a shaping error. Slomba, the engineer who noticed the abberations reported them promptly to Montagnino. However, Montagnino argued that the second device had to be wrong--he had complete confidence in the original null corrector (not knowing of course that it had been assembled incorrectly).

On May 21, 1981, the company missed yet another opportunity to discover the flaw in the mirror. A group of scientists met and discussed the project.

> "They issued a memorandum urging a number of final actions. Number three on the list of five said an independent test of some kind should be performed on the mirror.
>
> ....In any case, the consensus among company officials was that there was no need for such a test," (Capers & Lipton, p. 53-54)

Finally, the mirror was trucked to the Wilton plant in December of 1981, and the technicians started assembling the documents they would need for a final review of the project.

> "Then they were told to stop. Perkin-Elmer was shutting their project down. ....The orders came from Kent H. Meserve, the project manager... To Meserve, it was just one more demand for time and money he wasn't able to fulflll; and in this case it didn't seem necessary...'we did not have the funding. We needed their talents on something else'.
>
> ...Rigby also fought for the final review....(and) 'It was just common sense to conduct a review' Montagnino says, 'like checking your parachute before jumping out of an airplane.'" (Capers & Lipton, p. 54-55)

However, had the review been complete it is almost certain that the error in the mirror would have been identified before it was placed into the telescope and sent into space. Of course, once in place in the telescope and launched into space the cost of correcting the error became magnified many times over.

SUMMARY AND ANALYSIS:

* It is clear that one of the most important factors in the Hubble failure was the lack of double checking or "process auditing" as the mirror was

being ground. Several opportunities for discovering the flaw were missed. When flaws were discovered they were dismissed as being due to flaws in the additional equipment being used to test the mirror; complete faith was placed in the original null corrector.

* The project was underbid and underfunded from the start. By the time the grinding started, the project was nine months behind schedule. Perkin-Elmer was unable to obtain additional funds from Congress to cover its costs, and therefore began to cut corners on the project in an attempt to trim its losses. Quality assurance became a secondary consideration.

* The initial design for the project was of a lower cost than its competitor, Eastman Kodak, but the design also had no tolerance for error built in.

* The company appears to have had a low risk perception: Montagnino refused to buy the "fire insurance" suggested by Scott by getting an independent test of the mirror; the senior management of the company refused to allow the final review of the mirror (which should have revealed the error prior to it being installed in the multi-million dollar telescope).

* The command and control system at the company appears to have been flawed. The matrix management system impaired critical communications about possible flaws that were showing up in the mirror. It also complicated reporting authorities, with many personnel reporting to two bosses.

3.6 Space Shuttle Challenger

The Space Shuttle Challenger disaster was not only a disaster for NASA, but a national tragedy as well. As thousands of school children watched on television, the spacecraft carrying the first "teacher in space" and other astronauts exploded in a fiery ball shortly after liftoff from the launch pad when the O-rings in the solid rocket booster failed. All future flights of the shuttle were delayed for several years while the causes of the explosion were

determined and new safeguards were put into place (which will hopefully prevent another such disaster).

Numerous players were involved in the shuttle disaster which had a long genesis or incubation period. Although there are many parties cited in the accounts of the shuttle by Vaughan (1990) and others, I will try to focus only on the most important ones; later in this section I will describe how the interactions between these parties contributed to the ultimate failure.

THE PLAYERS:

Safety, Reliability, and Quality Assurance Program (SR&QA): This was one of two inter-organizational agencies created by NASA to assure safety by intensively scrutinizing technical design and program management. (The other agency was the Space Shuttle Crew Safety Panel). According to Vaughan, "...SR&QA bore the major responsibility for safety oversight." (p. 234). The job of SR&QA was as comprehensive as its name suggests. It published safety standards that were highly detailed and updated annually (Vaughan, 1990).

> "The SR&QA staff monitored and implemented these standards on a day-to-day basis at all NASA locations and at contractor sites....SR&QA personnel situated in contractor facilities monitored compliance with written procedures and worked closely with contractor personnel...SR&QA audit teams audited contractor activities periodically. " (Vaughan, p. 235)

With all this monitoring going on, how was it that the O-ring problem was overlooked? According to Vaughan, the NASA engineers at Marshall and the SR&QA staff at both Marshall and Morton Thiokol (the O-ring

manufacturer) were monitoring the problem (p. 235). However, Vaughan notes that the following reasons caused NASA to not consider the O-ring problem hazardous to mission safety:

> 1. Safety-critical items: Originally, the solid rocket booster joint was listed as having redundancy. However, it was later updated to a more serious category indicating that it did not have redundancy (loss of the part could cause solid rocket booster failure). This change was not properly noted in some internal NASA documents.
>
> 2. Trend data: "Beginning with the tenth mission of the shuttle in January 1984 and concluding with the twenty-fifth (the Challenger flight), more than half the missions experienced O-ring problems. This trend was not identified and analyzed by SR&QA (Vaughan, p. 235)
>
> Problem-reporting requirements:
> "...First, SR&QA did not establish and maintain clear and sufficient requirements for reporting shuttle problems up the NASA hierarchy....Second, SR&QA failed to create a concise set of requirements for reporting in-flight anomalies" (with rules often contradicting each other) ...Finally, SR&QA failed to detect violations of problem reporting requirements. Because of the problems found in the O-rings on prior flights, a launch constraint was issued to Level III managers requiring corrective action to be taken before the shuttle could fly again. However, after that was done, each time a shuttle launch approached the Level III solid rocket booster project manager simply waived the constraint, allowing the mission to proceed." (Vaughan, p. 236)

Furthermore, according to Vaughan (p 236), the Level I and Level II NASA administrators were not informed of the constraint or the subsequent waivers. This was a violation of the launch constraint reporting requirement. Additionally, Vaughan reports, the SR&QA did not discover the reporting requirement violations.

However, it must be noted that SR&QA was operating under severe

constraints of its own. After four test flights of the shuttle, NASA began reorganizing SR&QA and reducing its personnel.

> "Between 1970 and the Challenger tragedy, NASA trimmed 71 percent of its safety and quality control staff...At the time of the accident, total SR&QA personnel numbered about 500; total NASA employees were about twenty-two thousand....staff reductions made it all but impossible to adequately monitor a system as complex as NASA's" (Vaughan, p. 238)

The Space Shuttle Crew Safety Panel (SSCSP): This unit was created in 1974 by NASA to be solely responsbile for crew safety. Its mission was "(1) identifying possible hazards to shuttle crews, and (2) advising shuttle management about these hazards and their resolution" (Vaughan, p. 239). The panel of 20 people came from the Johnson, Kennedy and Marshall space centers. Unfortunately, this panel could function effectively only if it had information regarding possible hazards available to it. According to Vaughan, "Although the O-ring problem was first noted at NASA in 1977, (there is) no indication that the O-ring problem was addressed by this panel", (Vaughan, p. 240).

Another problem with the panel concerned questions about its necessity. Since the shuttle appeared to be operating successfully, the mission of the panel seemed to have disappeared. So, when the flight safety manager retired in 1981, the SSCSP simply went out of existence.

NASA's Contracting System: NASA's contracting system was designed in such a way that it encouraged contractors to focus on cost saving and meeting

deadlines instead of focusing on safety.

> "The incentive fee rewarding cost savings and timely delivery, could total as much as 14 percent of the value of the contract; the award fee, rewarding the contractor's safety record, could total a maximum of 1 percent. No provisions existed for performance penalties or flight anomaly penalities. Absent from a major mission failure which entailed a large penalty after the fact, the fee system reinforced speed and economy rather than caution". (Vaughan, p. 247)

Morton Thiokol: Morton Thiokol designed and manufactured the O-rings which were the cause of the shuttle disaster. But, Thiokol was driven by financial incentives and not by safety concerns. As the House Committee on Science and Technology reported in 1986, there was little financial incentive for a contractor to fix a problem unless such a problem was likely to cause mission failure (resulting in a huge financial penalty). Furthermore,

> "Even the possibility of contract loss appears to have reinforced production interests at Thiokol, not safety. Post-accident investigations suggest that Thiokol managers approved the launch over engineering objections because launch delay might jeopardize the company's ongoing contract negotiations to continue producing the solid rocket booster for NASA." (Vaughan, p. 248)

> "...no evidence exists that sanctions were used to gain compliance at Morton Thiokol prior to the Challenger launch. There had been more than twenty-five occurences of O-ring erosion and related SRB anomalies at the time of the accident. Thiokol had never been penalized, nor was there evidence that punishment had been threatened ...Rather at the time of the Challenger accident, Thiokol was eligible to receive a near-maximum incentive fee of approximately $75 million." (Vaughan, p. 248)

The Countdown to Disaster:

The countdown began with a phone conference between Level III management at NASA (Levels II and I are above Level III), and Morton

Thiokol. Lawrence Mulloy was the level III manager in charge. During the teleconference on January 27, Morton Thiokol recommended against the launch because of the effects that the unseasonal cold temperatures might have on the solid rocket booster O-rings. (Schwartz, 1987). The discussion became heated as a result, since NASA did not want to delay the mission; it had a lot of prestige riding on the mission which would include the famous "teacher in space" for America's schoolchildren. In addition, President Reagan was giving his "State of the Union" message on television that night and NASA wanted him to be able to comment on the successful launch. Consequently,

> "Lawrence Mulloy said that he did not accept the recommendaton (by Thiokol) and asked if Morton-Thiokol wanted him to wait until April to launch. At the same time, George Hardy, Deputy Director of Science and Engineering said he would not launch against Morton-Thiokol's recommendation, but that he was 'appalled' that they would make such a recommendation.
>
> At this point, Morton-Thiokol management asked to go off the teleconference loop while they reconsidered the recommendation. When they came back on, as the result of the processes which may be signified by Robert Lund, Vice President of Engineering, 'taking off his engineering hat and putting on his management hat', and despite the fact that there was not one engineer who recommended the launch, Morton-Thiokol had been able to change their assessment and had come to approve the launch. Even so, when they sent their written approval, the letter still brought up the engineering grounds upon which they had previously recommended against launch." (Schwartz, p. 64)

Later, Mulloy and another Level III manager mentioned to William Lucas (the Marshall Center Director) that Morton Thiokol had some concerns about the O-rings, but gave the impression that the matter had been completely resolved. During the pre-launch hours, Mulloy sat with Mr. Moore (the

Associate Administrator for Space Flight; number one in command), and with Mr. Aldrich, (National Space Transportation Program manager; number two in command), and never mentioned the discussions with Morton-Thiokol.

Thus, two key factors failed in the command and control system. Decisions were made at the wrong level (Mulloy made the decision at Level III and did not consult with supervisors). In addition, Mulloy essentially bullied Morton-Thiokol into agreeing to go along with the launch despite their reservations (not unlike the reservations of the control room operators at Chernobyl).

Furthermore, we see that this system was not tightly coupled. Thus, management was afforded plenty of opportunities to reconsider their decisions if they had utilized "migrating decision making" and left the decision up to the people most qualified to make such a decision--the engineers and the senior levels of management at NASA.

SUMMARY AND ANALYSIS:

* Anomalies in the O-rings were well known to NASA and Morton-Thiokol before the fatal Challenger mission. However, monitoring systems within NASA appear to have broken down with respect to following the problem.

* The reward system was structured so that Morton Thiokol had little incentive to fix the O-rings unless they felt that failure of the seals would cause a complete mission failure.

* The NASA quality assurance and safety system had degraded over time, particularly when compared to the Apollo program. Under the Apollo program, the mission controllers operated under the guideline "Tell me why we should fly this mission". In the Shuttle program, that

changed to "Tell me why we should not fly this mission".

* Risk perception appears to have been low and/or nonexistent. Those parties at NASA and Morton Thiokol that knew of the O-ring problems appeared to regard them as not serious--although the engineers at Thiokol did see them as serious when the launch decision was made. Other more senior parties at NASA, at Levels II and I, were not informed of the risk involved, nor was the Space Shuttle Crew Safety Panel.

* Command and Control failures were evident in the shuttle launch. Level III NASA officials asked Morton-Thiokol for agreement to launch and Thiokol initially refused. Later, the managers at Thiokol, over the protests of the engineers, gave in to aggressive arm-twisting by NASA and agreed to the launch. Additionally, Level I and II managers at NASA were never informed of the discussion with Thiokol despite an existing launch constraint regarding O-rings.

3.7 Building the Model

So far, summaries of five catastrophic failures have been presented. The intent of this section of this paper is to find similarities across those failures and use those similarities to build a model for failure based on the five cases.

In examining the five cases, I found five similarities, or factors, that seemed to have contributed to failure in all or most of the cases. The factors are defined and listed below:

1. **Process Auditing:** An established system for ongoing checks designed to spot expected as well as unexpected safety problems. Safety drills would be included in this category as would be equipment testing. Followups on problems revealed in prior audits are a critical part of this section as well.

2. **Reward System:** The reward system is the payoff that an individual or an organization gets for behaving in one way or another. In this case, we are concerned with risky behavior. As all organizational theorists know, the reward system within an organization tends to have a powerful influence on the behavior of individuals within it. Similarly, the reward system that exists interorganizationally also influences the behavior of

organizations.

3. Degradation of Quality and/or Inferior Quality:
This refers to the essential quality of the system involved as compared to a referent system that is generally regarded as the standard for quality.

4. Perception of Risk: Two elements of risk perception are involved here. (1) Whether or not there was any knowledge that risk existed at all, and (2) If there was knowledge that risk existed, the extent to which it was acknowledged appropriately or minimized.

5. Command and Control: This factor is borrowed from Roberts (1989, 1988, 1992). Roberts outlined command and control elements as separate factors, but I am combining them here and listing her separate factors as subfactors in my broader model.
The command and control elements are:

a. Migrating decision making (the person with the most expertise makes the decision).
b. Redundancy (people and/or hardware), i.e. backup systems exist.
c. Senior managers who can see the "big picture", i.e. they don't micromanage.
d. Formal rules and procedures. A definite existence of hierarchy but not necessarily bureaucracy in the negative sense.

In this next section I will show how evidence for these factors is provided from each of the case studies. Using the evidence from the cases, I will then propose formal hypotheses based on each of the factors outlined above. (Exhibit 3A summarizes the case evidence and its relationship to the factors.)

3.7.1 Process Auditing

All of the cases reviewed here show serious flaws in process auditing as I have defined it. At Chernobyl, drills and tests appear to have been done on an ad hoc basis. The accident itself was caused by a testing procedure in progress.

Exhibit 3A-- Results: Analysis of Five Cases

	Process Auditing	Reward System	Degradation of Quality	Perception of Risk	Command and Control
Challenger	O-rings had anomalies in other flights.	No incentive to fix O-rings unless failure would cause complete mission failure.	NASA quality assurance and safety system had degraded over time (compared to Apollo program).	O-ring problems not seen as serious except by a few engineers.	Low level NASA officials and managers at Thiokol made decision to launch.
Bhopal	Drills non-existent. Corp audit showed flaws which were not corrected.	Plant losing money. Focus was on cost cutting, not safety.	Machinery and equipment were deteriorating. Safety standards were lower than in U.S.	Managers and personnel in plant did not understand dangers of chemicals they were using.	Complete breakdown. No standard rules and procedures.
Hubble	Relied on single instrument to measure mirror. Never double-checked despite "warnings".	Project was underbid. Company focused on cutting costs and less on quality.	Project design had no error tolerance built in. Also, measurement instrument assembled wrong.	Sr. Manager refused to get independent measurement of mirror. Low risk perception.	Matrix management.
Chernobyl	Improper testing of unit caused accident.	Rewards were politically based rather than meritorious.	Reactor was of inferior design.	Ignorance of risk compounded by "conspiracy of silence".	Senior management not nuclear scientists.
Valdez					
Part A (Spill)	Personnel screening for substance abuse inadequate.	Coast Guard trying to cut costs.	Pilotage requirements dowgraded. Radar coverage of ships downgraded.	12 years with no accidents led to false sense of security.	Captain left bridge during critical point in time.
Part B	State unable to make Alyeska comply with spill plan.	Alyeska wanted to keep costs as low as possible.	Alyeska refused to buy more modern equipment.	Alyeska apppeared unconcerned with risk.	Intra-organizational disputes worsened impact of spill.

In the Exxon case, the Coast Guard renewed Hazelwood's master's certification without checking his driver's license record (which would have shown three suspensions for driving-while-intoxicated). Furthermore, the state of Alaska, through its inadequately funded DEC, was completely unable to monitor Alyeska and to make it conform to its contingency plan. Alyeska acted with impunity.

In the Bhopal situation, safety monitoring and drills were inadequate or nonexistent. The previous corporate safety audit revealed fatal flaws which were not corrected.

In the case of the Hubble Telescope mirror, audits were not allowed. Although somewhat inferior null correctors revealed that there might be a flaw in the mirror, one of the key project managers refused to allow the mirror to be measured by a very precise null corrector, such as the one owned by Kodak.

Finally, in the Challenger situation, there was no comprehensive system in place for following up on flight anomalies and monitoring them. And, despite a launch constraint on the O-rings requiring corrective action before the shuttle could fly (placed in April, 1985), the constraint was simply waived at Level III before each flight. Much of the responsibility for monitoring the quality and safety of shuttle components appears to have been left with the manufacturer.

Based on the similarities in the cases dicussed above, I expect:

Hypothesis 1: Risk mitigating organizations will have extensive process auditing procedures. Non-risk mitigating organizations will not have good process auditing procedures.

3.7.2 Reward System

The reward system in the Soviet nuclear power industry was based on political influence rather than technical expertise. As result, all of the "players" in the control room at the time of the accident, as well as their supervisors at the plant, were engineers with non-nuclear backgrounds. Furthermore, within the system, one was rewarded for going along with the "tradition of silence" about nuclear accidents and dangers.

In the Exxon Valdez case, the reward system was based on cost minimization. The Coast Guard, as an organization, was trying to minimize radar costs, so it downgraded its systems and also stopped plotting tanker crews. Alyeska, as an organization, (led by British Petroleum) was also trying to minimize costs, so it failed to buy more modern or larger equipment, or even properly maintain the equipment it had.

At Bhophal, the organization was also focused on cost minimization. The plant was losing money, so even safety personnel were eliminated as part of the cost cutting drive.

In the case of the Hubble telescope, Perkin-Elmer underbid the project and then was unable to receive additional funding. Cost cutting pressures became intense and caused the final review of documents (which would have revealed a flaw in the mirror) to be canceled.

Finally, in the Challenger case, the reward system for the prime contractor was set up so that it was not eocnomical to fix a problem unless the prime contractor believed that a problem would result in complete mission failure. The contract reward for cost savings and timely delivery was up to 14% contract amount; the contract reward for safety was up to 1%.

Hypothesis 2: Risk-mitigating organizations will have reward systems that encourage risk-mitigating behavior on the part of the organization and/or its members. Non-risk mitigating organizations will have reward systems that reward or promote risky behavior on the part of the organization and/or its members.

3.7.3 Degradation of Quality and/or Inferior Quality

At Chernobyl, the reactor was an RBMK type, considered to be of an inferior and much more hazardous design by experts in the West. At Valdez, the Alyeska consortium allowed its spill equipment to deteriorate and/or be stored improperly; it refused to upgrade the equipment over time. At Bhopal, the plant and equipment were literally falling apart from lack of maintainance and capital spending on the part of the parent organization. In the Hubble situation, the null corrector was accidently assembled wrong due to extreme time pressures placed on the assemblers. Finally, in the Challenger case, the quality of program administration and degree of safety concern had degraded substantially as compared to the Apollo program.

Hypothesis 3: Risk-mitigating organizations will have quality standards that meet or exceed the referrent standard of quality. Non-risk mitigating organizaions will have quality standards that do not meet the referrent quality standard.

3.7.4 Perception of Risk

At Chernobyl, there was a low perception of risk based primarily on lack of knowledge and ignorance. As noted earlier, information about nuclear accidents was suppressed through a policy known as a "tradition of silence". And many operators, including those involved in the Chernobyl accident, were not trained as nuclear scientists but as engineers in other fields; their understanding of the many risks involved in operating nuclear facilities was limited.

In the Exxon Valdez incident, there is ample evidence that the Coast Guard, in general, regarded the risk of an accident as minimal since it was downgrading its radar system and had stopped tracking ships as far as it had previously done. Furthermore, Alyeska regarded spill risks as minimal; only under protest did it provide a contingency plan to the Alaska DES for a 200,000 barrel spill.

At Bhopal, risks were not understood by plant managers or personnel because they had little or no training with regard to the hazardous chemicals being used in the plant.

In the Hubble telescope case, risk was not perceived as a result of denial on the part of one of the key project managers, Montagnino. Despite evidence that kept showing up indicating that something was amiss, Montagnino refused to obtain an independent test on the mirror.

Finally, in the Challenger incident, risk was also not "perceived" by the

organizations (NASA and Morton Thiokol) as a result of denial. Despite the arguments and protests from the Thiokol engineers, managers at Thiokol and mid-level managers at NASA decided to go ahead with the mission anyway.

Hypothesis 4: Risk mitigating organizations will correctly assess the risk associated with the given problem or situation. Non-risk mitigating organizations will not correctly assess the risk within a given problem or situation; such failure may be due to lack of knowledge about risk or mis-estimation of risk.

3.7.5 Command and Control

At Cherynobyl, the command and control system was compromised by managers who did not have nuclear power experience. Furthermore, in the actual accident, the operator who wanted to shut down the reactor was overruled by his superior (this violated migrating decision making). In addition, formal rules and procedures did not appear to exist. The accident was caused by an ad hoc test program written by the plant manager as a "pure experiment".

At Valdez, there were numerous ways in which the command and control system was dysfunctional. Alyeska, for one, refused to abide by the rules and procedures that it had agreed upon with the Alaska DEC. Once the spill happened, confusion and disagreements over which agency was in charge worsened the impact of the spill.

At Bhopal the command and control system also had numerous flaws. The plant manager could not have the "big picture" because he did not know anything about running a chemical plant. Rules and procedures were ad hoc at best, and existing rules were continuously broken.

In the case of the Hubble Telescope, decision making was diffused through a matrix management system. As a result, the managers making the decisions often didn't have the proper information.

Finally, in the Challenger incident, the command and control system broke down in two places. At Morton Thiokol, managers made the decision to launch, over-ruling the engineers who protested the launch, based on their (the engineers) expertise and knowledge. At NASA, mid-level managers approved the launch violating existing NASA rules, and without informing senior management of Morton Thiokol's reservations about the O-rings.

Hypothesis 5: (from Roberts, 1992). Risk-mitigating organizations will have a strong command and control system consisting of the four following elements:

a. Migrating Decision Making
b. Redundancy
c. Senior Management Has the "Big Picture"
d. Formal Rules and Procedures

Non-risk mitigating organizations will have command and control systems that lack some or all of the above four elements.

3.8 Integration with the Turner Model (1976, 1978)

As noted earlier in chapter two, Turner examined three "man-made" disasters for similarities in their causes. The disasters he chose were all of low technological complexity (although he does not note this as a feature of the analysis). Turner noted seven factors that contributed to the cause of each disaster. As I will show below, all but one of these factors fits into one of the categories or factors that I have outlined in my model in this chapter. Turner notes the following factors:

* Rigidities in perception and beliefs in organizational settings. (Risk perception, H4).

* The decoy problem (Risk perception/estimation, H4).

* Organizational exclusivity: disregard of non-members. (Risk perception/estimation, H4).

* Information difficulties. (Command and Control, H5).

* The involvement of 'strangers', especially on complex 'sites'. (Not included in my model, nor did I find the phenomenon appearing in the five cases studied).

* Failure to comply with regulations already in existence. (Command and Control, H5).

* Minimizing emergent danger. (Risk perception/estimation, H4).

Two of Turners factors fit under the Command and Control factor that I have identified in my model. Three of his factors fit under the risk perception factor that I have identified in my model. Thus, the Turner model, which has been largely ignored in the U.S. disaster literature, provides additional support for the model which I have constructed in this chapter.

One further note one the Turner model should be made here. It is not known why one of his factors "the involvement of strangers, especially on complex sites" emerges in his cases and not in mine. It may be simply that the cases he picks are idiosyncratic in displaying this characteristic.

3.9 Chapter Summary

This chapter has used grounded theory to build a model for catastrophic failure, using five well known cases. In looking for common factors or causes

for disaster across the cases, I was able to identify five such factors. My hypotheses for the model are built around these factors.

The model that I have built suggests that five factors are important to risk mitigation in organizations as follows:

1. **Process Auditing**
2. **Reward System**
3. **Quality of Operations Relative to Industry**
4. **Perception of Risk**
5. **Command and Control**

I also noted that my model is not entirely new nor unrelated to past literature. My fifth hypothesis, regarding the command and control system is drawn from Roberts' work (1992). The hypotheses for risk perception (H4) and commmand and control (H5) are also supported by previous research by Turner (1976, 1978). Exhibit 3B shows how my model relates to the other models mentioned so far in this paper.

As can be seen from Exhibit 3B, my model incorporates prior work, but goes beyond existing studies by adding at least two factors that help explain the propensity for risk-mitigation or non-risk-mitigation by firms (process auditing and reward system). Furthermore, my model is richer and more integrated than the previous models.

In the next chapters I will test the model I have developed here on a set of organizations. I will use ten banks, some failing and some successful to see if the hypotheses outlined above seem to explain their success or failure.

TABLE OF CONTENTS