Analysis of the Challenger Disaster as a Normal Accident

Michael Salib

November 13, 2002

The question of whether the Challenger disaster constitutes a normal accident as defined by Perrow (Perrow, 1999) hinges on how one chooses to define the system in question. If we restrict our definition of the system so that it consists only of the technological components involved (e.g., Solid Rocket Motor, Orbiter Main Engines, Orbital Maneuvering System), then the Challenger disaster was not a normal accident. However, if we expand our definition of the system to encompass the organizational aspects of the space shuttle system in addition to the technological components, the Challenger Disaster easily meets Perrow's criteria for a normal accident. We will examine why the space shuttle system meets many of Perrow's requirements when analyzed solely in terms of its technological components, yet ultimately fails to qualify as a normal accident. We will then discuss how the combined technological and organizational system satisfies the requirements of a normal accident. Finally, we will consider the necessity of considering organizational as well as technological failures when

understanding normal accidents.

Perrow argues that a normal accident is one which arises from the interaction of multiple failures in a complex, tightly coupled system (Perrow, 1999, p. 4–5). Moreover, these failures do not occur in a direct operational sequence and thus cannot have been foreseen by system designers (Perrow, 1999, p. 22–23). In addition, he argues that normal accidents are often (but not necessarily) incomprehensible at the time of their occurrence (Perrow, 1999, p. 9). Looking only at the technological aspects, the Challenger disaster meets many, but not all of these criteria as we shall now see.

Ample evidence suggests that the space shuttle was an extremely complex system. For example, during his interview on the *MacNeal-Leher News Hour*, Rogers Commission member and Noble Laureate Richard Feynman pointed out that even after years of analysis by the thousands of experts, they were still not completely certain of what caused the explosion. The system was so complex that not only were operators unable to diagnose and respond to problems in-flight, but years after the fact, America's best scientists and engineers were still mystified about the precise causes of the disaster. Rogers commission member and astronaut Sally Ride refused to fly on the shuttle after seeing just how badly the system complexity overwhelmed the NASA bureaucracy charged with ensuring astronaut safety (Whitbeck, 1998, p. 143). Neil Armstrong, another astronaut on the commission, described the shuttle as a "tender design" (Vaughan, 1996, p. 390); in fact, both investigatory commissions were so awed by the overall system complexity that they took pains "to repeatedly and publicly emphasize that the technology was developmental, not operational" (Vaughan, 1996, p. 390).

One very strong indicator of system complexity was that the system became so complex that the bureaucratic process for managing it grew large enough for decision rules to become completely cut off from the scientific process that produced them. Diane Vaughan writes that a key "launch decision rule had become dissociated from its creators and the engineering process behind its creation" (Vaughan, 1996, p. 391). Reversing Arthur C. Clarke's old adage that "any sufficiently advanced technology is indistinguishable from magic", the NASA administrators became shamans, reducing complex engineering decisions to mantras and rituals, in the face of overwhelming technological complexity. This failure of the bureaucratic process explains why those who knew about the launch temperature requirement could not apply it correctly. However, most people did not even know about that requirement because the system had grown so complex that individual workers were required to be far too specialized to know about such important global requirements (Vaughan, 1996, p. 391).

The complexity of the system so strained the bureaucratic culture charged with managing it that vital information about life critical flaws was widely ignored. Whitebeck cites the case of a deputy NASA administrator who wrote a memo describing the O-ring problem several years before the accident; this man was later shocked to learn that "Jesse Moore, the NASA decision maker in charge of the Challenger flight, did not know of the O-ring problem" (Whitbeck, 1998, p. 143).

In addition to being a highly complex system, the space shuttle was also a tightly coupled system. As the Challenger accident demonstrates, failures rapidly cascade: an O-ring seal

breaks and allows hot exhaust gasses to escape which then easily penetrate the thin skin of the disposable external tank, igniting hundreds of tons of liquid hydrogen. The rapidity with which this one failure propagated throughout the system demonstrates how tightly coupled the system was. In keeping with Perrow's definition, we note that failure propagated so quickly that it was impossible for operators to either understand what was happening or to react appropriately to the imminent explosion.

Yet despite that apparent complexity and tight coupling present in the technological system, it fails to meet Perrow's definition of a normal accident. A key component of that definition is that the accident result from *an interaction between failures that the designers never anticipated*. The failure that ultimately led to the Challenger accident was both well understood and anticipated. For example, we know that Roger Boisjoly wrote a memo to Robert Lund, the vice president of engineering at Thiokol, outlining his fears that a cold weather launch would cause the shuttle to explode (Whitbeck, 1998, p. 137). This memo "got the attention of top management" (Whitbeck, 1998, p. 138). The night before the launch, "Boisjoly went directly to Bob Lund and convinced him" to stop the launch (Whitbeck, 1998, p. 140). In a lecture in which he explained his actions during the crisis, Roger Boisjoly notes that after the fateful engineering review the night before Challenger's launch, he wrote in his journal of his expectation that the boosters would return with completely burned out seals.

This paper trail demonstrates just how well NASA and Thiokol managers understood the potential for catastrophic failure. They knew that there was a certain probability that

the seals would fail given the low temperature at launch. Furthermore, they knew that a complete seal failure would most likely cause the vehicle to explode. These people made "a management decision" that night, fully aware of the risks. The failure that eventually destroyed the Challenger space shuttle was thus well understood; we have seen that the designers gave a great deal of consideration to this particular failure mode. Therefore, the Challenger disaster cannot qualify as a normal accident when we consider only the technological system.

However, when we consider the combined technological and organizational system, the story changes. Like the technological system, the organizational system was also highly complex. It consisted of thousands of people spread across the United States working in different groups but often on the same problems from within different organizations. The organizational system was also tightly coupled. If the organization was designed so that managers could not override the engineering team's decision to postpone the launch, then their failure in succumbing to schedule pressure (in the case of NASA managers) or financial pressure (in the case of Thiokol managers) would not have allowed the earlier failure in seal design to propagate through the system. In other words, if Thiokol and NASA were decentralized enough that a single engineer could halt the launch process if he thought that it presented unacceptable risks, the accident would never have happened because the earlier design failures would not have been able to propagate. This suggests that points of organizational centralization indicate tight coupling in organizations.

Since both the technological and organizational systems were complex and tightly cou-

pled, the combination of the two was also complex and tightly coupled, if not more so. This meant that small organizational failures, like the engineers' difficulty making effective presentation graphics to illustrate their warnings (Vaughan, 1996, p. 398) or the lack of an ombudsman's office at both Thiokol and NASA (Whitbeck, 1998, p. 140) contributed in complex ways to the accident.

Now that we have verified that the combined system is both complex and tightly coupled, we can determine if the combined system meets the other requirements needed to satisfy Perrow's definition. The unanticipated interaction of failures proceeded as follows. The first failure occurred when the original joint design team made a mistake in their design. Other failures include the unusually cold weather and NASA's inability to apply the shuttle's launch temperature requirement correctly (Vaughan, 1996, p. 391). More importantly, because Thiokol was struggling to remain sole contractor for the SRB program, their management failed in allowing such contract considerations to undermine an engineering decision that directly impacted safety (Whitbeck, 1998, p. 142). Similarly, because NASA had "overpromised achievement and failed in many of its promises, it felt pressure to have the flight with 'the teacher in space' as a viable success that could be mentioned in the State of the Union Address" (Whitbeck, 1998, p. 142). Moreover, much of the pressure on NASA stemmed from the fact that "Congressional and Administration policy indicated that a reliable flight schedule with internationally competitive flight costs was a near-term objective" (Vaughan, 1996, p. 390). In the eyes of the House committee investigating the accident, this pressure helped cause the tragedy, and thus constitutes another failure.

Had any one of these failures not occurred, Challenger would not have exploded that day, and yet, none of these failures individually was sufficient to cause the accident. The accident resulted from the interaction of all these failures. Moreover, this particular combination of failures was not foreseen by the system designers. This system had explicit safeguards to prevent many of the organizational failures that occurred from happening, but its designers never anticipated what would happen if those safeguards failed. For example, the Flight Readiness Review (FRR) was designed to prevent the "normalization of deviance" from occurring, but no one anticipated how financial and political pressure on NASA and Thiokol would hinder the FRR's effectiveness. More specifically, even though "the original technical culture struggled to survive amid institutionalized production concerns" (Vaughan, 1996, p. 396), none of the participants ever questioned how the two competing cultures interacted with one another, and ultimately compromised organizational goals.

Like many normal accidents, the Challenger disaster was associated with a certain incomprehensibility. The people involved never realized that the organizational safeguards used to ensure that failures in the technological system were dealt with appropriately were collapsing all around them under a barrage of political and financial pressure. Not only did they not realize that their safeguards were failing, but those failures guided and reassured them. Indeed, "the fact that they did everything they were supposed to do reinforced the technical choices they made" (Vaughan, 1996, p. 397).

Combining all the evidence, we can see that the Challenger disaster does satisfy Perrow's definition of a normal accident when we consider both the technological and organizational

systems together. The role that failures in the organizational system played in bringing about the accident can best be summarized by saying "the interweaving of structure, process, and layered cultures that affected all participants' behavior at a subtle, prerational level combined to produce the outcome" (Vaughan, 1996, p. 399). This is not a novel contribution; the Presidential Commission investigating the accident "made it clear that the disaster was not merely a technical failure, but implicated the NASA organization" (Vaughan, 1996, p. 390). The real lesson in the Challenger disaster is the suggestion that organizational centralization is associated with tight coupling, and is thus the harbinger of disaster. This notion is supported by Perrow who notes that normal accidents implicate organizations trapped by internal contradictions: complexity dictates the need for decentralization while tight coupling dictates centralized management (Perrow, 1999, p. 10). Ultimately, centralized organizations lack the flexibility to safely manage systems beyond a certain threshold of complexity. A society intent on self preservation should bear that in mind.

References

Charles Perrow. *Normal Accidents: Living with High-Risk Technologies*. Princeton University Press, 1999.

Diane Vaughan. *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*, chapter 10 Lessons Learned. University of Chicago Press, 1996.

Caroline Whitbeck. Two Models of Professional Behavior: Roger Boisjoly and the *Chal-*

lenger, William Lemessurier's Fifty-None Story Crisis. In Caroline Whitbeck, editor, *Ethics in Engineering Practice and Research*, pages 133–156. Cambridge University Press, 1998.