Massachusetts Institute of Technology
Engineering Systems Division

Working Paper Series

Short Takes on the Literature

ESD-WP-LIT-2003-01

"NORMAL ACCIDENTS" BY CHARLES PERROW - REVIEWED BY DANIEL E. WHITNEY

Daniel E. Whitney

July 2003

NORMAL ACCIDENTS BY CHARLES PERROW

Daniel E Whitney

This book is a classic analysis of complex systems conducted from the point of view of a social scientist. It was the first, or one of the first, to propose a framework for characterizing complex technological systems such as air traffic, marine traffic, chemical plants, dams, and especially nuclear power plants according to their riskiness. "Normal" accidents are called that because they seem to start with something that seems ordinary or that happens all the time, almost always without causing great harm. Perrow also uses a term that seems better, *system accidents*, which conveys the idea that apparently trivial events cascade through the system in unpredictable ways to cause a large event with severe consequences.

It is interesting that social scientists have been the creative thinkers in this domain, which would seem to belong to technologists. Among technologists, only Tom Sheridan comes to mind as a thinker in this area. In ESD, Nancy Levison thinks about such systems in similar ways, and John Carroll has drawn conclusions that are consistent with those of Perrow and others.

Speaking roughly, psychologists and cognitive scientists deal with the "components" of social phenomena while social scientists and organizational theorists deal with the "system" aspects. Looked at this way, Perrow concerns himself with the relationships between the human components and both a technical situation's components (valves, pumps) and its system aspects (pipes that connect pumps and valves, wires that connect valve actuators to panel indicator lights). Perrow concludes that the accidents he analyzes, such as Three Mile Island and a number of others, all began with a mechanical or other technical mishap and then spun out of control through a series of technical cause-effect chains because the operators involved could not stop the cascade or unwittingly did things that made it worse.

Other thinkers, such as Jens Rasmussen, James Reason, and Karl Weick, (see the References for representative articles by these authors) consider the system on the social side (the organization and its managerial incentives) as well. Rasmussen and Reason say that organizations contain latent weaknesses that harbor or nuture "accidents waiting to happen" that are caused when some trigger event occurs. Rasmussen stresses that the actual accident should not be examined in itself too carefully because it is only a symptom and an example of an entire ensemble of things that could have happened. Weick notes that there are some kinds of organizations, called High Reliability Organizations (HRO), that perform distinctly better during system accidents than other organizations do. Weick et al carefully compare HRO theory with Normal Accident Theory. These thinkers have also contributed a number of conceptual lenses that help us to understand the issues on a higher level of abstraction. Among these are "a culture of diminished expectations" that takes small problems as normal instead of thinking of them as warnings, and "creeping toward the edge" that allows gradual deterioration of procedures or standards because past deterioration has not caused a problem. The distinction between "scenario analysis" and "hazard" analysis is also useful in deconstructing some of the accidents.

Perrow's framework is two-dimensional. On one axis is an indicator of what we would call an architectural characteristic, although Perrow does not use this word. This axis is labeled tightness of coupling. It generally indicates how fast cause and effect propagate through the system. Systems with low coupling have slack along one or more dimensions such as time or space. The other axis measures "complexity," which generally indicates not only how many interactions there are but how hard they are for the operators of the system to see and understand. The loosest and least complex situations are routine bureaucracies like the Post Office while the tightest and most complex are nuclear power plants and the nation's nuclear defense missiles, radars, and retaliation protocols. The tight-complex systems present fast-moving events to befuddled operators. These operators react too slowly, and the automatic systems installed to react faster are broken or give confusing signals.

Perrow was prompted to write this book by his objections to the Kemeny report on TMI. This report primarily blamed the plant operators for the accident. Perrow felt that this conclusion was unfair to the operators and masked the more serious system problems. He concluded that such plants are simply too hard to operate, and this is reflected in his framework. More generally, blaming the operators is called "person theory" by Rasmussen and Reason,[1] whereas they call Perrow's framework "system theory." The latter is clearly the more sophisticated. It has been applied to problems such as "the wrong patient" mistakes in hospitals [Chassin and Becher], in which there are no mechanical errors at all, and in fact the events do not seem to have a cause-effect relationship but just "come together" in some unfortunate way.

Moreover, Perrow is a technological pessimist. He says repeatedly that nuclear power plants cannot be improved, that all the safety systems only make them more complex or prone to false alarms or complacency, and that even one accident could be so catastrophic that it really does not matter if the plants are improved because nothing will succeed in eliminating accidents. He also says that complexity requires that such systems be governed in an authoritarian top-

---

[1] It is called the "fundamental attribution error" by psychologists. See Plous, S., *The Psychology of Judgment and Decision-Making,* New York: McGraw-Hill, 1993.

down way with rigidly enforced procedures which are incompatible with the initiative and resourcefulness needed to combat unforeseen events. Weick never claims that accidents can be eliminated, but he is nevertheless an optimist in the sense that great improvements are possible. He outlines a number of characteristics of HROs that permit them to be both hierarchical in normal circumstances and improvisational during emergencies. I think it is fair to say that we joined ESD because we are optimists.

Perrow wrote his book during 1981-85. The edition I have is a reissue in 1999 with an Afterword that reviews both the technical and social science literature spawned by his book as well as the record of accidents that have occurred since 1985. Here he acknowledges some of the extensions published by Rasmussen and Reason and frankly puzzles about why his dire predictions of more TMIs have not come true. In an unfortunate Postscript, he predicts that Y2K will bring the world to its knees. In writing this Postscript, he relies primarily on information he obtained from the Internet.

Perrow is also somewhat politically motivated, and this clouds his message. He is convinced that we have these technologically accident-prone and dangerous systems because certain "elites" (also referred to as "those in power" or "those who make decisions for us") have foisted these systems on us for their own gain. The word "elite" or its obvious synonyms occurs 27 times in 411 pages. This line of reasoning is used to cut both ways: air travel is comparatively safe because the elites also fly. He never argues that elites avoid living near nuclear power plants but he does argue that the rest of us cannot avoid it.

There are in fact a number of methodological problems with this book. He argues basically from examples and he almost never understands the need for a null hypothesis or a base case. He says "I hope I have convinced you that nuclear power plant accidents are frequent," but he never answers "compared to what?" In fact, he acknowledges many of these shortcomings in a footnote on page 97. He also acknowledges in the Afterword that he is not a quantitative analyst.

Nevertheless, his book can be used to raise a number of important questions:

1. Are some architectures better than others regarding safety and other important characteristics? Weick and the HRO community argue that the human system can be used to compensate for the technological system.

2. How can we measure the complexity of two systems in order, among other goals, to be able to rationally compare their rate of, or

susceptibility to, accidents in order to see if one of them is performing worse that we should expect?

3. Is emergence inevitable? Equivalently, are systems without emergence of too little economic significance to be worth building? (Perrow, in one of his best passages, notes that loosely coupled systems are less efficient in their use of resources, can be wasteful of time, and so on.)

4. Does emergence result from just the architectural decisions or characteristics of a system, or are detailed design decisions operative as well? Note that the TMI reactor lacked a direct indicator of its main hazard, that coolant had fallen below the top of the core. All the designed-in indicators were indirect and required the operators to reason about how the plant worked in order to decipher the accident.

5. Perrow acknowledges that some systems are loosely coupled or not very complex within a limited definition of their system boundaries, but become more complex if the system boundary is expanded. He also notes that human cognitive limits are important in causing system accidents. Thus these two factors remain on our plate.

References

M. Chassin and E. Becher, "The Wrong Patient," Annals of Internal Medicine, vol 136, # 11, June, 2002, pp 826-833. A "non-series" of 17 "non-events" involving 13 different hospital staff, such as failure to use the patient's exact name, caused one patient to get another patient's procedure. "No single error caused this adverse event; there is no reason to expect that punishing individuals would reduce the likelihood of recurrence."

J. Rasmussen, "Human Error and The Problem of Causality in Analysis of Accidents," Phil Trans Royal Soc of London, series B, vol 327, 1990, pp 449-462. The accident analyst's mental model of satisfactory explanation can cloud the analysis. "The causal tree found by an accident analysis is only a record of one past case, not a model of the involved relational structure."

J. Reason, "The Contribution of Latent Human Failures to the Breakdown of Complex Systems," ," Phil Trans Royal Soc of London, series B, vol 327, 1990, pp 475-484. Analyses of recent accidents concluded that "rather than [the operators] being the main instigators of these accidents, those at the human-machine interface were the inheritors of system defects created by poor design, conflicting goals, defective organization, and bad management decisions."

K. Weick, K. Sutcliffe, and D. Obstfeld, "Organizing for High Reliability," Res in Org Beh, vol 21, 1999, pp 81-123. "Most organizations are not frozen into

one of the four combinations that are possible in Perrow's 2x2… Instead, whole organizations change character in response to changed demands…"