Sagan, S. (1993). <u>The Limits of Safety: Organizations, Accidents, and Nuclear Weapons</u>. Princeton, Princeton University Press.

Introduction: Expecting the Unexpected

Sagan seeks to compare two "theories" of accident occurrence in organizations: Normal Accidents Theory (NAT) and High Reliability Theory (HRT). He attempts to do this through investigating the nuclear weapons safety record with respect to the 1962 Cuban Missile Crisis, the 1968 Thule Bomber Accident, and a few later incidents (including the 1979 "practice tape" and 1980 "computer chip" incidents at NORAD). He speculates on plausible scenarios via which the incidents he discusses could have become disasters instead, finds political cover-ups and organizational screw-ups that inhibit prevention or learning of mistakes, and concludes that NAT is a better descriptor than HRT.

Chapter 1: The Origins of Accidents

He starts out by identifying two "schools of thought:" Normal Accidents and High Reliability. He starts out acknowledging that these are not coherent theories, but later treats them as such.[1] HRT, according to Sagan, treats organizations as closed, rational systems.[2] He lists several characteristics which HR Organizations (HROs) have, including:

1. Safety is a primary objective held by those in command.
2. Redundancy is necessary, not wasteful.
3. Personnel must be socialized into a common organizational culture of reliability, so that they are "centralized" through this culture while acting in a decentralized fashion in order to maintain maximum flexibility. Additionally, they must continuously operate and train so as to keep their skills up.
4. The organization must have a strong capability to learn.

By contrast, normal accidents theory treats organizations as "organized anarchies," open, "natural" systems in which the limits of bounded rationality (i.e. limited information and time to make decisions, with ill-defined preferences, scant attention, where no one knows what really happens in the organization) are all too apparent. Politics are rife in the organization; elites who control them and set their goals are unaffected by organizational problems. This situation, combined with social/technological systems which are tightly coupled (little slack or time between operations or actions) and highly complex (difficult to wholly comprehend; too many parts with too many interactions), leads to dire predictions of "normal accidents," in which unexpected/unanticipated interactions between complex parts quickly spreads through the tight coupling to cause the organization to fail. Normal accident theorists[3] would thus claim that (compared to 1-4 above):

1. Organizations will have multiple, conflicting, political objectives
2. Redundancy will lead to tighter coupling;
3. The military-like high reliability culture needed is anti-democratic; training is not always possible; simultaneous centralization and decentralization is impossible.
4. Learning is limited by bounded rationality and politics.

Sagan also claims that since the nuclear weapons complex seems to fit the HRO description (does it?), this should be a "tough test" for NAT.[4] See p.46, Table 1 for a summary of Sagan's perspectives on HRT and NAT.

Chapter 2: Nuclear Weapons Safety during the Cuban Missile Crisis

Sagan looks at four different aspects of the CMC: the SAC bomber alert, the emergency ICBM alert, ADC operations, and European alert operations. (Note Table 2.1 on p.64 with the US DEFCON system) For each, Sagan points out errors and mistakes that were made and claims that these are more in line with NAT than with HRT.

[1] Note: I worked with Gene Rochlin and Todd La Porte at UC Berkeley, both of whom are associated with the HRO school of thought. When I told Todd that I was going to be presenting HR "theory," his reaction was, "it's not a theory." Rather, it's a series of case studies in which they seek to identify necessary, but not sufficient, conditions for high reliability operations. Sagan's book led to a vitrolic debate among La Porte, Rochlin, Sagan, and Perrow which filled an entire journal issue. See La Porte, T. R., C. Perrow, et al. (1994). "Systems, Organizations and the Limits of Safety: a Symposium." <u>Journal of Contingencies and Crisis Management</u> **2**(4 (December)): 1-240.

[2] An attribution fiercely denied by La Porte.

[3] Sagan refers to hypothetical "NA theorists" and "HR theorists" throughout the book. For the first, read "Charles Perrow," and for the second, read "Straw Man."

[4] Note the rhetoric of theory testing which Sagan uses, which is your standard IR/positivist/Lakatosian terminology. Also consider whether he is selecting on the dependent variable: what about the dogs that don't bark? Finally, a central question (never properly resolved in any of the literature) is: what is an accident, as opposed to a failure or an incident? For example, in the opening paragraph, we have nuclear-armed planes that almost took off as a result of unexpected, complex interactions in a tightly coupled situation: does "almost" make it an accident? Among the NWS, as of 1997, we have logged a total of 1,857,852 weapon-years without an accidental or unauthorized use.

Sagan, S. (1993). The Limits of Safety: Organizations, Accidents, and Nuclear Weapons. Princeton, Princeton University Press.

SAC Bomber Alert

SAC B-52s continuously flew during the CMC (and before, and after – but with a dramatic increase in forces during the crisis) in order to ensure the survivability and prompt response or to engage in a preemptive attack upon the USSR. At a first cut, they flew 2088 missions with 47000 hours and 20 million miles with 4076 refuelings without a crash or incident. At a second cut, Sagan points out a minor controversy over arming B-52s with a possibly riskier bomb, and a more important case regarding a lost B-52 that almost flew into Soviet airspace. He emphasizes the fact that this occurred despite precautions, and that the routes (which were a partial cause) were not changed until two months later.

Emergency ICBM alert

At Vandenberg AFB, nine of the ten test silos with test weapons were turned over to SAC once warheads were loaded on nine of them (thereby marginally increasing total megatonnage); however, Vandenberg still launched the tenth as a test despite the crisis. At Malmstrom AFB, the standard system of Launch Control Centers wasn't set up yet, and so a jerry-rigged system was set up that violated safety procedures. This violation was covered up by official reports.

ADC operations

The Air Defense Command (which had air-to-air nuclear interceptor missiles) had planes relocated without proper safety precautions (i.e. disarming the missiles) before flying from one place to another. False warnings also occurred which almost led to scrambling of fighters (see p.99). Sagan speculates on the escalation potential of these problems, and here (as he does throughout the book) speculates on possible complex interactions which could have led/could lead to normal accidents.

European alert operations

In the European theatre, nuclear-armed interceptors and bombers were placed on a higher alert status than was called for by CINCEUR/SACEUR. Sagan uses this case (and others) to point out that the President does not have absolute final control over the deployment and force posture of nuclear-armed forces, due to local politics.

Chapter 3: Intelligence and Warning during the Cuban Missile Crisis

Sagan moves on to discuss problems with the intelligence-gathering mechanisms (both mechanical and human) used during the CMC. Here he has three examples: the problems with the Falling Leaves radar, the Alaskan U-2 incident, and Penkovsky's false warning. Note that the *Falling Leaves* in this section, as well as the *Emergency Alert* and the *ADC operations* in the previous section were situations that lacked an important HRO component: frequent tests and training, since all were pressed into operation quickly without having routinely done such operations.

Falling Leaves

This is an interesting case, due to the fact that attempts at providing redundancy (in the form of overlapping radars) helped cause safety incidents. Launches in Florida were not communicated to the Falling Leaves sites, so they might have misidentified them. At Moorestown, a practice tape was reported as a real launch. The Laredo tracker identified an object; military personnel thought that it was the (more reliable) Moorestown radar.

Alaskan U-2

A U-2 flight over the Pole to check for nuclear testing by the Soviets ended up straying over their airspace, ran out of fuel, and was escorted back by nuclear-armed interceptors who might have accidentally (or intentionally in the heat of combat) launched their missiles.

Penkovsky

A spy in Soviet Military Intelligence was supposed to contact the US if Moscow had decided to launch an attack. He was captured, and evidently told his captors how to contact the US through the DISTANT system. The signal was sent, although the US quickly realized it was fake (since there were KGB agents at the drop point).

Chapter 4: Redundancy and Reliability: The 1968 Thule Bomber Accident

SAC had three different routes for nuclear-armed B-52s to fly: the West Route (Alaska), the South Route (Spain), and the North Route (Greenland) (see Fig. 4.3, p.194). SAC changed one of the routes in order to supply a redundant system for observing the Thule, Greenland BMEWS site. The bomber crashed. If it had hit the BMEWS site, it would have provided a false (and non-distinguishable - see Table 4.2, p.182) signal that the site was under attack. Thus, redundancy ended up creating an additional way of causing an accident. Other factors contributed towards this possibility: other organizations were not informed of the additional flight path.

Chapter 5: Learning by Trial and Terror

Sagan focuses on organizational learning in this chapter, by looking at the October 73 DEFCON 3 alert, and NORAD's 1979 and 1980 false warnings. He concludes from the October 73 DEFCON alert that although the Air Force changed some risky practices from the 62 DEFCON alert, other problems still remained because they did not know about them. Likewise, with the 79 (practice tape inserted at NORAD into the computer) and the 80 (computer chip malfunctions, begins inserting "2"s into the number of missiles launched at the US), he notes that previous experiences (i.e. Morristown practice tape, see above) did not lead to learning. There's also a bit of "they should have known better" thought here, w.r.t. the type of message sent (e.g. it should not have been susceptible to the "2" problem.) As with all other chapters, Sagan theorizes about other failure modes which could have occurred. This is useful for policymakers, but proves little about the systems.

Chapter 6: The Limits of Safety

Sagan's conclusions and "lessons learned."
With respect to organizational theory:

- common organizational culture can be used not only to promote safety, but also narrow self-interest;
- conflicting interests abound everywhere;
- constraints on learning are extensive;
- organization theorists should be wary of systems that appear to be working.

With respect to deterrence theory, he warns that

- wars could start by accident, and
- the spread of weapons could lead to more accidents.

Finally, with respect to improving weapons safety, he argues that

- there are limits to the solutions provided by high reliability theory,
- military organizations should be monitored externally as well as internally,
- learning on safety should be shared among countries,
- more research should be done on the past record,
- the organizational culture of nuclear weapons units should be changed to emphasize safety,
- redundancy is not a cure-all, but should be implemented carefully;
- complete disarmament, while beneficial in the abstract, is not politically possible (but reductions are recommended),
- the structure of the US forces should be changed to minimize tight coupling and complex interactions, and
- operator error, whether on the individual or organizational level, is incorrect.