Chapter 14

FAILURE AS SYSTEM INFORMATION

> As is usually the case after a ... disaster of such proportions, the final stage in this sorry tale is the apportioning of blame -- the means by which society obtains a modicum of revenge for the wrong it has suffered, expiates its own guilt for [its] responsibility ... for the event in question, and finally seeks to prevent a repetition of the disaster. Of these only the last is in any way ennobling, for it is thus that the disaster can be turned to good account.
>
> Dixon's comments on the events that followed the infamous Charge of the Light Brigade. From "On the Psychology of Military Incompetence" p. 43

The last chapter suggested how difficult it is to understand accidents and incidents. The complexity of modern systems makes post accident investigation difficult in a number of ways. Layers of technical complexity hide the significance of subtle human performance factors. Awareness of hazard and the consequences of overt failure lead to the deployment of (usually successful) defenses against failure. These efforts create a setting where overt failures only occur when multiple small faults combine. The combination of multiple contributors and hindsight bias makes it easy for reviewers after-the-fact to identify an individual, group or organization as a culprit and stop. These characteristics of complex systems tend to hide the real characteristics of systems that lead to failures.

More importantly, they lead us to adopt ineffective strategies for responding to accidents. Unable to see the sources of success and failure, we tend to slide into various forms of 'blame and train' responses to failure. Seeing human operator failure as the cause, we seek to eliminate human operators and constrain operators in the hope

of protecting the system from the erratic human element. These kinds of reactions to failure are unproductive in two ways:

1. it distracts us from the real issues that drive system performance towards and away from accidents and
2. it leads us to create ever more difficult conditions under which operators must work to achieve success.

This chapter looks at the obstacles to learning and, using an industrial example, how learning from accidents actually leads to new insights and effective change.

Incident 4—Organizational Learning

A chemical fire occurred during maintenance on a piece of process machinery in the clean room of a large, high technology product manufacturing plant. The fire was detected and automatically extinguished by safety systems that shut off flow of reactants to the machine.

The reactant involved in the fire was only one of many hazards associated with this expensive machine and the machine was only one of many arranged side by side in a long bay. Operation and maintenance of the machine also involved exposure or potential exposure of thermal, chemical, electrical, radio frequency, and mechanical hazards. Work in this environment was highly proceduralized.[36] Both the risks of accident and the high value of the machine and its operation had generated elaborate formal procedures for maintenance and required two workers (buddy system) for most procedures on the machine.

The manufacturer had an extensive safety program that required immediate and high level responses to an incident such as this, even though no personal injury occurred and damage was limited to the machine involved. High level management directed immediate investigations, including detailed debriefings of participants, reviews of corporate history for similar events, and a 'root cause' analysis. Company policy required completion of this activity within a few days and formal, written notification of the event and related findings to all other manufacturing plants in the company. The cost of the incident may have been more than a million dollars.

Two things prompted the company to engage outside consultants for a broader review of the accident and its consequences. First, search for prior similar events in the company files discovered a very similar accident at a manufacturing plant in another country earlier in the year. Second, one of the authors (RIC) recently had been in the plant to study the use of a different machine where operator 'error' seemed prevalent but

[36] The site had repeatedly undergone ISO 9000 certification and review.

> only with economic consequences. He had identified a systemic trap in this other case and provided some education about how complex systems fail a few weeks earlier. During that visit, he pointed out how other systemic factors could contribute to future incidents that threatened worker safety in addition to economic losses and suggested the need for broader investigations of future events.
>
> Following the incident two of the authors returned (RIC and DDW), visited the accident scene, and debriefed the participants in the event and those involved in its investigation. They studied operations involving the machine in which the fire occurred. They also examined the organizational response to this accident and to the prior fire.

The obstacles to learning from failure are nearly as complex and subtle as the circumstances that surround a failure itself. Because accidents always involve multiple contributors, the decision to focus on one or another of the set, and therefore what will be learned, is largely socially determined.

In the incident just described, the formal process of evaluating and responding to the event proceeded along a narrow path. The investigation concentrated on the machine itself, the procedures for maintenance, and the operators who performed the maintenance tasks. For example, they identified the fact the chemical reactant lines were clearly labeled outside the machine but not inside it where the maintenance took place. These local deficiencies were corrected quickly. In a sense, the accident was a 'normal' occurrence in the company; the event was regretted, undesirable, and costly but essentially the sort of thing for which the company procedures had been designed and response teams created. The main findings of this formal, internal investigation were limited to these rather concrete, immediate, local items.

A broader review, conducted in part by outsiders, was based on using the specific incident as a wedge to explore the nature of technical work in context and how workers coped with the significant hazards inherent in the manufacturing process. This analysis yielded a different set of findings regarding both narrow human engineering deficiencies and organizational issues. In addition to the relatively obvious human engineering deficiencies in the machine design discovered by the formal investigation, the event pointed to deeper issues that were relevant to other parts of the process and other potential events.

There were significant limitations in procedures and policies with respect to operations and maintenance of the machine. For example, although there were extensive procedural specifications contained in maintenance 'checklists', the workers had been called on to perform multiple procedures at the same time and had to develop their own task sequencing to manage the combination. Similarly, although the primary purpose of the buddy system was to increase safety by having one worker observe another to detect incipient failures, it was impossible to have an effective buddy system during critical parts of the procedures and parts of this maintenance activity. Some parts of the procedures were so complex that one person had to read the sequence from a computer screen while the other performed the steps. Other steps required the two individuals to stand on opposite sides of the machine to connect or remove equipment, making direct observation impossible.

Surprisingly, the formal process of investigating accidents in the company actually made deeper understanding of accidents and their sources more difficult. The requirement for immediate investigation and reporting contributed to pressure to reach closure quickly and led to a quick superficial study of the incident and its sources. The intense concern for "safety" had led the company to formally vest safety in a specific group of employees rather than the production and maintenance workers themselves. The need for safety as an abstract goal generated the need for these people as a separate entity within the company. These "safety people" had highly idealized views of the actual work environment, views uninformed by day to day contact with the realities of clean room work conditions. These views allowed them to conceptualize the accident as flowing from the workers rather than the work situation. They were captivated in their investigation by physical characteristics of the workplace, especially those characteristics that suggested immediate, concrete interventions the could be applied to "fix" the problems that they thought led to the accident.

In contrast, the operators regarded the incident investigation and proposed countermeasures as derived from views that were largely divorced from the realities of the workplace. They saw the "safety people" and their work as being irrelevant. They delighted in pointing out, for example, how few of them had any practical experience with working in the clean room. Privately, the workers said that production

pressures were of paramount importance in the company. This view was communicated clearly to the workforce by multiple levels of management. Only after accidents, they noted, was safety regarded as a primary goal; during normal operations, safety was always a background issue, in contrast to the primary need to maintain high rates of production.[37]

During the incident investigation, it was discovered that a very similar incident had occurred at another manufacturing plant in another country earlier in the year – a precursor event or rehearsal from the point of view of this manufacturing facility. Within the company, every incident, including the previous overseas fire, was communicated within the company to safety people and then on to other relevant parties. However, the formal report writing and dissemination about this previous incident had been slow and incomplete, relative to when the second event occurred. Part of the recommendations following from the second incident addressed faster production and circulation of reports (in effect, increasing the pressure to reach closure).

Interestingly, the relevant people at the plant knew all about the previous incident as soon as it had occurred through more informal communication channels. They had reviewed the incident, noted many features that were different from their plant (non-US location, slightly different model of the same machine, different safety systems to contain fires). The safety people consciously classified the incident as irrelevant to the local setting, and they did not initiate any broader review of hazards in the local plant. Overall they decided the incident "couldn't happen here."

This is an instance of a *discounting or distancing* process whereby reviewers focus on differences, real and imagined, between the place, people, organization and circumstances where an incident happens and their own context. By focusing on the differences, they see few or no lessons for their own operation and practices.

---

[37] Remarkably, the workers themselves internalized this view. There were significant incentives to provided directly to workers to obtain high production and they generally sought high levels of output to earn more money.

Notice how speeding up formal notification does nothing to enhance what is learned and does nothing to prevent or mitigate discounting the relevance of the previous incident. The formal review and reports of these incidents focused on their unique features. This made it all the easier for audiences to emphasize what was different and thereby limit the opportunity to learn before they experienced their own incident.

It is important to stress that this was a company taking safety seriously. Within the industry it had an excellent safety record and invested heavily in safety. Its management was highly motivated and its relationships with workers were good, especially because of its strong economic performance that led to high wages and good working conditions. It recognized the need to make a corporate commitment to safety and to respond quickly to safety related events. Strong pressures to act quickly to "make it safe" provided incentives to respond immediately to each individual accident. But these demands in turn directed most of attention after an accident towards specific countermeasures designed to prevent recurrence of that specific accident. This, in turn, led to the view that accidents were essentially isolated, local phenomena, without wider relevance or significance.

The management of the company was confronted with the fact that the handling of the overseas accident had not been effective in preventing the local one, despite their similarities. They were confronted by the effect of social processes working to isolate accidents and making them seem irrelevant to local operations. The prior fire overseas was noticed but regarded as irrelevant until *after* the local fire, when it suddenly became critically important information. It was not that the overseas fire was not communicated. Indeed it was observed by management and known even to the local operators. But these local workers regarded the overseas fire not as evidence of a type of hazard that existed in the local workplace but rather as evidence that workers at the other plant were not as skilled, as motivated and as careful as they were, after all, they were not Americans (the other plant was in a first world country). The consequence of this view was that no broader implications of the fire overseas were extracted locally after that event.

Interestingly (and ominously) this *distancing through differencing* that occurred in response to the external, overseas fire, was repeated *internally* after the local fire. Workers *in the same plant,* working in

the same area in which the fire occurred but on a different shift, attributed the fire to lower skills of the workers on the *other shift*.[38] They regarded the workers to whom the accident happened as inattentive and unskilled. Not surprisingly, this meant that they saw the fire as largely irrelevant to their own work. After all, their reasoning went, the fire occurred because the workers to whom it happened were less careful than us. Despite their beliefs, there was *no* evidence whatsoever that there were significant differences between workers on different shifts or in different countries (in fact, there was evidence that one of the workers involved was among the better skilled).

Contributing to this situation was, paradoxically, safety. Over a span of many years, the incidence of accidental fires with this particular chemical had been reduced, and in general But as a side effect of success, personnel's sensitivity to the hazard the chemical presented in the workplace was reduced as well. Interviews with experienced "old hands" in the industry indicated that such fires were once relatively common. New technical and procedural defenses against these events had reduced their frequency to the point that many operators had no personal experience with a fire. These "old hands" were almost entirely people now in management positions, far from the clean room floor itself. Those working with the hazardous materials were so young that they had no personal knowledge of these hazards, while those who did have experience were no longer involved in the day to day operations of the clean room.

In contrast with the formal investigation, the more extensive look into the accident that the outside researchers' visit provoked produced different findings. Discussion of the event prompted new observations from within the plant. Two examples may be given. One manager observed that the organization had extensive and refined policies for the handling of the flammable chemical delivery systems (tanks, pipes, valves) that stopped at the entrance to the machine. Different people, policies, and procedures applied to the delivery system. He made an argument for carrying these rules and policies through the machine itself. This would have required more extensive (and expensive)

[38] Given this attitude of workers close to the context of the incident, workers and managers of other parts of the manufacturing process saw little relevance or potential to learn from the event.

preparation for maintenance on the machine than was currently the case but would have eliminated the hazardous chemical from within the machine prior to beginning maintenance. Another engineer suggested that the absence of appropriate labeling on the machine involved with the accident should prompt a larger review of the labeling in all places where this chemical was used or transported.

These two instances are examples of using a specific accident to discover characteristics of the overall system. This kind of reasoning from the specific to the more general is a pronounced departure from the usual approach of narrowly looking for ways to prevent a specific event from occurring.

The chemical fire case reveals the pressures to discount or distance ourselves from incidents and accidents. In this organization, effective by almost all standards, managers, safety officers, and workers took a narrow view of the precursor event. By narrowing in on local, concrete, surface characteristics of the precursor event, the organization limited what could be learned.

This case illustrates a general principle for organizational learning. Do not discard other events because they appear on the surface to be dissimilar. At some level of analysis, all events are unique; while at other levels of analysis, they reveal common patterns. Instead, look for areas where the other events are similar to your own work context. Each kind of contributor to an event and how they combined can guide the search for similarities. This will require shifting from surface characteristics to deeper patterns and more abstract dimensions.

When this process of learning was stimulated in this case, the organizational response changed. They derived and shared with us a new lesson – safety is a value of an organization, not a commodity to be counted or a priority set among many other goals.