System Effects, Failure, and Repair: Two Cases

Diane Vaughan[*]

Department of Sociology, Columbia University (United States)

Abstract

This paper argues for the importance of studying the systemic causes of organization failures. Taking a systems approach calls for both a theoretical and methodological framing that examines system effects: the relation between conditions, actors, and actions in the institutional environment, as they affect organizations, changing them, and consequently changing the workplace, technology, tasks, and the actions and reactions of the people who work there. All organizations are vulnerable to system effects — competition for scarce resources necessary to achieving organization goals, including survival, status, and legitimacy in their organization field. Consequently, this research aims to fill gaps in what is known about failure by asking how and why, of two organizations with similar operations and under the same constraints, one is subject to repeat catastrophic failures, while the other has been able to maintain safety. To this end, this research is a cross-case comparative analysis based on historical ethnographies of two crises in large socio-technical systems, looking for analogies and differences. Both cases reveal the institutional constraints and internal responses to the liabilities of technological and organizational innovation: NASA's decision to launch the Space Shuttle *Challenger*, and Air Traffic Control response to the intersection of a staffing shortage and automation. The conclusions have implications for both policy and for our understanding of institutional persistence, change, and agency.

Keywords: Boundary Work; Ethnocognition; Heterarchy; Liabilities of Technological and Organizational Innovation; System Effects.

---

*   ✉ dv2146@columbia.edu

A substantial body of scholarship exists on how organizations fail — or to put it more generally, how things go wrong in organizations — and the harmful consequences at the societal, organizational, and individual level. I say "more generally" because such events are typically defined in retrospect and whether the outcome will be defined as a failure or not will vary by the historic moment, the extensiveness of the harm, and the social location, experiential knowledge, cultural predisposition, and/or official responsibility of the person, organization, the public, or nation-state doing the assessing. Whereas failures in competitive markets and winner-take-all industries draw attention to the competitive ideology of capitalism and competition, a long history of scholarship indicates failures and harmful outcomes are not restricted to a particular type of organizational field, form, or function, an observation that the authors in this *Sociologica* symposium confirm. All socially organized systems, regardless of size, complexity, and function, are vulnerable to failure.

Merton's thinking (1936) was foundational to understanding systemic failures. He observed that any system of purposive social action inevitably generates unanticipated consequences that run counter to its objectives. Unanticipated consequences can be differentiated into consequences for the social actor(s) involved and to others, mediated through the social structure, culture, and society. Although Merton's position was that unanticipated consequences could be positive or negative, research has focused on the negative outcomes. Incrementally, sociologists have been identifying causal factors that have culminated in a framework for understanding the systemic causes of organizational failures.

Chronologically, the study of systemic failures began with Turner (1978), who found "failures of foresight" in organization systems and their interorganizational relations. Disasters were potentially foreseeable and avoidable, but at the time the early warning signs were overlooked due to cultural beliefs about the world and norms and rules about hazards and their avoidance. A second turning point was the work of Hughes (1979 & 1983), who specialized in the historical emergence of large-scale socio-technical systems. Hughes showed how assemblages of interacting social actors — material objects, technologies, engineers, managers, scientists and multiple heterogeneous organizations — constituted system complexity, producing unanticipated consequences affecting system change over time. Third and most well-known, Perrow, in his 1984 *Normal Accidents*, identified the "error-inducing" characteristics of high-risk technical systems, arguing that the complexity and tight coupling of a technical system's parts produce unavoidable, unanticipated negative consequences; hence, the *normal* accident. Finally, Jervis (1997) examined larger systems — international relations and nation states. He focused on the reciprocal relations between the larger institutional context and the arrangements of organization units/parts. Power, politics and ambition are part of the dynamic.

Over time, the association of system complexity, uncertainty, and unanticipated consequences have remained central to understanding how things go wrong in socially organized systems. Competition is a present but not-always-acknowledged connecting mechanism. Although not all organizations are competing for economic success *per se*, as in the case of competitive markets and winner-take-all organizations, all organizations must compete in order to secure the strategic resources they need to achieve their goals: equipment, personnel, expertise, organizational and technological innovation, interior space and land acquisition, collaborators, consumers, clients. However, an organization's ability to obtain requisite resources may be constrained by the larger system in which it exists. Factors and actors in the institutional environment — historical, political, economic, technological, cultural — affect the source, nature, and abundance of the resource, the behavior of other organizations in the organization field, or by scarcity: the resource itself may be in limited supply, so the organization is unable to meet

its goals.

Of particular concern are the failures of large complex socio-technical systems designed to serve multiple publics and accomplish larger purposes: airlines, education, criminal justice, corporations, government units and agencies, economic markets, churches, hospitals, the armed forces. Formal organizations are designed to produce means-ends social action by formal structures and processes intended to assure goal attainment (Vaughan, 1999). An organization's criteria for success are shaped by both financial conditions and by the other organizations with which it must compete. Standards for success reflect position in the organizational stratification system and may take three forms (Vaughan, 1983):

1. Shift in economic and social position: higher status competitors.

2. Shift in economic and social position: higher status among same competitors.

3. Maintenance of existing economic and social position.

The larger goal of the competition is institutional legitimacy and status in an organizational field (DiMaggio & Powell, 1983). To fail to maintain a position is to succumb to downward mobility, undermining legitimacy, possibly increasing resource scarcity, making achieving goals ever more important but more difficult, calling for both reorganization and adjustment of goals in order to persist as an organization, which may or may not occur. However, in all three of the above circumstances, organizations face new uncertainties and the possibility of unanticipated negative consequences. Consequently, scarcity, combined with the differential standards for economic and social success, raises the possibility of blocked access to resources regardless of an organization's size, wealth, age, experience, or previous record.

For our purposes, I define organization failure as:

> an event, activity or circumstance, occurring in or produced by a formal organization, that deviates from formal design goals and/or normative standards or expectations, either in the fact of its occurrence or in its consequences, and produces a suboptimal outcome. (Vaughan, 1999, p. 273)

Research on organization failure has flourished, especially by scholars concerned with accident, risk, and safety (Erikson & Peek, 2022; Sagan, 1993; Snook, 1996; Weick, 1993), as well as those specializing in changing social and economic conditions (Deener, 2020; Lounsbury & Hirsch, 2010; MacKenzie, 2011; Rilinger, 2021). However, we still lack understanding in two areas. First, only a few scholars have examined a problem within a multilayered systems framework that allows a macro-, meso-, micro- analysis (Burawoy, 1982; Vaughan, 1996 & 2021; Deener, 2020; Le Coze, 2021; Rilinger, 2021). Second, comparative research is missing that would allow us to explore why, given two complex organizational systems doing similar tasks under similarly challenging institutional constraints, one has produced catastrophic failures, while the other has been able to maintain safe operations, correct and learn from small failures, avoiding catastrophe. Better understanding of both not only has policy relevance for risk and safety but also contributes to what is known about institutional persistence, change, and agency (DiMaggio, 1988; Mahoney & Thelen, 2010).

To fill these two gaps, this paper is a cross-case comparison (as opposed to same-case), looking for analogies and differences between two large scale socio-technical systems: the National Aeronautics and Space Administration's (NASA) Space Shuttle Program and the Federal Aviation Administration's National Airspace System (NAS) (Vaughan, 1996 & 2021). Both have

national missions for which risk and safety are ongoing concerns, with the most serious consequences being loss of life. Most certainly, such large system failures have implications for the moral economy, but in addition, the participants themselves feel an individual moral obligation to keep their missions and passengers safe. Further, the performance of both agencies have implications for USA legitimacy in the international arena. Consequently, extensive safety measures are embedded in structures, processes, rules, procedures, worker training and expertise for both. The major question driving this case comparison is: how can we understand major failures by NASA in the Space Shuttle Program versus the ability of the Air Traffic Control system to maintain safety even though both organizations operate in environments in which perennial lack of government funding has been a continuing problem, undermining their ability to achieve their goals and increasing risk? The analysis contributes not only to our understanding of systemic failure, but to our understanding of institutional persistence, change, and agency.

In both cases, I explore *system effects*: how conditions in the institutional environment — historical, economic, political, technological, cultural — affect an organizational system, changing it, and consequently, how those changes affect the work place, the tasks, and the interpretation, meaning, actions and *reactions* of the people who work there. The cross-case comparison relies on analogical theorizing — searching for similarities and differences — and historical ethnography that locates a case in its history, showing how the past manifests in the present (Vaughan, 2004 & 2014). The research timing and methods varied by case. The *Challenger* research began shortly after the 1986 accident. Extensive archival data collected by the Presidential Commission investigating the case were available at the National Archives. Engineering documents, memos, and over 9000 pages of interviews with everyone involved were divided in two separate archives: the history of decision-making 1981-1986, and the eve of the launch. After extensive analysis, in 1992 I began in-person and phone interviews with key people, some repeatedly.

Air Traffic Control also included archival data, but in addition, I did observations plugged in with controllers while working, and interviews at 4 facilities: Boston Logan Control Tower, Boston Terminal Radar Approach Control (the TRACON), a radar facility controlling middle altitude airspace between the Tower and the large, high-altitude radar Boston Air Traffic Control Center in New Hampshire, and the small but busy Bedford Tower in Bedford, Massachusetts. The four were selected because they represented the four kinds of work that controllers do — and because they exchanged airplanes with each other, they represent a microcosm of the larger system. There were three periods of field work: March 2000–June 2001; 2002, post 9/11 attacks (3 of the four handled the hijacked planes that flew into the Twin Towers); then fall 2017, during automation and staffing shortage.

Although the NASA and Air Traffic Control are different in size, complexity, and function from other complex organizational systems, the cross-case comparison allows us to see structures and processes common to all organizations, otherwise invisible to us. The analysis that follows is necessarily brief, based on selective examples of a few key factors. Drawing from data for the larger analysis (Vaughan, 1996 & 2021), I first examine the analogies and then the differences between the two systems. Then I explore two historic turning points for each when risk increased: NASA's *Challenger* disaster and failure, and an Air Traffic Control crisis and repair.

1   System Effects and Unanticipated Consequences: How the Past Manifests in the Present

1.1   Launching Shuttles and Airplanes: Analogies

Both NASA and the National Airspace System are government agencies responsible for moving objects and people through space. Monopolies in the USA, their respective systems and their successes or failures have symbolic meaning and practical implications for the leadership of the nation at home and globally. Also in common, both work on technologies that have "interpretive flexibility," (Pinch & Bijker, 1984) so decisions about the safety and movement through space are made by highly skilled technical professionals. For both, all operations — organizational and technological — are driven by time, schedule, and deadlines. Moreover, historically their ability to achieve their goals has consistently been constrained by decisions by Congress and/or the Administration in power that have limited essential funding and other resources, thus changing the operations of these two organizations, their technologies, the workplace and work, increasing risk. I begin with NASA.

During the Apollo program (1961–1975) NASA was fully supported by Congress. The standards for engineering excellence behind the Apollo successes manifested in a NASA technical culture that relied on deference to in-house professional expertise, based on experiential knowledge gained by working closely on the technology. As the Apollo program neared completion, changes in US domestic and international affairs took priority over the Space Shuttle Program funding. NASA top administrators made a political bargain: they were only able to get the program approved by convincing Congress that the shuttle would essentially pay its own way, carrying "payloads" — scientific experiments for other programs and corporations — that would produce income because the shuttle would operate like a bus, transporting people and objects back and forth in space. At the predicted launch rate, the program would survive as a business, essentially becoming self-supporting. Thus, cost effectiveness became part of operations. Meeting the schedule was essential. For the middle managers and engineers assigned to the hardware, performance pressures and political accountability invaded the original technical culture (Vaughan, 1997).

The system effects of the political bargain on the organization was that the space agency became "bureaupathological," with bureaucratic accountability becoming part of the cultural mix. NASA expanded its hierarchical structure by, for the first time, "contracting out:" rather than producing all component shuttle parts in-house, the agency would rely on contractors. Many engineers were assigned to coordinate and keep records with contractors, doing deskwork. Huge amounts of paperwork had to be turned around in order to qualify each of 9 shuttle components prior to each launch. The schedule was the problem, not money for hardware redesign. The budget was based on a launch rate that was never achieved. Unless data clearly indicated a component was a serious threat to flight safety, delay was out of the question. From the first shuttle launch through *Challenger*, the original technical culture, bureaucratic accountability, and political accountability coexisted.

Whereas the NASA system preexisted the shuttle program, the development of the airplane preceded the inception of a National Airspace System. As planes began to fly higher, pilots could no longer see the runways, so airport owners began using airport workers to signal pilots from the ground: their first technologies were signaling flags, binoculars, a wheel barrow, and an umbrella — the purpose of the wheelbarrow being to move everything from one end of the runway to the other when the wind changed. As planes began to fly even higher and greater

distances and speeds, the sky became airspace, marked by artificial lines — boundaries — to keep planes from colliding. The system on the ground developed boundaries, too. Responding to the increasing capabilities of the airplane, air traffic controllers moved into Towers, then to high altitude Centers.

In order to move airplanes across the boundaries in the sky, controllers had to pass them across the boundaries on the ground to controllers in other locations — initially communicating via telephone connections; then, by airline telephone operators; then aided by blackboards listing planes and routes with controllers relying on compasses and maps, marking progress and direction. Radar was imported from Europe by the end of WW II. By then the system on the ground was divided into regions, establishing the formal structure of the air traffic control system both on the ground and in the sky. The legitimacy and technological development of the airplane resulted from the intertwined interests and resources of the airline, the military, and government, leading to interdependence of all three. The nascent air traffic control system became dependent upon them, reactive rather than proactive.

The contrast between the uneven development of the aviation system on the ground and the rapid development of airplane capabilities was stark (Vaughan, 2021). The military needed planes for war; the airline industry's problem was competition with rail travel for passengers. The airlines used military innovations to develop a larger, faster commercial airplane that would beat the competition — not only with rail traffic, but within the airline industry in this country and internationally. With increased size, speed, and height, time, timing, and deadlines were driving movement of traffic in the sky. But the system on the ground, dependent upon the government for money, lagged behind in ability to handle the changes. Some technological innovations were ongoing that would soon transform control of an aircraft from the pilot in the sky to the controller and devices on the ground. Pilots flying by Instrument Flight Rule became fully dependent on controllers who worked in organizations that were "centers of coordination" (Suchman, 1997).

Rather than telephones, controllers relied on devices to engage in *dead reckoning*: from early marine navigation, dead reckoning refers to the prediction of the position of objects in space and time by deduction, without benefit of direct observation or direct evidence. Coordination of movement across the boundaries of the sky and the system on the ground was tightly regulated by rules and procedures. The mandate of the system was "The Safe, Orderly, and Expeditious (read: speedy, cost effective, and on time) Delivery of Air Traffic." Government funded, the system routinely lacked resources. By the late 1970s, Controllers were working overtime on old and flawed equipment, with inadequate personal benefits, in the midst of a staffing shortage. In 1981, members of the Professional Air Traffic Controllers Organization (PATCO) went on strike. Then-President Ronald Reagan, fired over 14,000 striking controllers — coincidentally, the year of the first Space Shuttle Flight — leaving the system in crisis.

1.2 Organizational Structures and Processes: Differences

The organization structures and processes of getting Space Shuttles and airplanes off the ground varied, shaped by the vastly different technologies and consequently, the work required. At NASA, the shuttle design was an experimental vehicle; for Air Traffic Control, the technology — airplanes — was standardized.

The Space Shuttle has four component parts: the Orbiter, Main Engine, External Fuel Tank, and the Solid Rocket Boosters. The physical location, technical production, and deci-

sion making actors for each part was different. For the Solid Rocket Boosters (SRBs), the part of the shuttle that failed during the *Challenger* launch, the locations were Marshall Space Flight Center, Huntsville, Alabama, and Morton Thiokol, the contractor constructing the SRBs, in Wasatch, Utah. NASA was a "matrix" organization. It has a chain of command that is hierarchical, but differs from a classic hierarchical structure, where each level reports to the one above, with a CEO at the top. A NASA Project Manager had authority over a component's Work Group, reporting to the director of the larger component of which the project was a part, not to a CEO. NASA's matrix structure was duplicated by the contractor, the parallel structures making daily engineering discussions between Morton Thiokol and NASA easy.

All NASA Work Groups were comprised of engineers and technical people drawn from different parts of the system in order to bring together different engineering specializations and perspectives to create contradictory points of view and dissonance (Stark, 2011). Comprised of NASA and Thiokol engineers, the SRB work group explored the unprecedented technology, doing lab tests, technical analysis, and revising risk assessments, but the sky was the laboratory: the anomalies discovered after a mission were crucial. Differences of opinion were routine. When the inevitable controversies about risk occurred, scientific positivism reigned; it was dispute resolution by the numbers. The schedule was always important, but the entire operation was rule bound: do not launch unless all tests verify that all Launch Commit Criteria have been met. Consensus required.

A hierarchical pre-launch decision-making structure, Flight Readiness Review (FRR) began about a month or two before the launch date to bring together all shuttle components. FRR had four reporting levels that moved launch decision making up the FRR hierarchy. Each stage of the review was adversarial, with people with different expertise present to critique the engineering analysis. At Level 1, Thiokol engineers and technical people brought their risk assessment to Marshall, meeting with the SRB Project Manager and NASA engineers, all reviewing their test data, airing their concerns and differences of opinions, doing more tests and fixes to come to agreement about "Acceptable Risk," meaning that after all tests and evidence had been done, it was safe to fly. At each level, more people, with different expertise from different parts of the system, participated in the review. The Level IV review was at Marshall Space Flight Center, headed by the Center Director. 150 people participated. Ironically, and contradicting the dissonance designed into the FRR structure, at each level a found technical problem was fixed before moving up, so the original assessment of the work group incorporated more supportive data, confirming the original risk assessment to "Accept Risk and Fly." "Action Items" to fix things often extended FRR, but rarely was a launch delayed because of a technical problem found in FRR.

In contrast, the National Airspace System's multiple locations were designed to be standardized, alike in task, physically located to cover the movement of air traffic in the US within and between the nine regions of the system on the ground. Overseeing all Air Traffic Operations was the Command Center in Virginia, with a Director, Regional Representatives, and Weather Specialists to coordinate weather changes, traffic movement or incidents throughout the larger system, receiving input from all, and making decisions that affected all. Air traffic control was hierarchical on paper but in practice was a heterarchy — a collaborative organizational form that spawned dissonance and open discussion at each level (Stark, 1999; Beunza & Stark, 2004): within and between each facility, between facilities and region, within and between regions. Moreover, dissonance and collaboration were ongoing between controllers and FAA management at all levels because, unlike NASA engineers, controllers are unionized, belonging to the National Air Traffic Controllers Association (NATCA), born in the years after

the Reagan firings.

Also in contrast to NASA, all controllers had the same task. In Towers, high altitude Radar Centers, and Terminal Radar Approach Control (TRACONs), they work in teams of 3–8 with a supervisor in small, intimate spaces, elbow to elbow, so they can hear each other and coordinate traffic movement. Although the work is standardized, no two facilities are alike because as the complexity of the airspace varies, (volume, types of aircraft, crossing or single direction air patterns) the architecture, technology, and task of a facility vary. As the work varies, so does the culture of a place: the ways of doing and being. As one controller said, "You move to a different place, you have to become a different person." Consequently, the system is only *allegedly standardized*: it is riddled with variation. Necessarily, the work they do combines standardization and improvision. Heterarchy and negotiation of differences within and between the parts is built into the system, as follows.

In contrast to the Shuttle Program, the time and timing of identifying anomalies is not pre-flight, but when planes are put in motion. Quick decision-making is essential. Controllers interpretive work consists of ethnocognition and boundary work. Ethnocognition (Geertz, 1983) includes a shared cultural system of knowledge as well as a fine-tuned local knowledge. Cognition is not only distributed between people and technologies in the room (Hutchins, 1995), it is distributed beyond the room to controllers in other facilities, making coordination possible across the system. Controllers do two kinds of boundary work: they move airplanes across the boundaries of the sky, and in doing so, they also must move planes to other controllers across the boundaries of the other facilities on the ground. Because of airspace variation throughout the system, boundary work is not easy. One controller may not always be able to accept an airplane from another into their airspace ("unable"), causing the sender to hold the plane, crowding their own airspace and backing up the next neighboring airspace. Thus, boundary work is a major source of stress on the job, producing dissonance, competition and shout-outs between controllers in the same facility and across facilities. Because planes have to keep moving, boundary disputes *compelled* negotiation of differences between controllers and improvisation within their own facility and between other facilities in order to keep the system working safely.

2   NASA: The Liabilities of Technological and Organizational Innovation

The Presidential Commission investigating the *Challenger* disaster revealed that the Solid Rocket Booster O-ring failure that caused the tragedy was preceded by questionable middle management actions and decisions. First, the Commission learned of a midnight hour teleconference on the eve of the launch, in which contractor engineers located at Morton Thiokol in Wasatch, Utah protested against launching in the unprecedented cold temperatures predicted for launch time the next morning. Following a heated discussion NASA middle managers proceeded with the launch, apparently violating safety rules about passing information up the hierarchy in the process (Vaughan, 1997). Second, in the years preceding the January 28, 1986 tragedy, NASA had repeatedly and knowingly proceeded with shuttle launches in spite of recurring damage on the O-rings. The conventional wisdom conveyed by the media at the time was that NASA managers at Marshall Space Flight Center warned that the launch was risky, succumbed to production pressures, and violated safety rules in order to stick to the launch schedule.

The National Archives records contradicted the conventional wisdom, revealing instead an explanation rooted in the history of decision making, the liabilities of technological innovation, and how, on the eve of the *Challenger* launch, the past manifested in the present. The decision-

making history was studded with early warning signs. Anomalies — deviations from design expectations — were found on many missions prior to *Challenger*. But in post-flight analysis, Marshall and Thiokol working engineers continually normalized the technical deviation they found. By normalized, I mean that in all official engineering analyses and launch recommendations prior to the eve of the *Challenger* launch, Thiokol and NASA engineers analyzed the evidence that the booster design was not performing as predicted and reinterpreted it as acceptable and non-deviant (Vaughan, 1997). Tests showed that if the primary O-ring failed, the secondary O-ring would provide a redundant back-up, therefore qualifying the design officially as an "Acceptable Risk."

History and precedent were influential. The critical decision was the first one in 1981, when expecting no damage to the O-rings, inflight damage occurred and they found it acceptable. They thought the found the problem and fixed it, because the next launch had no anomaly. The engineering analysis and testing that supported this decision were foundational. The normalization of technical deviations continued. Over the years that decision was reinforced by increasingly sophisticated tests and analysis that supported the redundancy of the O-rings. Incrementally, the work group accepted more and more damage to the O-rings. At the time, each of these decisions seemed correct, routine, and insignificant. But in retrospect, they had a cumulative directionality that was stunning. How could this happen?

Sensemaking is context dependent (Weick, 1993). Shuttle technology was unprecedented, so having anomalies was expected and taken-for-granted on all shuttle parts. Initially, they had no rules to guide them about how it would operate. Despite all the lab tests, field tests, and calculation, post-flight analysis taught them the most about how the vehicle behaved. They were learning by doing, creating engineering standards and correcting them one launch at a time. The interpretive work of engineers also was influenced by the pattern of information as problems began to occur. What in retrospect appeared to be clear signals of danger that should have halted shuttle flights were interpreted differently at the time. For the SRB working engineers, the history of decision making had established a cultural belief in O-ring redundancy and SRB safety that was passed upward through FRR, so was the collective understanding prior to the *Challenger* teleconference.

2.1 System Effects and Failure: How the Past Affected the Present

The launch decision was the outcome of a two-hour teleconference between 34 people in three locations: Morton Thiokol in Utah, Kennedy Space Center in Florida, and Marshall Space Flight Center in Alabama. This decision scenario was unprecedented in three ways: the predicted cold temperature was below that of any previous launch; launch decisions always were discussed face-to-face in Flight Readiness Review, held two weeks before a launch; and Thiokol had never before come forward with a no-launch recommendation (Vaughan, 1997).

Concern about temperature came up early in the day. Thiokol needed to prepare, so chose a time for the three-location teleconference to begin, setting it at 8:15 pm. Accustomed to working in a dead-line oriented culture concerned about cost and schedule, they knew if they could reach a decision before 12:30 AM EST, when the ground crew at Kennedy would begin putting fuel into the External Tank, they could avoid the costly de-tanking if the decision was "No-Go." Production pressure drove the proceedings. The engineers collectively decided their position, then hurried to put together the engineering charts containing their analysis. They divided up the work. However, some people were putting together the final recommendation chart without seeing the data analysis charts other engineers were still creating. In the press for

time, the group never collectively discussed all the charts prior to faxing them to people in the other two locations. As it turned out, the engineering charts contained inconsistencies that did not live up to the standards of NASA's original technical culture: quantitative, scientific data for every engineering launch recommendation. Moreover, the final launch recommendation chart stated, "Do not launch unless the temperature is equal to or greater than 53 degrees," reflecting the temperature of the coldest launch, which had experienced the most O-ring damage. However, data on some of the Thiokol charts contradicted the 53 degree limit they proposed.

Recognizing their own political and bureaucratic accountability, angry Marshall managers challenged Thiokol's data analysis and conclusions. Marshall managers would be the ones who would have to carry forward the no-launch recommendation. They had done so before, but this time it was with flawed data. Moreover, the 53 degree launch limit set a new decision criterion for all launches, which would delay many launches. The effects of hierarchy and organization structure on the discussion were equally devastating. People were in three locations and could not see each other. Moreover, midway in the teleconference, the people at Thiokol held an off-line caucus. A Thiokol administrator who knew little about the technology took charge. Without any new data to support their arguments, the engineers could not build a stronger data analysis.

Then at Thiokol, bureaucratic accountability came into play. A "management decision" was made: excluding engineers, four managers reversed the no-launch decision, went back online saying they had re-examined their data, and recommended launch. When Marshall managers asked, "Does anyone have anything more to say?" No one spoke up. In three locations with no visuals, the silence of the off-line caucus created *structural secrecy* (Vaughan, 1983 & 1996). People at Marshall and Kennedy did not know that Thiokol engineers still objected. And Thiokol engineers did not know that many people in the other locations supported them and were preparing to cancel the launch. This was a "no-launch" recommendation. In an unprecedented situation, all participants invoked the usual rules about how decisions are made, when (hindsight shows) the usual rules were inappropriate. Perhaps in a situation of uncertainty, a cooperative, democratic heterarchical decision-making session that brought the dissonance and diversity of all points of view into play would have produced a different outcome (see, e.g., Beunza & Stark, 2003). Not only did the silent Thiokol engineers abide by the norms of the hierarchical system, but people in other locations had potentially useful information they did not enter into the conversation because they, too, were subordinates. The result was that conforming to all the rules, on the eve of the launch they normalized the technical deviance once again.

Many changes to increase safety followed. However, in 2003, 17 years after *Challenger*, NASA's Space Shuttle Columbia disintegrated upon reentry into the earth's atmosphere. The official accident investigation concluded that the causes of *Challenger* had not been fixed (Columbia Accident Investigation Board Report, 2003). Cameras at the launch pad showed that a large piece of foam insulation flew off the External Tank, hitting the leading edge of the shuttle wing, then the heat at reentry caused fire and disintegration. Foam had been a recurring problem, hitting protective tiles on the wings, but the damage was minimal, so tiles were replaced. The anomalies had been normalized — treated as a maintenance problem, not a risk. Further, engineers' several requests for close up satellite photos of the damage were dismissed by the Mission Manager, some for not following the mandated reporting hierarchy, others because satellite photos would take time and delay the next launch, and "there is nothing we can do anyway." Engineers were excluded from the decision. Consequently, no collaborative discussion of possibilities occurred.

3   Air Traffic Control: The Liabilities of Technological and Organizational Innovation

Beginning in the early 1990s, two trajectories of independent events intersected in the 2000s, increasing system risk and threatening safety. The first, was an FAA modernization effort, known as NextGen, which included both automation and organizational innovations. The goal was no less than shifting from a ground-based to a satellite based-navigational system, requiring new automated equipment in the workplace. The organizational innovation was to relocate and consolidate individual regional TRACONS in one regional Large TRACON in order to avoid the cost of upgrading deteriorating 1960s facilities. The second trajectory, also begun in the 1990s, was a serious staffing shortage due to years of Congressional budget cuts that resulted in hiring and was fueled by controller retirements.

Yet a third historical trajectory resulted in empowering controllers to intervene and salvage the situation. Historically, changes to improve system safety resulted in one-size-fits all standardized rules, procedures, technologies, and changes in work arrangements nationwide. However, because airspace differs, standardized changes do not work for all facilities. Informally, controllers engaged in repair, improvising to fit the change to the local situation. "How can we make this work here?" Then after several public FAA failures with technological innovations, in the 1990s the Clinton administration *legally* empowered controllers to have input into the design, development, and implementation of all technological and organization innovations, supplying the system resilience that made coordination possible.

NextGen became operational in the New England Region in 2004. Although the FAA already had several Large TRACONS successfully consolidated and in good working order, the new Boston Consolidated TRACON (BCT) was an experiment. The Large TRACONS had combined TRACONS that had airspace of the same size, traffic volume, and complexity, so the airspace could be "integrated," meaning that controllers for each facility could work each other's airspace. However, the Boston experiment would combine Boston TRACON with two small TRACONS with less airspace size and complexity, with the understanding that these controllers also would be trained to work each others' airspace. Becoming part of the new Boston Consolidated TRACON, Manchester TRACON New Hampshire moved into the new building in January 2004. The Cape TRACON would relocate in 2018 (Vaughan, 2021).

Years of planning had gone into construction of the new TRACON. Compared to the usual air traffic control facility, the building was spacious and comfortable throughout. Unfortunately, this included the Control Room. Although both Boston and Manchester controllers had been extensively trained separately on the new automated equipment in the new building before moving in it, controllers struggled to adjust to the automation and changes to the architecture, placement of material objects, and the necessary re-organization of tasks. Used to working radar elbow-to-elbow in small dark control rooms, they moved into a large, oval, brightly-lighted, high ceiled room. Hearing each other and adjusting to the light was difficult. As one said, "It was like moving from a shoe box to an airplane hangar."

The Control Room interior included an Outer Circle and an Inner Circle. The Outer Circle consisted of controller workstations side by side around the outer wall of the Control Room. At the closed end of the oval were the workstations for Boston's large airspace, and to the left were the Manchester workstations. However, because of the new automated equipment the workstations housed, they were wider and deeper than before, so controllers were no longer elbow to elbow, exacerbating the hearing problems. The Inner Circle was a large oval of con-

nected desks with computers and radar scopes for two Operations Managers, Manchester and Boston Supervisors, Traffic Management and weather personnel. The design left ample space between the Inner and Outer Circles, but size and design didn't work in practice. With only three openings in the Inner Circle, Supervisors and the other management people couldn't get to their controllers and scopes quickly enough, and they also couldn't hear.

Worse, inequalities were built into the project from the beginning. There were inequalities in salary, competence, and status as well as cultural difference in ways of doing and being for each TRACON. Also, the staffing shortage impaired ability to acquire and train new controllers on the automated equipment and at the same time train the Manchester controllers on the Boston airspace. In addition, the facility salary was based on air traffic complexity, so Manchester controllers had moved in at the Boston salary without being able to yet work the more difficult workspace. For all these reasons, resentment, conflict and dissonance were built in from the start, impeding the coordination so essential to their task. Moreover, once the training began, Boston controllers easily mastered the Manchester airspace, but the first two Manchester controllers failed early. Everyone was devastated. Some senior controllers retired early.

3.1   System Effects and Repair: How the Past Affects the Present

The Boston TRACON bore the official responsibility for integrating the airspace and training the Manchester controllers. However, Boston controllers also felt a moral responsibility to join the two facilities by reproducing the unique culture of collective responsibility that had typified their own workplace prior to relocating: pride in the accomplishment of group over the individual; looking out for one another. That was not only what they wanted for themselves and for Manchester but for the safe operation of the facility. Drawing on the expertise acquired since legally empowered by Clinton to have input into all organizational and technological innovations, they improvised, engaging in new forms of boundary work to repair the physical, social, technological, status, and cultural boundaries in the facility. Their primary goal was to rectify the inequalities in the facility.

The resulting effort reveals heterarchy in action, demonstrating the benefits of disruptive dissonance for discovery and change (Beunza & Stark, 2011). Collectively, facility managers, NATCA representatives, and several controllers from both Manchester and Boston — all with different points of view — formed a "Cooperative Work Group." Not so cooperative at the start, they worked through differences to develop a general plan. They began with the physical and technological fixes, implemented with the help of FAA architects and technical people. First, the Work Group redesigned the Inner Circle, keeping its position in the center of the Control Room, but splitting it into two smaller circles, each with four exits so people could get to all parts of the Control Room quickly.

To rectify inequalities and status dynamics, the group divided the Outer Circle airspace into two parts, "Boston North" and "Boston South." Some airspace sectors would be co-owned (jointly worked by controllers from both facilities) while other sectors would belong to each. Salary would match the complexity skill level attained, so Manchester controllers could opt to stay at their original airspace or work up. Finally, to "fully integrate" the separate cultures of the two facilities called for a *common cultural system of knowledge and material practices acquired only by being there*. Transforming culture was a long-term project, involving daily training and retraining of both former and new generations of controllers by those senior controllers already there. It was in the form of ongoing talking and teaching both while working traffic and off

position, often corrective and dissonant, demonstrating "This is the way we do it here." The effort was formalized: the Collaborative Work Group wrote and everyone approved and engaged in "The Five Core Values of PULSE: A Unifying Code of Moral Conduct." Originally an experiment, the Boston Consolidated TRACON became a prototype for other planned consolidated facilities that combined small and large TRACONs.

4 Conclusions

The purpose of this cross-case comparison has been to expand upon what is known about systemic failure in large socio-technical systems by exploring why, given two organizations doing similar tasks under similarly challenging institutional constraints — primarily, insufficient funding — one has produced catastrophic failures, while the other has been able to main safe operations, avoiding catastrophe. The research not only has policy relevance, but also contributes to what is known about institutional persistence, change and agency.

In common, both NASA and Air Traffic Control engaged in dead reckoning: not only were they predicting the position of airplanes and shuttles in time and space by deduction, without benefit of direct observation or direct evidence, but they also were predicting the position of their socio-technical systems in time and space in order to carry out their missions successfully. The comparison reveals system effects: how conditions, actors, and actions originating in the institutional environment impacted both organizational systems, changing them, and how those changes consequently had unanticipated consequences for the workplace, its technologies, the tasks and the interpretation, meanings and actions of the people who work there.

The cross-case comparative historical ethnographies of the two agencies reveal system effects: how historic conditions, actors, and actions originating in the institutional environment affected the organizational systems, changing them, and as a consequence changing the workplace, technologies, the tasks, and so affecting the actions and reactions of the people who work there. We can see how history manifested in the present. Both were underfunded by Congress. NASA's Shuttle Program had no secure budget to start, leading to payloads, then to operating more like a business, complete with contractors, bureaucratic hierarchy, and production pressure. We saw those factors affected decision-making on the eve of the *Challenger* launch decision and then repeated during *Columbia's* post-launch crisis meeting. Also chronically underfunded, Air Traffic Control developed a system on the ground that was worked by people with the same job, the same training, with the task of coordination action across the boundaries of the system that produced internal pockets of heterarchy: conflict, dissonance, and collaboration were built into the system. Given lack of staffing, aging facilities and equipment, and standardized changes, controllers began improvising local repair to make the system work. In 1991 legally empowered by Clinton, controllers applied their developed expertise to the unanticipated consequences of technological and organizational innovation, making repairs, supplying the resilience that kept the system working.

In addition, the data provide a rare look at decision making in daily routine and in crisis in the workplace. We see system effects on ethnocognition and agency in both places: how organization structures, cultural difference, and micro-level processes affect people in a particular time in place, acquiring shared cultural systems of knowledge and understandings that are enacted in responses consistent with their training and history, producing unanticipated consequences, both positive and negative. When risk increased, the NASA case reveals the connection between hierarchy, dis-empowered engineers, and ineffective change, so failure repeats; and in contrast, air traffic control shows heterarchy, empowered air traffic controllers; repair

and resilience. The comparison shows that choice is not simply an output of structure, but an input to the system as a whole.

The view from inside the workplace reveals the internal contradictions between past, present and future that plague modern organizations (Vaughan, 2021). We can think of all complex organizational systems as engaged in dead reckoning and vulnerable to unanticipated consequences due to history, external factors and actors, and technological and organization complexity. Drawing from this analysis, system effects will produce:

- Difficulty predicting the effects of system change on intra-organization structure, culture, cognition, meaning making, and everyday work practice.

- Liabilities of technological and organizational innovation.

- Problems modernizing, patching the new onto the old.

- Inability of insiders and outsiders to identify systemic causes in order to prevent repeat failures.

- Tensions between standardization and the need to customize to local conditions.

- Deterioration of experiential skills from automation.

- The potential role of workers in initiating change and repair that supply resilience to an organizational system.

We know a lot about failure, but less about repair and resilience and the larger issues of institutional persistence, change, and agency. The findings are a warning about the vulnerabilities of organizational systems and the contingencies that impact the work place. Equally as important, the air traffic control example shows the kinds of problem-solving solutions that worked over time and the importance of people, not just in crisis, but in daily routine. Across time and change, both cases expose the capacity and opportunity for the workforce — the people doing the hands-on technical work — to have input both in system change and repair. In all organizations, skills and expertise are acquired through socialization, but expertise is only developed by being there and understanding not only how the parts of a place work, but the social, cultural, and technical aspects of its tasks. Regardless of differences in organization size, complexity, and function, workers who know well the work and the workplace can participate in collaborative decision making and design of organizational and technological innovations and then upon arrival, implementation and/or improvising tools of repair, making adjustments after the fact.

References

Beunza, D., & Stark, D. (2003). The Organization of Responsiveness: Innovation and Recovery in the Trading Rooms of Lower Manhattan. *Socio-Economic Review*, *1*(2), 135–164. https://doi.org/10.1093/soceco/1.2.135

Beunza, D., & Stark, D. (2004). Tools of the Trade: The Socio-Technology of Arbitrage in a Wall Street Trading Room. *Industrial and Corporate Change*, *13*(2), 369–400. https://doi.org/10.1093/icc/dth015

Beunza, D., & Stark, D. (2011). Seeing Through the Eyes of Others: Dissonance Within and Across Trading Rooms. In K. Knorr Cetina & A. Preda (Eds.), *The Oxford Handbook of the Sociology of Finance* (pp. 203–221). Oxford: Oxford University Press.

Burawoy, M. (1982). *Manufacturing Consent: Changes in the Labor Process Under Monopoly Capitalism*. Chicago, IL: University of Chicago Press.

Columbia Accident Investigation Board Report. (2003). *U.S. Independent Agencies and Commission*, Vol. I. Washington, D.C.

Deener, A. (2020). *The Problem with Feeding Cities: The Social Transformation of Infrastructure, Abundance, and Inequality in America*. Chicago, IL: University of Chicago Press.

DiMaggio, P. (1988). Interest and Agency in Institutional Theory. In L.G. Zucker (Ed.), *Research on Institutional Patterns: Environment and Culture* (pp. 3–21). Cambridge, MA: Ballinger.

DiMaggio, P.J., & Powell, W.W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, *48*(2), 147–160. https://doi.org/10.2307/2095101

Erikson, K., & Peek, L. (2022). *The Continuing Storm: Learning from Katrina*. Austin, TX: University of Texas Press.

Geertz, C. (1983). *Local Knowledge: Further Essays in Interpretive Anthropology*. New York, NY: Basic Books.

Hughes, T.P. (1979). The Electrification of America: The System Builders. *Technology and Culture*, *20*(1), 124–161. https://doi.org/10.2307/3103115

Hughes, T.P. (1993). *Networks of Power: Electrification in Western Society 1880–1930*. Baltimore, MD: Johns Hopkins University Press.

Hutchins, E.A. (1995). How a Cockpit Remembers its Speeds. *Cognitive Science*, *19*(3), 265–288. https://doi.org/10.1016/0364-0213(95)90020-9

Jervis, R. (1997). *System Effects: Complexity in Political and Social Life*. Princeton, NJ: Princeton University Press. https://doi.org/10.1515/9781400822409

Le Coze, J.C. (2021). A Broad (Multi-Level) Safety Research and Strategy: A Sociological Study. *Safety Science*, *136*, 105132. https://doi.org/10.1016/j.ssci.2020.105132

Lounsbury, M. & Hirsch, P. (Eds.) (2010). *Markets on Trial: The Economic Sociology of the U.S. Financial Crisis: Part B*. Leeds: Emerald.

Mahoney, J., & Thelen, K. (Eds.) (2010). *Explaining Institutional Change: Ambiguity, Agency, and Power*. New York, NY: Cambridge University Press.

MacKenzie, D. (2011). The Credit Crisis as a Problem in the Sociology of Knowledge. *American Journal of Sociology*, *116*(6), 1778–1841. https://doi.org/10.1086/659639

Merton, R.K. (1936). The Unanticipated Consequences of Social Action. *American Sociological Review*, *1*(6), 894–904. https://doi.org/10.2307/2084615

Perrow, C.B. (1984). *Normal Accidents: Living with High-Risk Technologies*. New York, NY: Basic Books.

Pinch, T., & Bijker, W. (1984). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and Technology Might Benefit Each Other. *Social Studies of Science*, *14*(3), 399–441. https://doi.org/10.1177/030631284014003004

Rilinger, G. (2021). *The Organizational Roots of Market Design Failure: Structural Abstraction, the Limits of Hierarchy, and the California Energy Crisis of 2000–2001*. (MPIfG Discussion Paper No. 21/6). Max Planck Institute for the Study of Societies, Cologne. https://hdl.handle.net/21.11116/0000-0009-8D53-B

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

Snook, S. (1996). *Practical Drift: The Friendly Fire Shootdown over Northern Iraq*. Cambridge, MA: Harvard University Press.

Stark, D. (1999). Heterarchy: Distributing Intelligence and Organizing Diversity. In J.H. Clippinger III (Ed.), *The Biology of Business: Decoding the Natural Laws of Enterprise* (pp. 153–179). Hoboken, NJ: Jossey-Bass.

Stark, D.C. (2011). *The Sense of Dissonance: Accounts of Worth in Economic Life*. Princeton, NJ: Princeton University Press.

Suchman, L. (1997). Centers of Coordination: A Case and Some Themes. In L.B. Resnick, R. Säljö, C. Pontecorvo, & B. Burge (Eds.), *Discourse, Tools, and Reasoning: Essays on Situated Cognition* (pp. 41–62). Berlin: Springer. https://doi.org/10.1007/978-3-662-03362-3_3

Turner, B.A. (1978). *Man-Made Disasters*. London: Wykeham.

Vaughan, D. (1983). *Controlling Unlawful Organizational Behavior: Social Structure and Corporate Misconduct*. Chicago, IL: University of Chicago Press.

Vaughan, D. (1996). *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. Chicago, IL: University of Chicago Press.

Vaughan, D. (1997). The Trickle-Down Effect: Policy Decisions, Risky Work, and the *Challenger* Tragedy. *California Management Review*, *39*(2), 80–102. https://doi.org/10.2307/41165888

Vaughan, D. (1999). The Dark Side of Organizations: Mistake, Misconduct, and Disaster. *Annual Review of Sociology*, *25*(1), 271–305. https://doi.org/10.1146/annurev.soc.25.1.271

Vaughan, D. (2004). Theorizing Disaster: Analogy, Historical Ethnography, and the Challenger Accident. *Ethnography*, *5*(30), 313–345. https://doi.org/10.1177/1466138104045659

Vaughan, D. (2014). Theorizing: Analogy, Cases, and Comparative Social Organization. In R. Swedberg (Ed.), *Theorizing in Social Science* (pp. 61–84). Stanford, CA: Stanford University Press.

Vaughan, D. (2021). *Dead Reckoning: Air Traffic Control, System Effects, and Risk*. Chicago, IL: University of Chicago Press.

Weick, K.E. (1993). The Collapse of Sensemaking in Organizations: The Mann-Gulch Disaster. *Administrative Science Quarterly*, *38*(4), 628–652. https://doi.org/10.2307/2393339

Diane Vaughan – Department of Sociology, Columbia University (United States)
✉ dv2146@columbia.edu
⇱ https://sociology.columbia.edu/content/diane-vaughan
Diane Vaughan, Professor of Sociology at Columbia University (USA), has written three books on how things go wrong in organizations: *Controlling Unlawful Organizational Behavior* (The University of Chicago Press, 1985), *Uncoupling* (Doubleday, 1990), and *The Challenger Launch Decision* (The University of Chicago Press, 2015). The fourth book, *Dead Reckoning: Air Traffic Control, System Effects, and Risk* (The University of Chicago Press, 2021) is her negative case, looking at how the air traffic control system gets it (mostly) right. Currently she is writing *Theorizing: Analogy, Cases, and Comparative Social Organization*.