Basic Flaws in Vaughan's Analysis of the *Challenger* Accident

Frederick F. Lighthall

Cite as: Lighthall, F. F. 2014, Basic flaws in Vaughan's analysis of the *Challenger* accident. www.high-techdanger.net

Diane Vaughan's (1996) widely cited analysis of the causes of the *Challenger* accident makes six serious errors. Vaughan's errors in interpreting the *technical* dynamics that caused the accident rendered inaccurate her analysis of the *human* failures that caused the accident.

Vaughan assumed that the best form of explanation of the process that produced the disaster would be a continuous, cumulative cause rather than a discontinuous, suddenly emerging cause precipitating the disaster. Second, she considered *design specifications* of the shuttle's components to be the only legitimate criteria of safe shuttle functioning – despite the fact that those specifications were written before the shuttle was built, before its flight complications could be known. Any deviation ("anomalies") in actual flight performance from those specifications Vaughan viewed as ipso facto dangerous. Therefore, any empirical tests engineers conducted showing as harmless a particular deviation from design that occurred on several occasions -- particularly one form of *O-ring erosion* ("impingement" erosion) -- constituted a dangerous "normalization of deviance." NASA's and Morton Thiokol's repeated framing of that deviating anomaly as safe -- thus "normalizing" the supposedly dangerous anomaly -- played a crucial role, according to Vaughan, in causing the disaster.

Third, Vaughan mistakenly assumed that it was *erosion* of O-rings in a booster joint that caused the O-rings to fail to seal the joint. Fourth, Vaughan misread a central table of engineering data, interpreting the effect of cold temperature as making the O-rings *harder* therefore slower to seal and so subject to a fatal amount of *erosion*. This dynamic was present, but negligible in relation to the dynamics that actually caused the failure. Vaughan missed the actual, more complicated dynamic of cold temperature and its effect on the sealing shape of the O-ring. Fifth, Vaughan argued that the engineers and managers involved in the launch decision violated no norms; instead they conformed to all norms of decision making and safety. Finally, Vaughan's analysis failed crucially to include the definitive post-accident evidence and analysis of the physical causes of the accident, results of two independent studies showing that cold O-rings without erosion failed to seal booster joints.

Vaughan's misdiagnosis of the physical failure as caused by O-ring erosion led her down the false path of discovering the many institutional, organizational, and individual forces that caused the engineers and managers to accept O-ring erosion. Having missed the actual physical cause, Vaughan missed altogether the individual and group failings, complex situations, inter-role slippages, linguistic confusions, dominating styles of leadership, processes of communication and persuasion, decision rules, and market forces that combined to cause the fatal decision. The interplay of those forces caused decision makers to resist the correct, specific, and advance warnings of expert engineers, warnings resisted on the basis of spurious reasons arrived at under demanding conditions and shaped by biasing preoccupations that combined to produce the *Challenger* disaster. [1]

Diane Vaughan's (1996) idea that engineers and managers dangerously "normalized" the effects of hot gas on O-rings and her analysis of the crucial power of organizational culture to shape thought has become so influential, so accepted as the way to understand the *Challenger* accident,[2] that when another malfunction destroyed the space shuttle *Columbia* seventeen years later, the official board investigating the *Columbia* accident adopted as their own the discourse, concepts, and framing Vaughan used in her analysis of the *Challenger* accident. [3]

Because Vaughan's analysis of the *Challenger* accident is flawed in each of the six central ways I have listed, it is important that these be pointed out simply as a matter of advancing knowledge about the *Challenger* accident in particular as well as the later *Columbia* disaster and, more generally, advancing our knowledge of how in situ, naturalistic deliberation and decision making can go wrong in high-tech organizations. [4]

It is all the more important to make these shortcomings explicit when the flawed analysis has continued (Vaughan, 2005) and has become so influential as to become not only conventional wisdom about shuttle accidents but also the basis for future corrective and preventative efforts. [5]

However, while my own analysis of the disaster and of its still current lessons (Lighthall, 2015) is at odds with Vaughan's on these six important points, I can only build on other strengths of her research. One marvelous contribution of Vaughan's analysis is her detailed examination and narrative of how the Thiokol engineers examined the boosters' performance deviations from initial design ("anomalies") like O-ring impingement erosion and brief gas leakage, to determine their source, limits, and likelihood (Vaughan, 1996, 110-112). While Vaughan's intent in this analysis is to show how these anomalies became accepted ("normalized") as harmless – in her view a grave error by allowing deviations from design that she regarded as dangerous to be accepted as safe – her detailed description of the engineers' process of defining, systematically measuring, and understanding the anomalies' dynamics reveals the process by which the supposedly dangerous anomalies were actually shown empirically and correctly to be safe. It shows nicely how engineering practice protects safety.

Vaughan's book about the *Challenger* accident introduces into disaster analysis important perspectives from the social sciences -- particularly the force of institutional and organizational structures, norms, and procedures. She argues that social science perspectives must be brought to the analysis of disasters, particularly the idea that organizational and institutional structures, norms, and procedures constitute a crucial part of the train of cause-effect events.

With that door thus opened for social science perspectives, we must step through it prepared to probe a wider range of dimensions, with a broader and deeper penetration of data, and with a broader selection of analytical tools provided by the integrative perspectives of ergonomics, specifically macro-ergonomics, and the other social sciences.

The Train of Cause-Effect Events

To understand how we might reduce the likelihood of such accidents in the future, we must understand more than the first- and second-order causes, that is, more than the physical part that failed and the physical and dynamic causes of the accident. On that point Vaughan and I agree. However, those first- and second-order causes must be our foundation, our starting point. If we get either of those wrong, all the rest of our explanation will be wrong, since we will then end up explaining how the misidentified supposed physical cause arose from faulty human assessments of it. We will then miss entirely the actual human causes (the third- and fourth-order causes of miscalculating the actual first- and second-order causes) that led to missing the real physical causes. Accepting a misdiagnosed cause is like convicting the innocent and allowing the real criminal freedom to perpetrate more crime. In matters of cause, as in crime, we must convict the guilty culprit.

To then understand how the real physical failures in the vulnerable booster *were allowed* to arise, we need to proceed to the mental and social processes that took the individual and collective minds down the wrong paths in deliberating about them, the third-order causes. Vaughan's attention to the engineers and managers' thinking was *strategically* sound. We cannot reach full understanding of an accident, or full opportunity to correct its causes, until we understand the participants' perceptions, interpretations, and deliberations. Finally, we must come to understand the fourth-order causes, the conditions that gave rise to and sustained the failed deliberations—the organizational, professional, institutional, and cultural forces.

Some accidents are caused by conditions and forces so complicated that no participant on earth could understand the causes before the accident. These accidents have been called "normal accidents" (Perrow, 1984), normal because they must be expected in complex, high-technology engineering creations that entail causes beyond all (prior) understanding. Vaughan (1996, p. 415) considered the *Challenger* accident "normal" in this sense, not preventable because of its causal complexity. Contrasted with "normal" accidents are the preventable accidents. Those are accidents whose decision participants might have correctly perceived and avoided the dangers if they had engaged in deliberations well within their mental capacities. Or the accident could have been avoided if they had followed procedures otherwise available to them but were prevented from doing so by blocking or distracting factors (motives, habits, conditions, conflicts, pressures, gaps in skills or knowledge), factors that prevented those capacities and procedures from being activated. Both the *Challenger* accident and later, the loss of *Columbia's crew,* were of this preventable kind.

The Structure of Cause-Effect Analysis

The cumulative sequence of cause-effect events producing an accident can be thought of as having roughly five categories of constraining events, besides the accident itself, as schematized

Figure 1.3 Examining Successive Constraints of Cause-Effect Events

F ⇒	E ⇒	D ⇒	C ⇒	B ⇒	A: The Effect
Institutional and wider cultural forces, processes, structures, and norms as limiting and shaping organizational culture, structures, and processes	Social-organizational culture, norms, structures, procedures, and training that limit and shape situations and deliberations	Situational demands and participants' subjective definitions of their situations as they deliberate	Individual and collective deliberations, and possibly arguments, by participants about risky and safe functioning	Physical-chemical conditions and forces: the site and dynamic causes of failed technological functioning	The accident
Cultural Setting	⇐Trace Backward	⇐Trace Backward	⇐Trace Backward	⇐Trace Backward	⇐Trace Backward

Figure 1.3 presents a sketch of how an accident becomes triggered by layers of remote causes, from earlier deliberations about risky and safe functioning to a succession of distant and nearer conditions and forces that shape those deliberations. The top row shows the direction of cumulating constraints ending in the accident. The middle row of text describes the layers of substantive constraints. The bottom row reminds us that a complete tracing of the cause moves backward in time through each successive layer of constraints from first- and second-order causes (B) to third-order causes (C and D) and finally fourth-order causes (E and F).

in figure 1.3.[6] The top row shows the accumulation of constraining events from the macro level of institution and culture (F) to the micro level of individuals (C) and the immediate physical failure (B) triggering the accident.

While the idea of a cumulative series of successively shaping and constraining events is important, the human causes in such accidents are not simply unidirectional or irreversible. At certain points actual events can, at any level, deflect direction, cumulativity, or reversibly. The first *Challenger* launch decision, [7] in fact, exhibited a dramatic reversal of direction—from a group of engineers recommending a delay of the shuttle's launch to a reversal of that recommendation -- due principally to the powerful intervention of two managers -- and then the acquiescence in that reversal by all participants, including the engineers in the original group. The progress of collective decision thinking can be tortuous.

The middle row of figure 1.3 describes categories of constraining events and conditions at various levels of social complexity. Each level on the left sets constraints on conditions and events on its right, at the next lower level of social complexity. By "sets constraints," I mean to indicate something less controlling than "shapes" and certainly not "determines," but rather more like "presents somewhat limited possibilities that help to shape" events and conditions at the next lower level of social complexity. Thus, organizational norms, at level E, present limited conditions from which participants define their situations at level D, which in turn shape deliberations at level C. Selection among possibilities is an interactive affair among the interplaying forces at each level, including selection explicitly negotiated or unwittingly adopted by the participants.

The third row of figure 1.3 shifts attention away from causal forces and participants themselves, taking instead the perspective of the analyst who, after the accident, tries to understand the train of causal events. The analyst starts at the end of the cause-effect sequence and works backward, from determining the immediate physical cause to the human action that allowed those physical causes to operate freely. Of course, the actual temporal order in which the analyst investigates events will usually not follow the arrows linearly. Yet to approach a full understanding of an accident's causes, all five of these levels of constraining conditions must be probed.

Analytical Choices: Two Modes of Explaining the Cause of a Sudden New Event

Consider now a choice any analyst of an accident must make, consciously or unwittingly. To explain a sudden shift in a trajectory of events, for example, the shift from a string of successful space launches and flights to a shuttle disaster, the analyst must adopt one or some mixture of two fundamental explanatory modes. One mode sees the cause of the sudden shift in events as present all along, hidden, gradually growing by small increments until a breaking point is reached. An example from government would be where small increments of police powers over time accumulate such power that at some critical point they transform a democratic country into a dictatorship. Or, small increments in taxes over time can become sufficiently burdensome to cause drastic economic reform. Each increment builds on, expands the domain of action beyond the previous increment. This is the mode of *continuous cause.* This mode is expressed in the vernacular as the straw that broke the camel's back, history as cause, the slippery slope to disaster, the early wrong decision point starting down the long path to catastrophe.

The second explanatory mode sees the cause of the sudden shift in events as emerging suddenly. In this explanation, the cause of the shift is absent from a trajectory of events leading up to the shift. It arises just before the shift to cause it. For example, several brands of multivitamin are taken by a person over time with no change in digestion. Then a new brand is taken with a large increment of iron and niacin, leading to sudden attacks of indigestion. This is the mode of *sudden, discontinuous cause*—no straw accumulating on the camel's back, no slippery slope, but a sudden shift in causal events triggering a sudden new event.

To show that one or the other of these two explanatory modes best accounts for an actual shift in events, evidence and argument of two contrasting kinds are required. To show that the continuous causal mode provides the best explanation, one must both refute the discontinuous explanation and also provide evidence that the cause in question a) was active continually during the normal trajectory of events before the shift, b) did in fact increase cumulatively in force during the trajectory of events leading to the shift, and c) was sufficient, itself, to trigger the sudden shift in events. To show that the discontinuous causal mode best explains the shift in event trajectory, one must both refute the continuous explanation and also provide evidence that the cause in question a) was absent in the normal course of events leading up to the event, b) appeared in evidence just before the event, and c) was itself sufficient to trigger the sudden shift.

A Précis of Vaughan's Analysis

Vaughan (1996, p. 125) identifies the core of the supposedly fatal practice of normalizing deviance: "Official act indicating the normalization of deviance: accepting risk." By reasoning backwards from her interpretation of the physical cause of the *Challenger* accident, eroded booster O-rings that failed to seal a joint against hot exhaust gas, Vaughan examines the social, organizational, and cultural processes that led the work group of engineers and managers to accept O-ring erosion as safe. To accept erosion of O-rings was to accept dangerous risk.[8]

The core of her argument about the work group's dangerous mental slippage is that by continually allowing ("normalizing") performance deviations in the boosters' joints – a deviation from original design specifications, like erosion of O-rings -- they accepted more risk. Tests and analysis showing each instance of erosion to be "acceptable" were deceiving, she argues, but false confidence in the deviations as safe was supported by continued safe shuttle flights. Once the work group had now confidently accepted the deviations, each as "proven" safe, they had no criteria or procedures that limited the further acceptance of deviations and "acceptable" risk. Each newly accepted deviation (e.g., O-ring erosion) and each new test showing it to be "acceptable" actually added more risk. This trajectory into danger, Vaughan argues, led the engineers and managers finally to allow the fatal risk, disastrous erosion of O-rings.

From post-accident evidence of massive erosion in the failed field joint Vaughan (and much of the Commission's own language) identified O-ring erosion as the cause of the joint's failure, and thus the physical cause of the *Challenger's* destruction. [9] (Both Vaughan and presidential commission analysts thus committed the well-known fallacy, *post hoc ergo propter hoc*. Seeing massive erosion after the accident they then reasoned, therefore, that erosion must have been the cause.) Reasoning backwards from erosion as the physical cause, Vaughan discovered the many human causes that led to that physical cause – all normal and beyond anyone's capacity to prevent. Or so it appeared to

Vaughan.

That appearance, however, is false. O-rings did fail to seal the aft joint of *Challenger's* right-hand booster, and that failure was the immediate cause of the disaster. Further, those O-rings did become eroded, along with the booster's steel casing, eroded by the booster's hot gases escaping through the joint. But erosion itself was caused by another dynamic missed by Vaughan, a dynamic rather more intricate.

The Actual Physical Cause

The physical cause of the accident was not O-ring erosion, but the very different dynamic of O-ring temperature. That difference in identifying the physical cause of the shuttle failure, between O-ring erosion and O-ring temperature, is not a matter of mere engineering quibbling. Vaughan's tracing as supposedly dangerous the forces and decisions that led *Challenger's* engineers and managers to accept O-ring *erosion* as safe, their "normalization of deviance," led her to concentrate on forces and decisions that in fact were not dangerous, forces and decisions having little or nothing to do with the *actual* danger, the danger engineers tried to warn about the evening before the accident, namely O-ring *temperature*, which they knew at launch time would be 29°F, much colder than ever before.

Eroded O-rings were an effect, not a cause. In fact the kind of O-ring erosion that the engineers and managers "accepted" (i.e., impingement erosion) never came near to causing any joint to fail. Understanding that there were *two distinct kinds of erosion* is crucial to understanding the physical cause, and crucial therefore to understanding the social, organizational, cultural and market processes that led the work group of engineers and managers to accept *one kind of* O-ring erosion as safe.

The physical cause of the *Challenger* disaster was not impingement erosion, as Vaughan's analysis assumed. Rather, the disastrous erosion itself, erosion from hot gas blowing *past* an O-ring *("blow-by erosion"* or *"by-pass erosion"),* was an *effect*, caused by the unexpected appearance of cold weather creating the actual physical cause, cold, unresponsive, flattened ("squeezed") O-rings that had become structurally incapable of sealing their joint. Vaughan's attention to how the engineers and managers responded to impingement erosion misconstrued the physical source of danger. As a consequence she missed the human processes and dynamics, and the mistaken paths of deliberation, by which the disaster was actually caused.

It is the contents, course, and pitfalls of deliberation about O-ring *temperature* as cause that we must understand in order to diagnose the flawed causal deliberations in this disaster. The thinking that participants exhibited about impingement erosion and other factors must figure in our inquiry, but only as thought-paths offering context rather than as addressing the human cause of the boosters' failure – the human social, political, and organizational dynamics that prevented expert engineers' warnings from being grasped and believed.

Some Technical Background

Vaughan's analysis, which adopts the continuous mode of explanation, does not fit the actual trajectory of events. To understand those events several pages of technical background will be necessary, providing information about the boosters' field joints, the three joints of each booster created when the four long cylindrical segments of each booster’s motor were assembled and stacked on top of each other at Kennedy Space Center in Florida.

The universally agreed-upon immediate physical cause of the accident was failure of the aft joint of the right solid-fuel booster. Since the technological causes of the accident could have been avoided, *it was the very human pre-launch debate about those technical dynamics that actually allowed the accident to happen.* The debate focused principally on the boosters’ field joint dynamics before and after ignition, a debate shaped by emotional commitments but carried on in very technical terms. The debate cannot be understood without this technical background. It entails understanding the physical contours and positioning of the boosters’ field joints, what happens to the joint when the booster is ignited, and rates of change within the joint. To convey these to readers requires diagrams, charts, and descriptions of them that I hope to make easy to understand by presenting the technical complications in three steps.

Step 1. The joints between booster segments. One of the O-rings’ dynamics that was understood by the engineers issuing the cold-O-ring warning was that typical, warm O-rings recapture most of their normal size and shape when they are released after being squeezed. They are *resilient*, recovering from their squeezed condition as the joint opens from ignition pressure. Two dynamics that the engineers expert in field joint dynamics also understood, but which the two key decision makers (and Vaughan) did not understand (discussed below) were 1) that cold O-rings lose resiliency (their capacity to regain their size and shape after being released from their “squeezed” condition in the joint) and *very* cold O-rings lose virtually all of their resiliency and 2) that O-ring resiliency was an O-ring property absolutely fundamental to its capacity to seal its joint when the joint opened, milliseconds after booster ignition.

For readers to understand these two dynamics and the associated change in O-ring shape requires knowing how the O-rings became positioned and shaped when the boosters were first assembled. The four cylindrical segments of each booster were fueled with solid propellant and sent by rail from Utah to Florida. They were stacked on top of each other at the Kennedy Space Center to create a complete booster. Figure 2.3 shows how segments were joined. Between each segment a tongue-in-groove joint was created, shown in the magnified circle of Fig. 2.3. The U-shaped lip of the booster segment (e.g., an Aft Segment) that receives another booster segment (e.g., an Aft Center Segment) stacked on top of it formed a joint between the segments called a field joint. That joint always contained a gap between the two segments being joined, and that gap in each of the six field joints (three joint gaps in each booster) had to be sealed by one of two rubber-like O-rings. Like the washer in the connection of a garden hose when the hose is screwed tight to the water faucet, the O- rings were squeezed into the gap to seal it against leakage.

Step 2. Details of the field joint and O-ring sealing. If we “zoomed in” on the circled detail of figure 2.3 we would see the up-close view of each field joint as in figure 3.3. Note the positions of the O-rings in their grooves, which circled the entire 39-foot, inside surface of the booster joint. The depiction of the primary and secondary O-rings in Fig. 3.3 is in one respect misleading, however. It shows the O-rings’ cross section as only very slightly squeezed between the tang and clevis. The O-rings varied in their degree of squeeze, but generally would be flatter than indicated in Fig. 3.3.

Notice in Fig. 3.3 the layer of putty that was inserted into each joint’ gap. To test

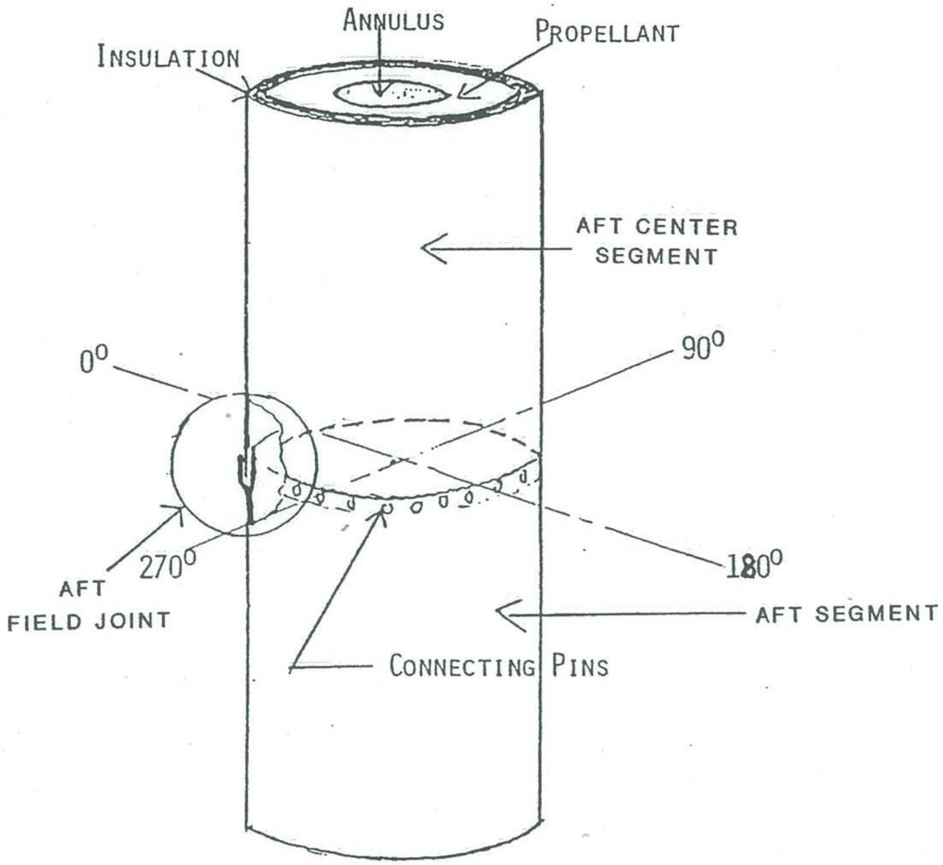


Figure 2.3. The right booster's aft field joint, with magnified view showing the tongue-in-groove ("tang"-in-"clevis") joining of the field joints.

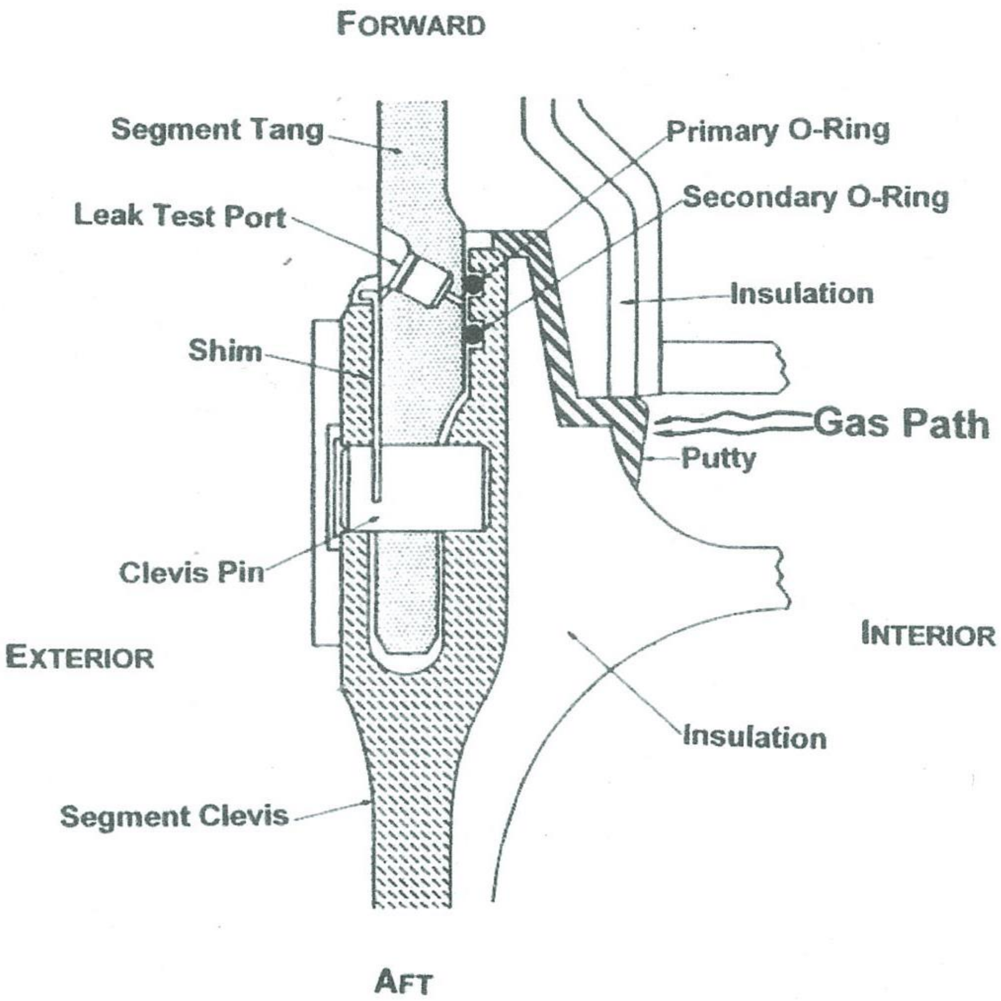


Figure 3.3. The field joint in detail, indicating the positions of the primary and secondary O-rings and the potential for a gas path through the joint's protective putty.

the tight sealing of the joints at the time the boosters were assembled ("stacked"), testing especially the sealing capacity of the O-rings, air was forced into the space between the primary and secondary O-ring through the Leak Test Port (Fig. 3.3). Before the primary O-ring could seal the upstream gap nearest to the putty some air from the leak test could pass the primary O-ring and press into the putty itself. At any point around the 39-foot O-ring the putty that protected the primary O-ring could thus experience air pockets, formed unpredictably.[10]

Those air "bubbles" could form, again unpredictably, small indentations into the putty or could reach almost all the way through it. Occasionally, the air forming the putty bubble could be forced all the way through, creating a pathway that breeched the putty completely, providing a "blow-hole" through which the hot gas from later ignition at launch could reach the O-ring itself. That blow hole would then constitute an open path or tunnel (see Fig. 3.3) through which hot gas from ignited boosters could break through and impinge directly on the primary O-ring.

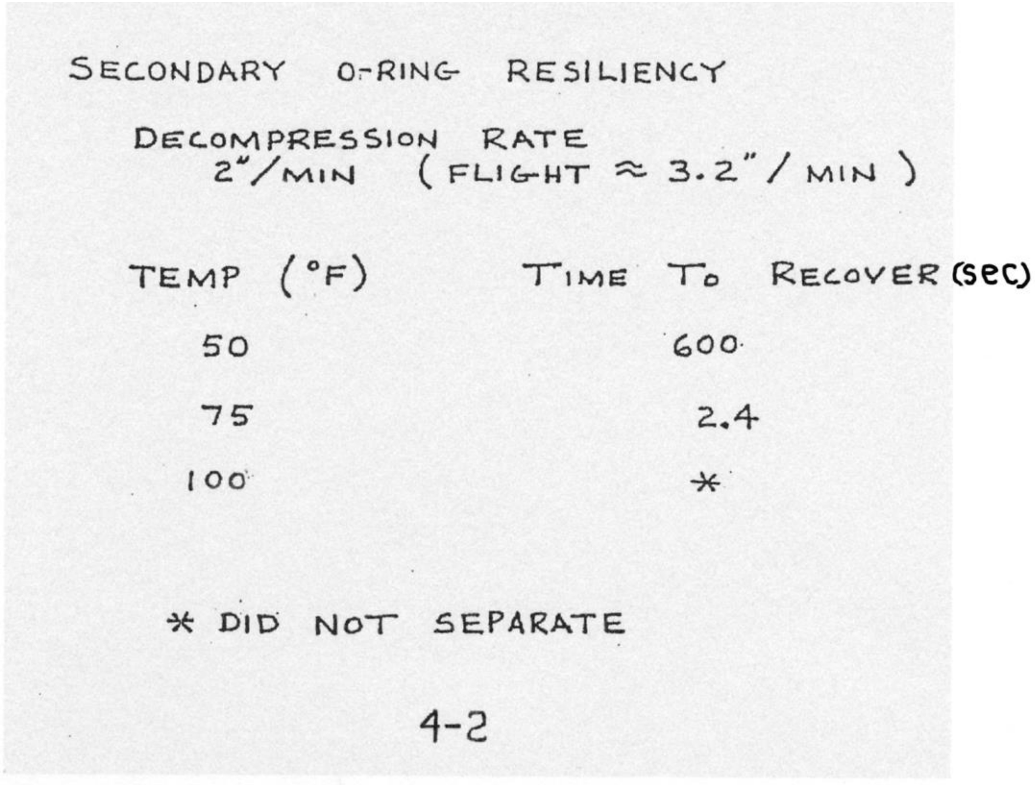
When the boosters were ignited the field joints opened, suddenly increasing the gap. The O-ring nearest to the inside of the booster (nearest to the hot gas from ignition), the primary O-ring, being normally pliant (or "resilient"), would respond to being released from its partly squeezed, flattened state when the joint opened. Upon being released from its squeeze, the normally resilient O-ring would expand and recapture most of its normal (and essential) round size and shape.

Step 3. O-ring temperature dynamics. The added dynamic of O-ring temperature must now be added to understand how the unusually cold O-rings of the *Challenger's* right-hand aft field joint failed to seal that joint. Cold temperatures made O-rings hard and less “resilient,” less able to recover their sealing size and shape. When the joint opened up under ignition pressure the cold O-rings, now released from their squeeze, only sluggishly recovered some of their sealing size and shape. The secondary O-ring, also cold, squeezed, and sluggishly recovering, allowed the now opening joint to *remain* open.[11] The booster’s escaping hot gas continued the chain of events resulting in the destruction of *Challenger* and the deaths of its seven crew members.

All of these engineering details, remember, are what the decision-making managers (and Vaughan) got wrong. It is the processes that prevented those managers from getting it right that still had to be investigated since Vaughan’s account failed to focus on the individual motives and situations that prevented managers from understanding the dynamics of temperature and O-ring resilience. Now consider O-ring temperature dynamics in more detail, by considering the kind of evidence that made the Thiokol engineers worried.

Thiokol’s Thompson and Boisjoly had run an experiment investigating the impact of O-ring temperature on O-rings’ capacity to recover their size and shape when released from their squeezed condition in a field joint. The question was, did O-ring *temperature* have any important effect on the speed with which the O-ring could re-capture its normal sealing size? Did temperature, in other words, affect O-ring resiliency? Figure 4.3 depicts one of Thiokol’s 13 charts presented to NASA managers in a teleconference the evening before *Challenger* was launched. It presents the results of Thompson’s and Boisjoly’s experiment investigating the effects of O-ring temperature on the time it took for the O-ring to seal the field joint’s gap.

O-rings had been “soaked” to three temperatures, 100 °F, 75 °F, and 50 °F. Each



SECONDARY O-RING RESILIENCY

DECOMPRESSION RATE
2"/MIN (FLIGHT ≈ 3.2"/MIN)

TEMP (°F)	TIME TO RECOVER (sec)
50	600
75	2.4
100	*

* DID NOT SEPARATE

4-2

Figure 4.3. Thiokol's chart 4-2 and Vaughan's figure 11.8, p. 296 reporting the results of Thompson's experiment testing the relation between O-ring temperature and time taken by the O-ring to seal its simulated field joint. It shows O-ring temperature's strong influence on the O-ring's speed of sealing its joint.

in turn was inserted in an apparatus that would simulate the booster's joint dynamics as the joint's gap changed from its pre-ignition static state to its slightly more open condition (0.042 to 0.060 inches) triggered by booster ignition. That "transient" period, from closed gap to open, lasted only 0.6 seconds. Just 0.17 seconds into that transient period the primary O-ring in each joint had to seal the joint. If it delayed longer, the pressurized (1,000 pounds per square inch pressure) hot exhaust gas (5,700 °F) from the ignited booster could push past the primary O-ring and approach the secondary O-ring. Meanwhile the joint continued to open and the secondary O-ring faced a gap that was wide enough to prevent the secondary O-ring from sealing it. Safe sealing, then depended on the primary O-ring sealing its gap no later than 0.17 second after booster ignition! The experimental apparatus used by Thompson to produce the results of Fig. 4.3 was set to open at a rate slightly slower than the rate at which the actual booster joints opened up in the transient period of an actual launch. The results showed that as O-ring temperature gets colder the O-ring is slower to regain its girth and shape. That is, it loses its normal (i.e., warm) resilience, required to seal the joint.

O-ring temperature, then, was shown to have an enormous effect on the O-ring's capacity to recapture its size and shape to seal its gap. At 50 °F it failed completely to seal its simulated gap. (Observation of the 50 °F O-rings was terminated after 10 minutes.) While the simple experimental design failed to include some of the complicated dynamics of actual field joints under launch and flight conditions (e.g., gas pressure or gas temperature) it did capture a) the differential times taken by actual O-rings to recover their size and shape sufficiently to stay in contact with the receding tang surface b) with O-ring temperatures of 100, 75, and 50 degrees Fahrenheit c) when released from the same amount of squeeze as in actual launches, d) in a simulated joint that opened slightly slower than under actual ignition forces.

The Shuttle's Dangerous Situation

The afternoon of the day before the launch, January 27, 1986, Thiokol engineers called the teleconference with NASA officials to warn about the danger of proceeding to launch the *Challenger* the following morning. The engineers had been informed of the extremely low air temperatures (18 °F) predicted for the next day's launch and had calculated the temperature of the boosters' O-rings at 29 °F, 24 °F colder than the coldest O-rings on any earlier flight. They quickly assembled all information available about temperature effects relating to the O-rings and field joints to present to the teleconference showing the dangerous temperature situation of launching the next day.

Hurried by the next day's launch deadline, Thiokol's engineering group prepared the content and sequence of 13 charts and diagrams to present to NASA managers as evidence of danger -- including their chart 4-2 (Fig. 4.3). The managers and engineers at Marshall Space Center were looking for solid proof of danger sufficient to call off the next day's launch. The story of the engineers' expectations that NASA would accept their recommendation to delay the launch, of Marshall managers' misinterpretations of Thiokol's data, of the pressures on Marshall manager Larry Mulloy to avoid any unnecessary launch delays, of Thiokol's own top decision maker's faulty mental model of the joint and biasing contract negotiations with NASA, of how the reigning presumption and burden of proof fatally shaped the unfolding argument – all are pursued in detail elsewhere (Lighthall, 2015). We return now to examining Vaughan's assessment of the boosters' dynamics and the supposedly dangerous acceptance of O-ring erosion by engineers and managers at Thiokol and Marshall.

Vaughan's Claims

Vaughan's central argument is that engineers and managers came repeatedly to consider as acceptable an anomalous field-joint functioning, a deviation from the boosters' design specifications, that the engineers called "erosion." By "erosion" *they* usually meant *impingement* erosion, erosion of the O-ring's upstream, non-sealing surface. Vaughan concluded that erosion of O-rings was the dangerous condition that eventually caused the disaster.[12] She argued that the mental process, "normalization of deviance," by which engineers and managers repeatedly considered as safe that kind of deviation, O-ring erosion, from expected performance led to the accident.

Vaughan's claim is actually three claims in one. The first is that NASA and Thiokol engineers and managers repeatedly accepted as safe a condition, O-ring erosion, which deviated from design specifications. The second claim is that the amount of erosion accepted by engineers and managers actually increased from the first to the last incidence of O-ring erosion.[13] The third claim, the most important one, is that "O-ring erosion" was the physical cause of the fatal malfunction and therefore the engineers' and managers' repeated acceptance of "O-ring erosion" as a safe condition was a dangerous "normalization of deviance."

The first claim is valid. Engineers and managers did continue to find the boosters flight ready and to continue launching shuttles after finding evidence from five flights that primary O-rings in field joints had suffered impingement erosion (as deep as 19 percent of the O-ring's diameter), a condition that design specifications alone would rule unacceptable.

The second claim, that increasing amounts of erosion were accepted, must be bracketed by the understanding that it refers to impingement erosion only, not to blow-by erosion (or "by-pass erosion"). No engineer ever accepted blow-by erosion as anything but dangerous. However, second claim is valid only if a) "increasing amounts" is understood as "repeated amounts" and b) it refers to impingement erosion.

Vaughan has referred to what she perceived as the acceptance of *increasing* erosion ("escalating risk taking," Vaughan, 2005, 45) as a "slippery slope" to disaster. The actual data of impingement erosion in the field joints, however, does not support the idea of normalizing greater deviance. If Vaughan had plotted the erosion data of field joints for all flights -- available in volume II of the 1986 Presidential Commission on the Space Shuttle *Challenger* Disaster *Report* (1986, hereafter PC *Report*), which Vaughan cited -- the resulting picture might have led her to rethink the causal role of erosion or at the very least, to reject the idea that danger from successive instances of impingement erosion actually increased in the field joints.

Figure 5.3 shows the actual history of impingement erosion in field joints, a history of six instances out of 138 joints flown before the *Challenger* flight. The trace of maximum impingement erosion depths shows, not a slippery slope to disaster, but a steady downward slope of *decreasing* erosion depth, a slope toward increasing safety.[14] Figure 5.3 also includes, by contrast, the empirically established safety margin of 0.095 inches of purposely removed O-ring material in tests showing completely reliable sealing despite that depth of .095 in. of "erosion." [15] The distance between that safety margin and actual depths of the occasional

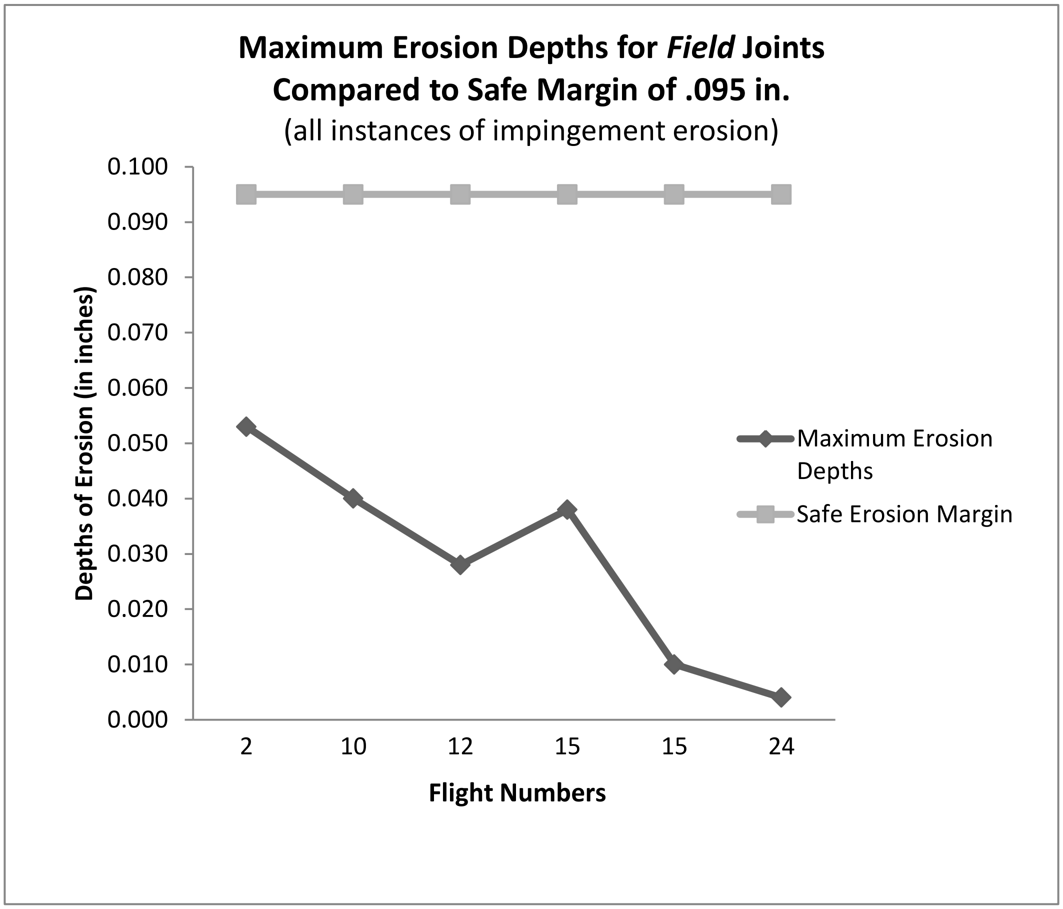


Figure 5.3. Depths of Field Joint Erosion v. Safe Erosion Margin

impingement erosion reflected the engineers' and managers' basis for increasing comfort regarding impingement erosion. They had, thus, an objective, empirically tested basis for "normalizing" the "deviant" erosion *as safe.* Remember, too, that in each of these six instances of impingement erosion of the primary O-ring (never the secondary O-ring), the O-ring sealed its joint (as would be expected from the safety margin).

If we look at the history of *nozzle* joint erosion (Fig. 6.3) we see ups and downs in depths of impingement erosion, but no general trend of increasing depth. Aside from the single flight of 51B, with its complete by-pass erosion of its primary O-ring and its singular occurrence of impingement erosion of the secondary O-ring, all erosion anomalies are well on the safe side of the empirically established safety margin of 0.125 inch for nozzle joints. [16]

The impingement erosion data shown in these figures, 5.3 and 6.3, along with analyses of the physical space and timing limits of the field joint, provided the technical basis on which engineers saw continued flights acceptable despite that erosion. The evidence refutes any claim that engineers and managers were accepting ever-increasing amounts of erosion or ever-increasing degrees of risk from erosion. We do indeed see in these graphs a true normalization of impingement erosion, but what the engineers normalized, by the proper employment of safety margins, was the *safety* of impingement erosion. The really dangerous normalization (or confirmation bias) occurred when the managers, particularly Mulloy and Mason (Lighthall, 2015, Chapters 3 and 5), treated all the variations of O-ring temperatures, in both flight data and experimental data, as irrelevant to O-ring sealing capacity: for them, the variable of O-ring temperature could be safely ignored.[17]

It is the third element of Vaughan's claim where the most serious invalidity occurs. At the center of her argument is the question whether the deviant field-joint performance that Vaughan focuses on, the impingement erosion of O-rings, was in fact the cause of the joint's failure to seal.[18] It was not. Neither impingement erosion nor the far more dangerous blow-by erosion caused *Challenger*'s field-joint failure. Blow-by erosion, which unlike impingement erosion had no safety margin, was caused by other conditions that caused both O-rings of one field joint to fail to seal, leaving that joint open.

At the core of Vaughan's failure to understand the dynamics of *cold* O-rings was her

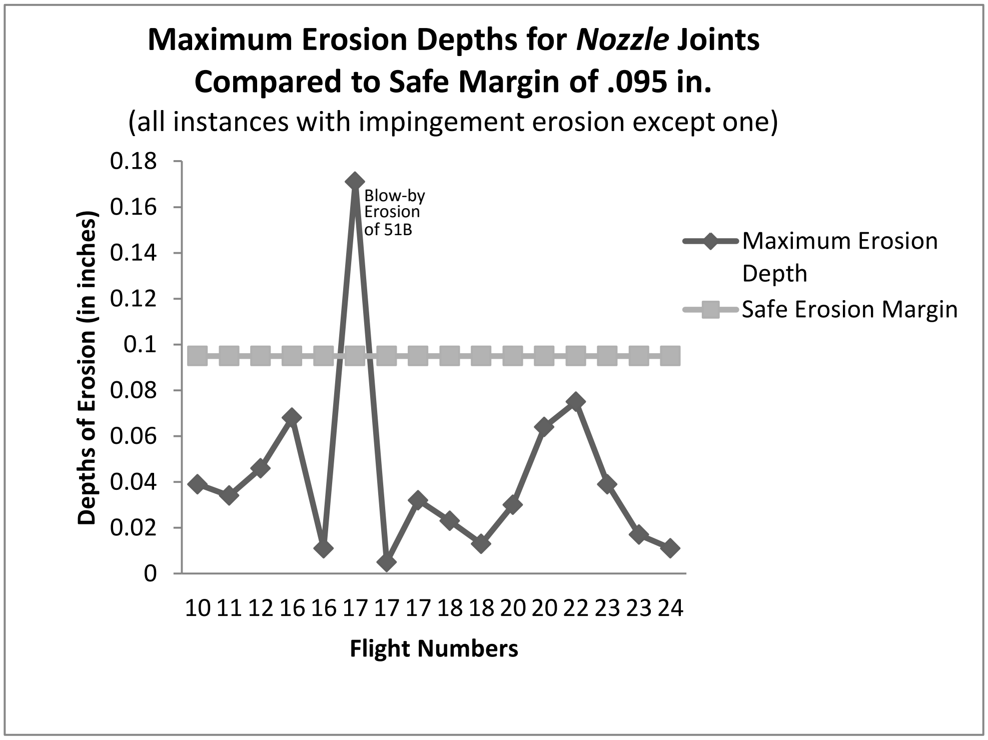


Figure 6.3. Depths of Nozzle Joint Erosion v. Safe Erosion Margin

failure to recognize the meaning and import of Thompson's and Boisjoly's data, data clearly showing how decreasing O-ring temperatures led to decreasing speed with which O-rings recovered their sealing capacity (shown in Fig. 4.3, p. 19; Vaughan's Fig. 11.8). The incapacity of both cold O-rings to seal a field joint due to the gap allowed when both were unable to recover their normal (warm) sealing girth and shape allowed the hot gases to escape -- the precise worry of engineers Boisjoly, Thompson and others at Thiokol.

Extensive post-accident testing precisely validated the Thiokol engineers' pre-launch warning. The testing was carried out at both Marshall and Thiokol, each performed by different sets of investigators. They used similar but not identical apparatus and reached the same basic conclusion elaborated in the next paragraph. Vaughan's failure to read or take seriously these studies was a serious flaw in her research and left her false assumption about erosion as the cause unchallenged by definitive data. [19] The findings of NASA's post-accident studies of O-ring temperature and sealing performance were reported in part in volume I of the *Presidential Commission Report*.[20] Much of the text of volume I, the tacit argument of pages 1–3 of appendix H in volume II, and much of the hearing testimony, like Vaughan, made the false assumption that O-ring erosion and its acceptance by engineers and managers constituted the dangers that led to the accident. In contrast, the Commission's own extensive *post-accident* tests that provide the most rigorous and conclusive basis for identifying the dynamic (second-order) cause of the accident found O-ring *temperature* to be crucial—independent of any erosion.[21]

These post-accident studies employed apparatuses that simulated the field joint and its pressure and rotation characteristics. They established that non-eroded, intact O-rings at temperatures below 45 ºF did not seal reliably and that intact O-rings at 25 ºF, configured like those of the *Challenger*, failed regularly to seal the joints.[22] The proper conclusion to be drawn, then, is that cold temperature, independent of erosion, reducing the resiliency of both primary and secondary O-rings, was sufficient as the initial cause of the field joint to fail to seal. Once 51L's hot gas later in *Challenger's* ascent found its way past the non-sealing O-rings, it eroded everything in its path.

While some of the tests performed at Marshall are reported along with Thiokol's studies in Figure 19 of Volume I (PC *Report*), the separate report of the unambiguous findings of the Marshall team itself, never reported or referred to in Volume I are summarized in figure 7.3. The *S*s (Successful sealing) in figure 7.3 represent test outcomes in which the O-ring in the simulated field joint successfully sealed, while the *F*s represent tests resulting in seal failure. A glance at the

Figure 7.3. The Effects of Temperature on the Sealing Capacity of O-Rings: Summary of 49 Post-Accident Marshall Space Flight Center Tests (From Figure 29, Presidential Commission *Report*, Vol. II, p. L-83)

% Seal Success or Seal Failure ⇒ Number of Successes/Failures ⇓	O Seal	33.3 Seal	70 Seal	100 Seal	100 Seal	100 Fail	66.7 Fail	30 Fail	O Fail	O Fail
10						F^{10}				
9				S^{9}		X				
8				X	S^{8}	X	F^{8}			
7			S^{7}	X	X	X	X			
6			X	X	X	X	X			
5			X	X	X	X	X			
4		S^{4}	X	X	X	X	X			
3		X	X	X	X	X	X	F^{3}		
2		X	X	X	X	X	X	X		
1		X	X	X	X	X	X	X		
0	S^{0}								F^{0}	F^{0}
Temperature of O-rings Tested (° Fahrenheit)	25°	45°	50°	55°	70°	25°	45°	50°	55°	70°

c..j:\chal\SHDwebsite\Fig.4.3. Post-accidnt O-ring v Temp tests.Marshall.7.4.13

figure shows that as one moves from the left, where O-ring temperatures were 25 ºF to the right, where O-ring temperatures increased to 70 ºF, the *S*s (successful sealing), start at 0 percent at 25 ºF and rise to 100 percent with O-rings at and above 55 ºF. Sealing failures are the complementing values of sealing successes, of course, represented in figure 7.3's *F*s (failures). They steadily decrease from 100 percent failure with O-rings at 25 ºF to 0 percent failure with O-rings at 55 ºF and 70 ºF. At 45 ºF and 50 ºF O-rings sealed unreliably.

Cold O-ring temperature alone, preventing the O-rings from expanding to fill the joint's gap as it opened, caused the unsealed space in the joint through which the hot gas could escape. The only evidence of any cause that led both a primary and a secondary O- ring to fail was the evidence gathered after the accident, reflected in part in figure 7.3, showing how the degraded resilience of both primary and secondary O-rings, due to their low temperature, caused their inability to seal the joint, independent of erosion.[23]

Causes: Sudden or Gradual?

What does this all imply for the mode of explanation that best fits all the evidence of causality? It is clear that cold temperatures were not typical, did not accumulate in force over the history of flights, but came rather suddenly upon the launch countdown, after the *Challenger* shuttle had been officially declared flight ready. This was a discontinuous cause, arising suddenly to bring about a sudden new effect, complete sealing failure of both O-rings in a field joint.

Why, then, has the continuous mode of explanation taken such a strong hold, a hold so gripping that large portions of the Presidential Commission's own explanation fixed upon erosion as the cause, this despite the commission's own reported investigations showing that temperature caused failure in the absence of erosion? One can only speculate about the persistence of that factually incorrect view, but one thing is clear. By seizing upon erosion as the cause, erosion so dramatically evident after the accident in the form of a large hole in the side of the recovered aft booster segment, those who took erosion as a cause engaged in post hoc thinking.

The best bulwark against post hoc thinking is careful examination of the evidence regarding *a number of conflicting* hypothesized causes—precisely what the teams of post-accident investigators at Marshall and Thiokol did. The results of those studies, the most telling of which is reflected in figure 7.3, call us to shift attention away from erosion and to focus on *Challenger*'s cold temperature and consequent degraded O-ring resiliency and incapacity of the O-rings to seal their joint. [24] The degraded resiliency, consequent O-ring obliteration, and melting steel were effects, not causes. The new, triggering cause was the cold weather reaching into the field joints and making the coldest and weakest of the squeezed O-rings fail.

Since Vaughan's analysis of normalized deviance focused not on temperature but on erosion, her analysis cannot further be considered as an explanation of the seal failure or of the accident. In terms of figure 1.3, since Vaughan incorrectly identified the physical cause (column B) that brought about the effect (column A, the accident), her tracing backward of the successive social, organizational, and institutional constraints leading to that supposed cause, including notably the normalization of the anomalous erosion, is a tracing of a non-cause, an effect. Her tracing becomes irrelevant to understanding the succession of cognitive, social, organizational, and institutional constraints and events that did, in fact, constitute the immediate *human cause* of the accident.

Dual Imperatives of Engineering: Production and Safety

In order to understand the flaws entailed in Vaughan's solution to the problem of safety versus danger, we must understand how the profession of engineering solves that problem. But before we turn to any solutions, we have to understand a fundamental problem of any engineering enterprise. The problem lies in a duality of commitments, a set of basic values that in many circumstances, perhaps most, pull in opposite directions. It is a conflict inherent in any engineering enterprise.

The Production Imperative

Engineering, being a profession that arose and grew up in response to the need to make things, to build tools or structures that serve important collective purposes, is deeply inscribed by the requirements imposed by constructing and producing something that solves some problem. Principal among its required ingredients are the following six:

1. Purpose—the goals and needs to be served by the product
2. Knowledge of materials and material properties, skills of designing, constructing, testing, and refining useful and usable products—the accumulated knowledge and skills that we usually think of as "engineering"
3. The engineers—those possessing the knowledge and skills to design, construct, and test the product
4. Resources—material, financial, intellectual, and temporal—to build the product, where resources are almost always limited and therefore usually require compromises between quality and production
5. Organized effort—people organized to carry out differentiated tasks according to coordinated functions and schedules, to produce the product in usable time
6. Clients/customers/market—those whose purposes are to be served by the product, those who will pay for it to the extent that it serves their purposes.

Omit any of these, and no engineering product of any complexity will appear. Note that the root word *engineer* appears in only two of these required ingredients. But all of them contain the root word *product*. An engineering enterprise is oriented toward production and is by its nature constrained by production requirements.

Production, however, is constrained and balanced by the competing value of *quality* of product, one attribute of which is its safety. Quality includes reliability, efficiency, effectiveness, and safety; and production entails delivering the product in good condition to the client in time for scheduled use. While both quality and production must be well served, at any given moment in the production process managers of the effort will give priority to one or to the other. Two questions that will operate tacitly in managers' strategic thinking are: "Is production going smoothly enough now and sales sufficiently steady that we can allocate time and resources to improving quality?" and "Is the quality of our product now good enough that we can start (or maintain or increase) production?" The production imperative is ever present and insistent in any engineering enterprise operating under competition, not only inextricable from engineering but also the source of design-guidance and resources necessary to produce the product.

A fundamental problem inherent in any engineering enterprise in a competitive market, then, is this elemental competition between the imperative of quality, with its important dimension of safety, and the imperative of production, of getting a useful product to the user in usable time.

Resolving the Contradictory Values

If the insistent presence of production goals conflicts with the equally important goal of safety, how does the discipline of engineering resolve that tension? How does engineering prevent production tendencies, always powerfully fueled by the pursuit of profits or schedule-driven success, from overrunning what engineers know to be safe? It was precisely this fear that production needs might trump safety that McDonald warned his assistant Ebeling about, insisting that Thiokol's launch decision be "an engineering decision" (see Lighthall, 2015, chapter 2).

How Engineering Protects Safety from Production Pressures

Vaughan herself had the same fear that McDonald had expressed as she approached her study of the *Challenger* disaster. She feared managerial "wrongdoing," the kind where managers know that a certain number of injuries or deaths will result from the design they want to produce, and that those injuries can be greatly reduced by a different, more costly design, but who decide to go ahead producing the more dangerous design because it will cut costs and yield greater profits. That "amoral calculation" Vaughan did not find in the *Challenger* case, but she had plenty of evidence from the history of manufacturing to give her good grounds for fearing it in the *Challenger* disaster. However, if Vaughan had interviewed Allan McDonald more extensively she might have understood the contract situation facing Thiokol's Senior Vice President, Gerald Mason, and how he resolved his dilemma as possibly involving some "amoral calculation" (see Lighthall, 2015, chapter 2). While her analysis found no such wrongdoing, it is important to acknowledge that production pressures, being ever present, can overwhelm safety in an engineering enterprise, and do so even when slogans about "safety first" find ubiquitous verbal and written expression in the organization.[25]

The Safety Imperative

What is engineering's answer to the fear that both Vaughan and McDonald expressed? How does engineering provide a safeguard that at some point holds fast against production pressures and yet at the same time allows changes, deviations from design specifications that improve the performance or safety of the as-built product?

The engineering solution to protecting safety against the pressures of production is precisely the answer that Vaughan saw as *a danger,* as leading to the normalization of deviance she saw in engineers' acceptance of "erosion." The solution of engineering is to test, measure, and calculate *safety margins* (for example, safe margins of depths of impingement erosion) resulting from forces exerted, to test for the sources and intensity of those forces, and then to add another margin to allow for unforeseen dangers.

In assessing the realities about the engineering function in question (for example, O-ring sealing of the field-joint immediately after ignition), engineers seek to know two kinds of limit, one that promises danger, the other promising safety. The danger limits are those beyond which performance-degrading stress must not be allowed to pass. The safe limits are those maximum stress levels that assure *completely safe* performance under the product's specific stress limits and environments of performance. One domain of limits concerns the *causes* of threatening stresses; another domain concerns the *effects* of threatening stresses. If the hot gas at ignition provides the *causal force* threatening O-ring capacity to seal, the *effect* of concern is the amount of damage (depth of erosion) that the gas can bring about in an O-ring.

At what depth of impingement erosion do O-rings give way and fail to seal under pressure like that produced by ignited fuel—the *minimum* stress point that actually brings

O-ring failure? All participants knew that erosion that deep must be avoided, and any intensity of stress leading to that depth must be avoided. They also sought to know a safe limit, the maximum depth of impingement erosion at which O-rings *always succeeded* in sealing.

Erosion of this maximum safe sealing depth can be tolerated, but it is a limit engineers will not want to approach closely. Rather, they will leave an additional margin, a buffer, between this safe sealing depth of erosion and the maximum depth they will decide to tolerate. Many shuttle margins had been set at 1.4, for example, meaning that in order to arrive at a margin that would be safe, one must require each shuttle element to withstand a factor of 1.4 times the tested safe load or stress limit in its performance. The safety margin regarding impingement erosion of O-rings in field joints provides a good example of the idea of safety margins in general.

Thiokol engineers tested the safe and failure limits of impingement erosion depth. They placed O-rings in an apparatus that simulated field-joint behavior in which the O-rings had been experimentally “eroded” (as in impingement erosion). Material on the upstream surface of the O-ring -- the O-ring surface directly exposed to any blow-hole in the insulation through which hot gas might exit -- had been cut away to various depths, simulating impingement erosion. The engineers found that at depths of simulated impingement erosion *greater* than .095 inch, the O-ring sometimes sealed and sometimes did not seal. O-rings with material excised to a depth of .145 inch failed regularly. But O-rings experimentally eroded to a depth of .095 inch reliably sealed the joint on all tests.[26]

In this fashion engineers had followed normal engineering principles by empirically determining the point of predictable sealing failure, determining the range of impingement erosion depth at which sealing was unreliable, and determining the depth of that erosion at which fully reliable sealing was predictable.[27] The *Challenger* engineers in this regard were treating the shuttle as an experimental vehicle, learning from each flight's deviations from design specifications or assumptions, responding with tests for limits and tolerance.[28]

Establishing such empirically quantified safety margins is the engineer's answer to all production pressures. You must determine safety margins away from product failure, and once they are determined, you don't violate them.

Vaughan's Safety Project

The physical danger Vaughan identified as the cause of the accident, and against which she sought safer practices was erroneously identified by her. But from within Vaughan's own frame of thought, the repeated acceptance of erosion by engineers and managers, that normalization of deviance had to be corrected, in her view. One of the principal bases for allowing launches to continue was the engineers' and managers' reliance on safety margins. Calculating safety margins of design-deviating performance of the field joints led to acceptance of erosion, she claimed, which was clearly a deviation from design. Fundamental for Vaughan are the original design specifications. [29] It is the design specifications, deviations from which, if "normalized" become dangerous in Vaughan's view. So to calculate *new* safety margins, after experimental flights had been completed, to test the extent of danger revealed by a new anomaly like impingement erosion was in Vaughan's view dangerous.

If such tests gave quantitative evidence that the anomalous phenomenon (e.g., impingement erosion) could not physically approach the point of failed performance (e.g., .095 inch of O-ring impingement erosion), those tests were, for Vaughan, dangerously misleading. It substituted a calculation that allowed *acceptance* of impingement erosion over design specifications or (“expectations”), specifications that did not permit any such erosion. Such acceptance constituted a “normalization of deviance,” i.e., a deviance from specifications that was for Vaughan a slippery slope to disaster.

Vaughan’s solution to the safety problem created by this reliance on safety margins was to call for their cessation; this particular engineering practice simply had to be eliminated. Safety demanded, she claimed, a very different practice, one that can be described in a simple rule: whenever any deviation from design specifications is detected in any function that is critical to flight safety, launches should be halted, completely discontinued until either the original specifications can be met or a complete re-design is validated by test (see pp. 118, 147-148, 149-150, 232-233).

Her project, then, was to eliminate a deeply ingrained engineering norm and practice (relying on empirically tested safety margins) and to substitute a new norm and practice, one of insisting on design specifications as absolute criteria of safety regarding any shuttle function critical to safe flight.

While critical design specifications must always be guides, and are crucial guides for initial construction, the history of engineering generally and the shuttle experience in particular speaks against casting aside the engineering norm and practice of determining and using tested safety margins, margins established after the vehicle is actually in regular use.

Taking critical design specifications as absolute guarantors of safety is an error on at least two counts. The first relates to the state of knowledge at the time specifications are set forth. The second relates to the competing requirements of safety and production, and how the discipline of engineering provides safe resolution of that competition.

Since design specifications are established before any engineering creation can be built (booster rockets, bridges, new models of aircraft), those design specifications are uninformed by actual tolerance limits of the new engineering creation in its as-built functioning. [30] If the boosters in actual performance are discovered to have strengths or weaknesses not specified in the design, it is necessary for post-design investigation to identify, measure, and correct any such weaknesses -- and, where important and useful, to specify any strengths not specified in the design. In any engineering creation as unique and experimental as the shuttle, many strengths and weaknesses that are wholly unanticipated in the initial design specifications will be discovered in its actual flight performance.[31] When encountered, they must be newly specified by test and measurement, the bread and butter of engineering. The *Challenger*'s boosters, we now know, had temperature limitations, limitations not imagined at the design stage. They also proved, again surprisingly, to have field joints that opened up at ignition. These were just two of many discoveries unmentioned in specifications.[32]

One specification completely unimagined at the time of design was that O-ring sealing could safely tolerate impingement erosion of primary O-rings up to .095 inches in depth, and therefore that impingement erosion up to .053 inches in depth could be tolerated as safe. Yet that is what the whole data base of the first twenty-four shuttles proved, without contradiction by the disaster of the 25th flight.

The second reason that design specifications should not be considered absolute is that engineering creations must always balance safety with production. Even automobiles, with their air bags and seat belts and crash-protecting measures, are approved, produced, and purchased while still possessing great dangers for drivers and passengers—vulnerable tires at legal but still high speeds and tanks of explosive liquid fuel. We accept those risks, and in doing so we reject the idea that safety is absolute. The population's requirement to be mobile makes automobile production in accessible price ranges more important than absolute safety. We add safety measures as they become available and economically feasible, but we go right on in the meantime producing, purchasing, and using automobiles, even while we are aware of a fairly steady rate of fatalities. Yet automobiles are no longer "experimental" or "developmental" vehicles. Space vehicles, in stark contrast, stand at the extreme, experimental end of the continuum from fully developed, "operational" vehicles to experimental vehicles. We tolerate their severe risks because space exploration is simultaneously valued and inherently dangerous.

NASA and Congress accepted severe risks as part of the approved design of a shuttle. For example, the Orbiter was designed, upon return to earth from a space flight to have one and only one attempt at landing. The Orbiter approached landing without motor power, pulled only by gravity in a one-time glide, with no misses possible, no second approaches. A similar risk attended the initial stage of ascent after launch, which allowed no escape for the astronauts if there were a malfunction. We citizens, the astronauts, the Congress, tolerate such risk in order to begin the process of learning by doing, learning how to explore space by creating space vehicles to learn from. Safety is balanced against getting the engineering creation built, tested, and used to serve a purpose, a purpose that we collectively value enough to pursue while accepting a vehicle with dangers that we know about, a vehicle, furthermore, that we also know has dangers we have yet to learn about.[33]

The shuttle showed itself to be experimental, continuously revealing hidden qualities. That means that its every preparation, launch, flight, and return was an experiment, each an occasion for it to teach us its real, in-use properties. These unknowns and discovery characteristics will be all the more true for the next stage of space exploration. Each flight of a new series, with new technological equipment, will teach us about the new vehicle's hidden strengths and weaknesses if and only if we will listen carefully as learners; if we watch, measure, study, and analyze those measurements.

One thing the shuttle preparation, flights, and returned boosters and Orbiter teaches us, if we will learn, is the ways in which its original design specifications are silent on matters that analysis of those flights tells us are important. One of the things it will teach us, moreover, is that some critical design specifications or assumptions about the vehicle will be insufficient or even dead wrong. It will also teach us that other specifications assumed to describe dangerous weaknesses will turn out to be manageable safely, well within safe margins that we derive from use of the vehicle and from experiments carried out while we use it. So we will learn both about new dangers the designers did not imagine and about imagined dangers that turn out, after all, to be safe.

In the last analysis, then, design specifications in developmental vehicles are *conditional,* conditional upon actual performance in actual environments. Only analytical study of the experimental vehicle can tell which specifications are valid and which need revision and, further, what specifications omitted in the original design need to be added. Vaughan's project to eliminate as dangerous the use of critical safety margins and to replace them with critical design specifications as absolute criteria for flight safety is both based on an erroneous analysis of what went wrong with the *Challenger* accident and ignores the fallibility and incompleteness of critical design specifications themselves.

The answer that the discipline of engineering gives to prevent production pressures from trumping safety, to summarize, is that safety margins of anomalies a) can be determined in quantitative terms, b) must be determined quantitatively, and c) must not be violated. These are engineering principles deeply and properly ingrained as professional norms. These principles are necessary to follow if safety is to be protected. But I have hinted, and hope to demonstrate in *Disastrous High-Tech Decision Making* (Lighthall, 2015), that even these crucial principles of safety margins fall short of being sufficient.

So far I have addressed three key issues. First, in the course of critiquing Vaughan's analysis of the second-order cause of the accident, the dynamic failure of the O-rings to seal the joint, I have identified the failure that actually did initially cause the disaster, namely the failure of unusually cold, squeezed O-rings to seal the field joint that failed. Having correctly identified the second-order cause (everyone agrees on the first-order cause), we are now in a position to examine the third- and fourth-order causes correctly, namely the key deficiencies in the participants' deliberations about the sealing capacity of cold O-rings, and the conditions that caused those deliberative deficiencies. That is a major task of *Disastrous High-Tech Decision Making: From Disasters to Safety* (Lighthall, 2015).

The second key issue was the nature of pre-accident deliberations that prevented participants from seeing the actual dangers. Vaughan's analysis focuses on the wrong physical cause, eroded O-rings, and so her analysis of deliberations about erosion is irrelevant to the actual weaknesses in the deliberations.

The third key issue addressed in this essay was the kind of condition that must be considered sufficiently dangerous to halt all launches. Dangerous is any violation of an empirically established safety margin for a critical function or, by extension, *any failure to establish an empirical safety margin for a critical function.*

The professional norm and practice of establishing empirically based safety margins for critical anomalies meets both safety and production demands that engineering anywhere must meet. All anomalies must be considered dangerous unless and until valid margins for safe performance are empirically established. Those safety margins are an important component of the infrastructure of safety.

However, in experimental programs like the shuttle program, or any high-tech, safety-critical enterprise that explores an unforgiving environment, new dangers will arise that require safe handling when no safety margin could have already been empirically established. In that situation of a signal of possible serious danger, with no prior testing, the wisdom of continuing production will depend on the believability of the warning signals as compared to the depth of commitment to continuing production. The struggle necessary to protect safety under those conditions is addressed prominently in *Disastrous High-Tech Decision Making: From Disasters to Safety*.

Vaughan also claimed that no norms were violated in the decision process leading up to the *Challenger* launch.[34] Vaughan's basis seems to be that the teleconference decision making was "unprecedented" and so no norms existed to regulate its deliberations. Her judgment that the teleconference was unprecedented, however, she herself contradicts. [35] Also, Mulloy himself regarded the teleconference as a flight readiness review.[36]

Any review of a shuttle's flight readiness, especially a review calling into question the readiness of a shuttle about to be launched, would require close examination of data-based evidence regarding flight readiness. Norms for doing that had been firmly established. First, it was normal practice, followed without exception, to present quantitative data in any such review. That norm was followed in the teleconference. But not just any data or interpretation of it would do.

Evidence in such reviews had to be, in Mulloy's phrase, "credible quantitative engineering analysis or test data." [37] High standards of data and reasoning constituted a universally recognized norm, standards that were adhered to in all formal FRRs, the ones that were answerable to William Lucas and that would come under his Marshall Center review. In the teleconference itself, however, and contrary to Vaughan's claim that it "proceeded according to the protocol for a formal Level III FRR," standards of data, interpretation, and reasoning were violated, by both Mulloy and Hardy, violated in their interpretation of Thompson's chart which showed a clear relationship between O-ring sealing capacity and O-ring temperature, and by Mason, who misinterpreted "blow-by" as innocuous unless it was accompanied by erosion.

The crucial misinterpretation was another, by Mulloy, in which he ignored the quantitative differences in extent and sooted blackness of blow-by evidence between the cold and warm flights, reducing those stark differences to zero by flawed reasoning. He reasoned that since both warm and cold flights showed evidence of blow-by there could be no correlation between temperature and blow-by. His reasoning focused on a discrete variable (presence-absence) but ignored the more relevant continuous variable (quantity). To ignore quantitative differences was a blatant violation of both Lucas's severely monitored norm of quantification and a deep norm of all professional engineering and of high-technology management. This violation, in effect hiding key evidence of impending danger, was given more force by another failure, a failure by all those who saw the danger of cold O-rings clearly. They failed by violating another norm of FRRs, that all evidence and reasoning be probed for consistency among data sources, for sufficiency and for coherence of reasoning.

The two most expert engineers on temperature effects and sealing dynamics, Boisjoly and Thompson, and the most expert manager regarding those dynamics, McDonald, failed to refute Mulloy's first and most telling argument against Thiokol's data-based warning. All three emphasized earlier points they had made, and McDonald added new considerations for delaying the launch. But none directly refuted Mulloy's obfuscating statement denying any correlation of temperature with O-ring sealing because of the common *presence* of blow-by in the joints of both cold and warm flights.[38]

To conclude, Vaughan's (1996) analysis of the *Challenger* decision making is seriously flawed in its mischaracterization of the physical cause of sealing failure as erosion, in its failure to evaluate the arguments and interpretations on both sides of the argument critically, and in its failure to include the crucial data in the Commission's report (in its Volume II, appendix L) of two sets of independently conducted post-accident experiments showing that O-rings' capacity to seal their joints was a function of O-ring temperature, not erosion.

Since Vaughan traced the collective thought process of accepting O-ring erosion (impingement erosion), a factor not involved in the accident, we had not yet learned about the collective thought processes that actually led to the *Challenger* accident. Because the research community has assumed Vaughan's account was both accurate and complete, no further digging into the primary documents has occurred after 1996 – other than the digging I have been able to do over the years since the accident. My version of the human causes of the accident (Lighthall, 2015) draws on a more complete accessing of primary documents than Vaughan's, and uses a richer breadth of analytical concepts – from ergonomics, naturalistic decision making, the social sciences, and legal argument – providing the kind of complex analysis required to comprehend decision making about realities as complicated as these.

The actual human causes of the *Challenger* accident remained to be examined, still at large, so to speak, contaminating decision processes in other high-tech, high-stakes enterprises. One of those still hidden contaminants is the perceptual and cognitive distance between engineers and technicians close to technical dynamics on one hand, and on the other, their managers empowered to make decisions about safety and danger but lagging or flawed in technical knowledge. That hidden, still unrecognized danger in high-tech organizational decision making is revealed both in the *Challenger* disaster (Lighthall, 2015, 137-138) and in the study on this website, Case Study: A High-Tech "Near Miss."

End Notes

[1] My critical essay here runs to 45 pages of text, a length required a) to lay out not only Vaughan's errors in understanding the boosters' high-tech dynamics, and not only b) to explain those dynamics accurately, but also c) to set the accurate analysis within broader explanatory frameworks for understanding complex causality in high-tech and other organizational accidents, near misses, and mistakes.

[2] See Tompkins' "mandatory resource" comment (Tomkins, 2005, p. 122). Tomkins follows Vaughan's claim that O-ring erosion caused the physical failure.

[3] See chapter 8 of the first volume of the board's official report, "History as Cause: *Columbia* and *Challenger*," Columbia Accident Investigation Board (2003) *Report*, vol. I, 195–204.

4. The genre of naturalistic decision making (NDM) inquiries is described succinctly by Zsambok (1997) (Zsambok & Klein, 1997, 5): "The study of NDM asks how experienced people, working as individuals or groups in dynamic, uncertain, and often fast-paced environments, identify and assess their situation[s], make decisions and take actions whose consequences are meaningful to them and to the larger organization in which they operate." See also Orasanu & Connelly (1993).

5. See for example Weick & Sutcliffe (2001, pp. 40, 59), Reason (1990, pp. 192, 253-54), and Tompkins (2005, 127, 133) for scholarly analyses that rely on Vaughan's analysis or on volume I of the Presidential Commission *Report*. Without going back to volume II of the *Report*, with its details of impingement erosion distinguished from blow-by erosion, the succession of measured erosion depths, the *safety margin* established for impingement erosion, and most particularly, the results of post-accident tests at both Thiokol and Marshall, these analyses carry forward the flaws and flawed implications of Vaughan's account – and continue the scholarly silence regarding *actual* causes, both physical and human.

6. The figures on this website contain a decimal from .1 to .3, denoting which of the three articles on the website www.high-techdangers.com they belong to: .1 denotes figures in the case study, "A High-Tech 'Near Miss' - Organizational Decision Making Up Close;" .2, denotes figures in my analysis of the *Columbia* decision making, "The *Columbia* Disaster: Choice Points, Deficiencies, Dangerous Thinking;" and .3, for figures in my critique, "Basic Flaws in Vaughan's Analysis of the *Challenger* Accident."

7. The first launch decision, about launching the *Challenger,* was followed by a set of deliberations and another decision the very morning of the fatal launch. The story of that process, never before subjected to systematic analysis, is presented as the second analysis of deliberation and decision on this website, *A High-Tech "Near Miss" – Organizational Decision Making Up Close.* It is unique, since much of its data are actual recorded conversations among the participants.

8. Vaughan sums up her view of the physical cause of the booster's malfunction in her preface: "O-ring resiliency was impaired by the unprecedented cold temperature that prevailed the morning of launch" [Vaughan views "cold temperature's effect on O-rings" as the "*alleged* cause of the *Challenger* disaster" p.554, italics added]. "Upon ignition, hot propellant gases impinged on the O-rings, creating a

flame that penetrated first the aft field joint of the right Solid Rocket Booster, then the External Tank…" (xi). Vaughan elaborates her view (p. 10) "O-rings, grease, and joint insulation began to burn." The destructive dynamic in her view was "a flame that penetrated…" after hot gas "impinged on" the O-rings, burning them, and then escaping from the field joint. Vaughan misses the effects of cold, non-resilient, squeezed O-rings as causing the failed joint to remain open for the hot gas to escape – entirely independent of O-ring erosion as a cause, as shown by the post-accident studies (See PC *Report*, vol. II, Appendix L, L72-L82, scenario 4d and Figures 28 and 29).

9. See also Vaughan (2005, 41): "The O-ring erosion that caused the loss of the *Challenger*…"

10. See Lighthall (2015, chapter 1) for an explanation of bubble formation in the insulating putty.

11. If the O-rings in all six of the boosters' field joints were cold, why did only one fail? Two explanations fit with some known facts. 1) The very one that did fail seems to have been at the coldest location, away from sunlight and close to the down-flow of cold air coming off the external tank filled with liquid oxygen. See Billy K. Davis's testimony before the Presidential Commission on his temperature readings with an Infra-Ray gun, P. C. *Report*, Vol. V., 960-965. 2) The second explanation is simpler, and refers to a phenomenon that had occurred before the accident. "Blow-holes" had occurred occasionally, and unpredictably, through the insulation. If a blow hole had occurred in the insulation at the point of the failed booster joint, it would have provided the hot exhaust gas a path to the now cold and squeezed, non-resilient primary O-ring. The secondary O-ring, also squeezed, cold, and non-resilient, would allow the joint to remain open so hot gas would escape through the joint.

12. See Vaughan (1996, xi and 10; 2005, 41, 43, 45, 57).

13. Vaughan writes about the "work group" (engineers and supervisors) "accepting the possibility of increased damage once again" (1996, 380). The normalization of repeated increases in O-ring damage is expressed by Vaughan in her later writing about the *Challenger* (Vaughan, 2005) in the metaphor of a "slippery slope" toward disaster—a habit of bad thinking that led to "more frequent and serious erosion" (57).

14. Figure 5.3 shows two instances of maximum depth because flight 15 (the coldest flight before the *Challenger*) experienced impingement erosion in two joints.

15. The safety margin of 0.095 inches for field joints was established in February, 1984, so was not known

at the time flights 2 and 10 (STS-2 and 41B) were flown (see P. C. *Report*, vol. I, p. 128 and vol. II, p. H9). Establishing this safety margin through empirical test confirmed an earlier safety margin established by analytical calculations (see P. C. *Report*, vol. II, appendix H).

16. The extraordinary blow-by erosion of the primary nozzle O-ring of flight 51B was explained as a singular anomaly combined with insufficient leak-test pressure. The latter was increased for all subsequent flights (see PC *Report*, vol. II, chart 127, p. H65; also vol. I, 138-139.).The safety margin of 0.125 inch was established for nozzle joints in June, 1985 (see P. C. *Report*, vol. II, p. H61, chart 119), so was not part of the rationale for flying until flight 19 and afterwards.

17. The concept of normalization, the social psychological process of framing repeated encounters with a situation as confirming it as a safe situation, has been extensively explored in cognitive and social psychology as the "confirmation bias" (Nickerson, 1998).

18. "O-ring resiliency was impaired by the unprecedented cold temperature that prevailed the morning of the launch. Upon ignition, hot propellant gases *impinged on the O-rings*…" (Vaughan, 1996, xi; emphasis added. See end note 8).

19. See PC *Report*, vol. II, Appendix L, L72-L82, scenario 4d and Figures 28 and 29. Four comments are in order regarding the data in Figure 28. First, all the tests reported in Appendix L were conducted with cold gas, not hot gas. Since *cold gas, even under high pressure, does not erode the O-rings*, all results reported concern the effects of O-ring temperature and other factors on O-ring sealing its gap ("pass test") or non-sealing ("fail test") wi*thout* erosion. Second, the figure suggests a higher order statistical interaction effect of Initial Gap X Speed of Putty Rupture ("Fast" v. "Nom") X Temperature, with the .004 in. initial gap opening to .029 in. final gap opening. With the 500 millisecond delay ("Nom") you begin to get leakage past the primary and secondary O-rings at 50 °F. However, third, with O-rings at 25 °F you get primary and secondary O-ring leakage under *all* conditions – a very big main effect of O-ring temperature, statistically speaking. Further, fourth, the temperature of 51L's O-rings were 29 °F at launch so the results closest to 51L's actual conditions in Figure 29 are where O-rings are at 25 °F, that is, failure under all conditions considered in Figure 29.

20. See P.C. *Report*, vol. I, 62, fig. 19. The text in volume I that describes the findings summarized in the figure fails to indicate both that the tests were carried out with cold gas and that the import of the

findings there summarized is that cold temperature alone would have caused 51L's O-rings to fail to seal wherever blow-holes were present to allow the hot gas to reach the O-rings.

21. Vaughan's only reference to "post-accident temperature analysis" is to the weak correlation the commission found between temperature and impingement erosion (Keel and Kehrli's charts presented as figures 6 and 7 in *P.C. Report*, vol. I, 146, and in Vaughan (1996, 382–83). Vaughan makes no mention of Thiokol's and Marshall's post-accident experimental studies relating O-ring temperature to actual sealing failure independent of erosion, reported in appendix L of volume II of the commission's report.

In focusing on erosion as the fatal trigger of the accident, Vaughan's analysis follows one of two quite different analyses of the immediate cause that appears in volume II of the *P.C. Report*, analyses with contradictory conclusions as to cause but whose contradiction was never noted, much less resolved by the Presidential Commission. Vaughan's analysis follows the cause, erosion, which is implicit in pages H1–H3 (appendix H) of volume II, an analysis that examines the sequence of FRR measurements and evaluations focused on erosion and on "the notion of 'acceptable' erosion" (appendix H, H1). Appendix H was apparently written by commission staff members who were unaware of the engineers' empirically established margins of safety for impingement erosion, margins fully accepted by engineers and managers at Marshall.

22. The language of the reports of post-accident experiments that identified the physical cause of the accident makes no mention of any measurements of erosion. It does make clear that the tests were all conducted with cold gas, which would not erode O-rings. The engineering experts designing those experiments understood that for a sealing surface of an O-ring to be eroded, the joint it was situated in had to have remained *unsealed* as a prior condition of gas passing *by* the O-rings. So the focus of all experiments logically moved to explore the physical conditions that would cause field joints to remain open, that is, for O-rings to fail to seal their gaps before any erosion took place. The two leading candidates were excessive squeeze, preventing the O-ring from being actuated, and cold-induced loss of O-ring resiliency. The latter proved to be the more important causal variable although Thiokol's experiments could be interpreted to indicate that the interaction of the two could be more potent than either squeeze or cold temperature alone. Of course, once a joint's gap remained unsealed due to the

cold, unresponsive O-ring, actual flight conditions with surging hot (5,700 °F) gas would bring catastrophic erosion of O-rings and steel alike.

23. Vaughan actually came close, however, to discovering how non-eroded O-rings could fail to seal the field joint's gap as it opened up under pressure. Vaughan understood that when the O-rings got colder they became harder, were "slower to respond," and took longer to fill the joint's gap when it opened up under ignition (Vaughan, 1996, 173, 304). But she evidently failed to see the significance of first, the condition of O-rings *when and where* they became cold and non-resilient, and second, how *non-resilience would necessarily create an open joint.* They became squeezed *out of shape* -- somewhat flattened, where their flatness compromised their sealing girth – when the booster segments became assembled at Kennedy Space Center. When thus squeezed and then became cold, the O-rings (both primary and secondary) stayed squeezed or, more precisely, they were *slow* to recover from their squeezed, out-of-shape condition, slow to regain their sealing girth, as a function of their *coldness,* thus leaving the joint open.

24. This central role of O-ring resiliency was pointed out to the Presidential Commission by one of its members, Richard Feynman, during one of the Commission's hearings (see Feynman, 1988, 150-153). His demonstration, though in front of the Commission itself, did not prevent the *Report* from including much text pointing to O-ring erosion as the culprit, leaving the *Report* somewhat ambiguous as to the physical cause.

25. Some may see Mason's behavior in Thiokol's caucus discussion as "wrongdoing" because of his bias toward launching in the context of high-pressure contract talks with NASA. Yet any priority he might give to maintaining flight schedule in the face of his inexact knowledge and his engineers' charts must be understood in the context of normal CEO production-oriented behavior and role commitments in a free-market economy, the confusing data, and the degraded deliberative resources in any countdown situation (of which more must be said: see Lighthall, 2015, chapters 5 and 6).

26. Thiokol engineers did not apply the added 1.4 margin to this .095 limit. Doing so results in a safety margin of .068 inch of erosion depth, safe but only a little deeper than the greatest depth of erosion experienced in actual flight.

27. The finding of this .095 inch safe limit confirmed engineers' earlier judgments, based solely on their

understanding of the physics of the joint, that the field-joint erosion observed on the second of the first four test flights of the shuttle (in November 1981)—to a depth of .053 inch—was not serious enough to stop flights. The next instance of field-joint O-ring erosion (maximum erosion depth .040 inch) was on the 11th flight, STS-41B, flown in February 1984. By March 8, a little more than a month later, Thiokol engineers were able to present their findings regarding the .095 inch depth of reliable O-ring sealing, using that finding to argue that the next shuttle flight, STS-13, could expect joint O-ring impingement erosion but that such erosion could be accepted since "laboratory test of full-scale O-ring/joint cross sections shows capability to sustain joint sealing integrity at 3,000 psi pressure, using an O-ring with a simulated 0.095 in. erosion depth." (See *P.C. Report*, vol. II, H9, chart 12.)

28. The engineering answer does not end with the search for the safe limits of stress effects. Engineers want to quantify not only effects, but also causes—the sources and intensities of the threatening forces themselves. How fast and by what time trace did the gas increase its pressure within the .6-second ignition transient? How much volume did the gas have to fill in the cavity around the booster case between the putty and the primary O-ring, the cavity extending away from the blow hole(s), before pressure equalized and impingement erosion stopped? How did the blow holes through the putty come about through which the hot gas was able to reach the O-rings? What percentage of O-ring diameter must be squeezed in the pre-ignition joint to assure a seal? What could prevent blow holes, thus preventing erosion altogether? What condition allowed the hot gas to pass by the primary O-ring without eroding it?

All but the last two of these questions were raised in the course of the first twenty-four shuttle flights, and all of those raised were answered in quantitative terms. While the kinds of condition that produced blow holes were identified, whether those conditions would hold true on any given flight was not discovered. Nor were engineers able to determine either the number of blow holes that might occur on any given flight, or how blow holes might be prevented.

29. See pp. 112 and 149-150. See also Vaughan's five-step decision sequence leading to the normalization, in her view, of erosion as acceptable. The fifth step in "accepting risk" (Vaughan, 1996, p. 125) indicates the design "expectation" from which the normalized deviations deviated: "…correcting the joint rather than redesigning it and flying *despite data that the joint deviated from expected*

performance [i.e., from *design*]. Italics added.

30. Lt. General James Abrahamson, former top administrator of the shuttle program, commented on the experimental nature of the shuttle in remarks before the House Committee on Science and Technology (U. S. Congress, 1986c, 196-229):

"We … had to strike the fundamental balance that any flight test program must achieve: specifically, flights must go on to gain knowledge of performance and strengths and weaknesses in the System… every flight was regarded as a learning experience (p.197) …. If I take the F-16 [military aircraft], for example, which I was responsible for, at 25 flights we had just barely begun to explore the envelope and the performance of the machine…" (p.213) See also Arnold Aldrich's explanations to the Presidential Commission of "significant correction of things [anomalies] we couldn't find until we flight-tested" (PC *Report*, Vol. IV, p. 63).

31. Vaughan quotes Henry Petroski (1985, p. 40): "a design is a hypothesis to be tested." Elaborating, she quotes further: "The very newness of an engineering creation makes the question of its soundness problematical. What appears to work so well on paper may do so only because the designer has not imagined that the structure will be subjected to unanticipated trauma or because he has overlooked a detail that is the structure's weakest link" (p. 80). In light of the Challenger booster's cold, squeezed, and malfunctioning O-rings, Petroski's words seem clairvoyant.

Vaughan devotes a page and a half in elaborating on the insufficiency of the engineering creation's design is conveying full knowledge of the operating characteristics of the creation in use – e.g., "Closure is always temporary, for the design hypothesis is tested again and again in use" (p. 202).

However, Vaughan's approval of the Petroskian view that an engineering creation like the space shuttle was a hypothesis to be tested creates a problem for Vaughan's argument. If the shuttle's design is a hypothesis to be tested it removes its *design* as specifying its safe limits and requirements. Those limits remain as hypotheses to be tested. What, then, are the Vaughan's "deviations" deviating *from* and why does normalizing them – by testing and finding some deviations like impingement erosion safe – make that normalizing ipso facto dangerous? In Petroski's view, testing anomalous deviations from original design a) is inevitably required for safety and b) if the testing follows normal engineering standards the test outcomes will be reliable guides for judging the creation safe or dangerous to use. Vaughan never examines the methods the engineers used to test the limits of erosion; her argument is that testing them as a way of continuing launches was itself dangerous because it was a way to obviate what had been established in the design (p. 125). To accept even the slightest deviation, to “normalize it,” is for Vaughan to start down the slippery slope, away from the secure ground laid out by the design. But the design does not lay out secure ground if what it provides is just a hypothesis. Vaughan does not seem to see the contradiction between design as criterion of safety and design as hypothesis.

32. The boosters’ temperature limitations had begun to be discovered in Thompson’s resiliency studies, results of which he presented in the teleconference. His resiliency results contradicted the general temperature tolerances specified by the O-ring manufacturer and accepted by NASA as its own operating range. Here, then, was a case where design specifications of a critical component, the O-rings, were in the books, but wrong, and were in the process of being corrected by Thompson’s tests of sealing capacity. The teleconference itself can be regarded as illustrating some of the process of assessing load limits of an experimental vehicle.

33. We pursue that purpose, however, always in the context of limited resources and other, competing programs of action. Vaughan (1996, 45) quotes John Young, then Chief of NASA’s Astronaut Office who wrote an internal NASA memo on March 4, 1986, just six weeks after the accident while the Commission was still conducting hearings. He excoriated NASA for putting schedule ahead of safety. Referring to the boosters’ tricky seal dynamics, he accused: “There is only one driving reason that such a potentially dangerous system would ever be allowed to fly – launch-schedule pressure.” After listing other potentially dangerous characteristics in support of his view, he comments on the kind of contradictory goals that are inherent in any high-tech, high stakes enterprise: “People being responsible for making flight safety first when the launch schedule is first cannot possibly make flight safety first no matter what they say. The enclosure shows that these goals have always been opposite ones. It also shows overall flight safety does not win in these cases.” Vaughan includes this quote among several to make the case that the public and the Commission had come to believe that the accident, like many others in the world of markets, was caused by bad managers who made “an amoral calculation” regarding human safety, placing safety subordinate to production. Her driving thesis, to use Young’s

term, is to reveal that view as being invalid by demonstrating the contrary view that the decision process was simply normal for such enterprises, with no amoral calculation involved. Vaughan at one point counts the *Challenger* accident (p. 415) as a "normal accident" (Perrow, 1984), beyond human capacity to prevent.

34. See Vaughan's comments refuting claims by several Thiokol engineers that decision norms for FRRs had been violated: **"**… neither NASA norms nor rules were violated on the eve of the launch... My review of rules, procedures, and norms used in FRR decision making for the SRB group in previous launches and by other work groups responsible for other parts of the shuttle allowed me to identify the same norms, rules, and procedures in operation on the eve of the launch," p. 339.

35. In the sentence preceding her quote of Russell (see the following end note), Vaughan characterizes the teleconference as an FRR: "The teleconference proceeded according to the protocol for a formal Level III FRR." Vaughan also commented on the teleconference participants' "imposing the rigors of FRRs on this ad hoc meeting." One of the consequences of this "was that participants abided by the stringent FRR standards about what was admissible as evidence" p. 357. They were, in other words, conforming to the norm of high standards of evidence in FRRs, according to Vaughan.

Her statement is partly true, partly false. It was true that the original set of engineers who included and spoke to *all* their evidence bearing on O-ring sealing were adhering to the FRR norm of complete data inclusion, whether pro or con one's conclusions. It is also true that they had framed the argument coherently and logically, and it proves with incontrovertible evidence, that flying with O-rings at or above 53 °F would be safe. If that argument had been in fact presented, they would have had the solid evidence of 24 safe flights. While their recommendation, that "O-ring temp must be ≥ 53 °F at launch" captured precisely their intended thesis about proving *safety*, the argument was quickly transformed by the discussion to *O-ring temp must not be < 53 °F*, an argument about *danger*. *That* argument, unwittingly and mistakenly accepted by the engineers as logically equivalent to their intended argument, could not be conclusively proven with the data available. That accepted argument, further, *presumed* safety while the intended argument, like all FRRs, *presumed* danger. (See chapter 8 of Lighthall, 2015 for an analysis of the crucial role of presumptions in determining disagreements when evidence is mixed. See also Tompkins, 2005, 113-116.)

As to adhering to the FRRs' high standards of evidence and argument, Mulloy's first and most telling argument against Thiokol engineers' argument for a launch delay violated that norm when he ignored the quantitative evidence in the charts in front of him about blow-by in the warm and cold flights. Instead Mulloy argued that because of the *presence* (he ignored the *quantities*) of blow-by in both warm and cold flights there could be no correlation between blow-by and O-ring temperature. (Chapter 8 of *Disastrous High-Tech Decision Making* discusses the protections and pitfalls of evidence-based argument, about which all participants were uninformed.)

36. See Mulloy's testimony on this point, stating the similarity between the teleconference and discussions at flight readiness reviews, in PC *Report*, vol. V, p. 863. Vaughan herself quotes Brian Russell, the engineering manager who presented Thiokol's first chart in the teleconference, showing that he regarded the teleconference as a flight readiness review: "In my own mind, it was very much like a Flight Readiness Review. In fact, that's what we were doing, was discussing the readiness of that vehicle to fly under the conditions that we anticipated" (Vaughan, 1996, 340). Also, Thiokol's inclusion in its teleconference presentation of all available data regarding field joint functioning irrespective of whether a study was complete or in process, followed a norm of data inclusion pointedly established by Lucas for all flight readiness reviews.

37. Personal e-mail from Larry Mulloy, Sept. 25, 2000, with permission.

38. Lighthall (2015) explores the evidence of these actions and inactions. McDonald, seated across the table from Mulloy, would seem to have had the greatest opportunity and persuasive power. He did offer two reasons for halting the ongoing launch countdown besides that of the unusual cold weather, trying to persuade Mulloy and Reinartz, Mulloy's immediate superior, to recommend a delay. McDonald even took a threatening tone, indicating that he would not want to be the one who allowed the launch to go forward with O-rings at 29 °F when the shuttle as a whole was qualified only to 40 °F – an assumption Mulloy found flatly wrong. See McDonald's own published account (McDonald and Hanson, 2009). But none of these added arguments constituted direct *refutation* of Mulloy's first, most telling, and fallacious argument against delaying the launch. That argument, allowed to stand unchallenged, denied any role of temperature in the subsequent thinking of all managers with decision-making authority.

References

Feynman, R. P. 1988. Ralph Leighton, (Ed.) *What Do You Care What Other People Think?: Further Adventures of a Curious Character*. W. W. Norton.

Klein, G. A. 1993. A recognition-primed decision (RPD) model for rapid decision making. In Klein, G. A., Orasanu, J., Calderwood, R., & Zsambok, C. E. (Eds.) *Decision Making in Action: Models and Methods (pp. 138-147).* Norwood, NJ: Ablex Publishing.

Lighthall, F. F. 2015. *Disastrous High-Tech Decision Making: From Disasters to Safety*. Indianapolis, IN: Kilburn Sackett Press.

McDonald, A. J. 1989. Return to flight with the redesigned solid rocket motor. *AIAA Paper No. 89-2404,* AIAA/ASME/SAE/ASEE 25th Joint Propulsion Conference, Monterey, CA, 10-12 July.

McDonald, A. J. & Hanson, J. R. 2009. *Truth, Lies, and O-Rings: Inside the Space Shuttle Challenger Disaster.* Gainesville, FL: University Press of Florida.

Nickerson, R. S. 1998. Confirmation bias: A ubiquitous phenomenon in many guises. *Review of general psychology*, ***2*** (2): 175–220.

Orasanu, J. & Connelly, T. 1993. The reinvention of decision making. In G. Klein, J. Orasanu, R. Calderwood, & C. E. Zsambok (Eds.) *Decision Making in Action: Models and Methods* (pp. 3-20). Norwood, NJ: Ablex Publishing.

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

Petroski, H. 1985. *To Engineer is Human: The Role of Failure in Successful Design.* New York: St. Martin's.

Presidential Commission on the Space Shuttle *Challenger* Accident. 1986. *Report*, vols. I-V. Washington, DC, United States Printing Office.

Reason, J. 1990. *Human Error*. Cambridge, UK: Cambridge University Press.

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

Tompkins, P. K. 2005. *Apollo, Challenger, Columbia: The Decline of the Space Program.* Los Angeles, CA: Roxbury Publishing

US Congress, 1986. *Investigation of the Challenger Accident*. Volume 2. Hearings before the committee on science and technology, U. S. House of Representatives, 99th Congress, second session, July 15-24, 1986, No. 139, Washington, DC: US Government Printing Office.

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

_______, 2005. System effects: On slippery slopes, repeating negative patterns, and learning from mistakes? In Starbuck, W. H. and Farjoun, M. (Eds.) *Organization at the Limit: Lessons from the Columbia Accident (pp. 41-59).* Malden, MA: Blackwell.

Weick, K. E. and Sutcliffe, K. M. 2001. *Managing the Unexpected: Assuring High Performance in an Age of Complexity.* San Francisco: Jossey-Bass.

Zsambok, C. E. 1997. Naturalistic decision making: Where are we now? In C. E. Zsambok & G. Klein (Eds.), *Naturalistic Decision Making (pp. 3-16)*. Mahwah, NJ: Lawrence Erlbaum Associates.

c..j:\chal\h-tdanger\1. Basic flaws.2016. .Vaugn.critique essay. PDF REVSN 6. 5.17.16.