“Something is Wrong”: Tracing the Lifecycle of Safety in High-Risk Aerospace Systems

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Nikita Ann Joy

Spring 2025

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Caitlin D. Wylie, Department of Engineering and Society

“Something is Wrong”: Identifying Factors For Assessing Aerospace Safety Prioritization

A physicist walks into a hardware store.

It sounds like the start of a joke, but in 1986, that’s exactly what Richard Feynman did. The Nobel Prize-winning physicist, serving on the Rogers Commission investigating the explosion of the space shuttle Challenger, bought a small C-clamp and prepared a simple but powerful demonstration for the next day’s televised hearing (Feynman, 1988).

During the hearing, Feynman clamped a piece of O-ring material—similar to that used in the shuttle’s solid rocket boosters—and submerged it in a cup of ice water. He reminded the audience that the night before launch, temperatures had dropped to 25°F, with liftoff occurring just above freezing—NASA’s coldest launch on record. When he removed the O-ring and released the clamp, it failed to return to its original shape, clearly showing how low temperatures compromised its elasticity. The visual demonstration brought immediate clarity to how gas could escape through faulty seals, leading to the explosion that killed seven astronauts and shocked the nation.

But Feynman’s experiment wasn’t just about physics. It was about flawed thinking. Engineers had long known about the risks, yet past success lulled them into complacency. “ ‘It flew before, so it must be OK,’ ” Feynman later wrote, criticizing the mindset. “Try playing Russian roulette that way: You pull the trigger and it doesn't go off, so it must be OK to do it again, right?” (Feynman, 1988, pp. 138)

In this paper, I argue that the prioritization of safety in the aerospace industry often follows a cyclical trajectory—rising sharply in the wake of disaster and gradually tapering as attention shifts toward innovation, cost-efficiency, and schedule adherence. Despite significant advancements in safety protocols and technology, catastrophic failures continue to occur. This paradox invites critical reflection on how safety is valued and operationalized within organizations.

This paper introduces a theoretical framework—Safety Prioritization Theory—to better understand the fluctuating nature of safety emphasis across time and context, while reflecting broader shifts in safety climate and safety culture. By applying this framework to historical case studies and existing theoretical frameworks such as the Normalization of Deviance and the Collingridge Dilemma, this paper seeks to identify systemic patterns that degrade safety and offer insights into how safety might be made more resilient in the future.

Conceptual Foundations: Safety Culture, Safety Climate, and Systemic Risk Frameworks

To understand how safety is upheld or compromised in high-risk industries such as aerospace, it is essential to distinguish between the concepts of safety culture and safety climate, and to contextualize them within broader systemic frameworks such as the Normalization of Deviance and the Collingridge Dilemma. These frameworks help illuminate the subtle yet powerful ways organizational behaviors, perceptions, and structures influence the likelihood of failure.

Safety culture refers to the enduring values, beliefs, and shared assumptions within an organization that shape how safety is understood and prioritized over time (Reason, 1997; Guldenmund, 2000). It is foundational and relatively stable, guiding behavior even in the absence of direct oversight. A strong safety culture fosters accountability, open communication, and proactive risk management, while a weak safety culture may lead to complacency, silence, and the institutional acceptance of risk.

Safety climate, contrastingly, captures the more immediate and measurable perceptions of safety at a given moment. It reflects employees' views on how safety is prioritized by leadership and peers, and how policies and procedures are enacted in daily practice (Zohar, 1980; Griffin & Neal, 2000). Safety climate can vary over time and across departments, and often serves as a real-time indicator of how deeply embedded cultural values are translating into practice. A strong safety climate is characterized by open communication, empowered reporting, and consistent safety enforcement. A weak safety climate, by contrast, forms when employees perceive that raising concerns is discouraged or futile (Hofmann & Morgeson, 1999).

Complementing these concepts is sociologist Diane Vaughan's theory of the *Normalization of Deviance*, developed through her investigation of the organizational dynamics behind the Challenger disaster. With a background in the sociology of organizations and deviance, Vaughan conducted extensive archival research and interviews at NASA to understand how a high-reliability institution could repeatedly downplay technical warnings. Her 1996 book, *The Challenger Launch Decision*, revealed how minor procedural violations became routine, reinforced by institutional pressure and the absence of immediate failure. These patterns dulled sensitivity to risk and ultimately enabled the fatal decision to launch under unsafe conditions. Her work regained relevance in the aftermath of Columbia, which echoed the same drift toward normalized risk and organizational complacency.

Another critical framework is the Collingridge Dilemma, introduced by technology policy scholar David Collingridge in his 1980 book *The Social Control of Technology*. Writing in the context of science and technology studies, Collingridge described a core paradox: early in a technology's life cycle, risks are unclear and hard to regulate; later, once risks are known, the system is so entrenched that change becomes difficult and costly. This dilemma is especially relevant in high-risk industries where innovation often outpaces oversight. For both Challenger and Columbia, early warnings were limited by uncertainty, while delayed action was hindered by institutional inertia—exactly the dynamic Collingridge predicted.

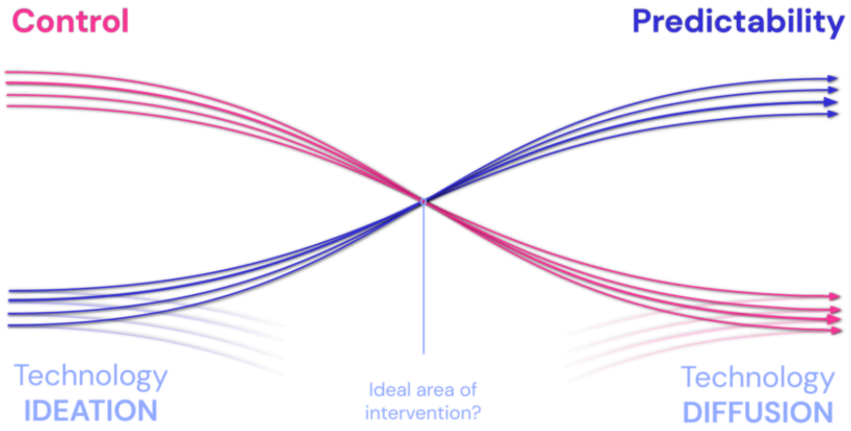

Figure 1: An visual depiction of the CollingRidge Dilemma[1]

Together, these frameworks provide a structured way to analyze how risk accumulates not merely through technical failures, but through organizational patterns and systemic pressures. Safety culture shapes long-term assumptions about risk; safety climate reveals how those assumptions are felt in practice; the Normalization of Deviance shows how routine decisions can drift toward danger; and the Collingridge Dilemma explains why timely intervention is so often elusive. These concepts serve as the foundation for evaluating both historical failures and future safety challenges in high-risk domains.

[1] Adapted from Besti, F. and Samorè, F. (2018), Responsibility driven design for the future self-driving society. Fondazione Giannino Bassetti. Cited in references

Human Error and Safety Culture: Understanding Behavioral Pressures in High-Risk Environments

Understanding how safety culture functions in practice requires close attention to the behavioral pressures that influence decision-making in high-risk environments. While safety culture is often framed in terms of shared values and institutional commitments, its impact is most clearly seen in the ways individuals respond to competing demands, ambiguous risk signals, and organizational expectations (Reason, 1997). The Challenger and Columbia disasters provide sobering case studies that illustrate how safety culture shapes behavior, how internal pressures contribute to lapses in judgment, and how the Normalization of Deviance framework explains the gradual erosion of safety practices over time.

Defining Human Error and Workplace Pressures

Human error refers to actions or decisions that deviate from intended safety protocols, leading to potential risks or failures (Reason, 1990). While some errors are unintentional—such as slips, lapses in attention, or miscalculations—others emerge from systemic workplace pressures that subtly shape decision-making. In high-risk industries like aerospace, nuclear energy, and manufacturing, workplace conditions significantly impact cognitive load, risk perception, and adherence to safety standards.

In the case of the Challenger disaster, engineers had long voiced concern about the O-rings' vulnerability to cold temperatures. Despite this, organizational pressures—including public and political expectations to maintain the shuttle schedule—overrode safety warnings. Management reinterpreted the recurring O-ring erosion as acceptable risk, illustrating how human error can stem not from ignorance, but from a workplace culture that prioritizes deadlines over precaution. Similarly, in the Columbia disaster, damage to the orbiter's Thermal Protection System (TPS) was noted after launch, but decision-makers dismissed the threat. Requests for further imaging were denied, due in part to flawed simulations and reluctance to involve external agencies, showing how cognitive biases and organizational silos can reinforce unsafe norms.

Workplace environments characterized by schedule demands, understaffing, or conflicting priorities compel individuals to rationalize risky behavior as necessary. These decisions—once made under duress—can become normalized, especially when no immediate consequences occur. Over time, such behaviors become institutionalized, transforming deviations from protocol into routine practice. The Challenger and Columbia cases underscore how management, under organizational inertia and budgetary scrutiny, cultivated environments where deviations were neither isolated nor rare—they were operationally embedded.

Safety Culture and the Normalization of Deviance

Understanding how safety culture interacts with the Normalization of Deviance is essential to explaining the persistence of human error in high-risk environments. While safety culture provides the underlying framework for what behaviors are expected, encouraged, or tolerated within an organization, Vaughan's theory illustrates how those expectations can be gradually reshaped by organizational experience.

The Normalization of Deviance is particularly insidious because it masquerades as normal operational decision-making. For Challenger's launch, the decision to proceed with despite known technical concerns was not framed as reckless—it was the product of a culture where past successes with O-ring erosion dulled sensitivity to risk. For Columbia, management downplayed a known breach in the Thermal Protection System, relying on flawed modeling and historical precedent rather than empirical scrutiny. In both cases, the absence of immediate failure after prior anomalies contributed to the belief that safety margins were adequate, allowing unsafe practices to become routine.

When deviant practices—such as procedural shortcuts or the dismissal of safety concerns—are met with success or no immediate consequence, they are increasingly reinterpreted as acceptable within the cultural logic of the organization (Vaughan, 1996). Over time, this alignment between culture and normalized deviation erodes the organization's sensitivity to risk, not through a single decision, but through a series of culturally sanctioned adaptations.

Corporate Motivations and Safety Climate: Understanding Systemic Pressures and Risk Normalization

In high-risk industries, the intersection of corporate incentives and safety climate presents ongoing challenges to maintaining operational integrity. Financial pressures, political considerations, and institutional inertia can quietly reshape how safety is perceived and practiced, particularly when organizational success is measured in cost savings, efficiency, or public image. The Challenger and Columbia disasters illustrate how these pressures can degrade safety climate over time, embedding risk tolerance into decision-making and enabling small procedural deviations to escalate unchecked.

External Interests and Their Influence on Safety Climate

While safety culture represents long-term values, safety climate reflects immediate perceptions of safety's priority within an organization (Zohar, 1980). The Challenger disaster reveals this clearly: engineers repeatedly warned against launching in low temperatures due to O-ring vulnerabilities, yet these concerns were overridden by NASA management, who feared the political and public consequences of another launch delay. The pressure to adhere to schedules and maintain public confidence effectively silenced engineering voices, undermining the safety climate and fostering risk tolerance.

Similarly, the Columbia disaster illustrates how bureaucratic priorities and risk underestimation can erode frontline safety vigilance. After foam debris struck the left wing during launch, engineers requested high-resolution imaging to assess the damage. However, NASA leadership dismissed the need, citing flawed simulation data and expressing concerns about involving the Department of Defense. These decisions were shaped not just by technical misjudgment, but by institutional reluctance to disrupt workflow or attract negative attention. In both cases, leadership framed potential risks as manageable based on past outcomes, further weakening the organizational safety climate.

The pressures to maintain production timelines and achieve economic or reputational goals can distort risk assessments. This is not unique to government agencies; in the private sector, companies may similarly dismiss early safety warnings to preserve commercial interests. Fir the Challenger case, schedule fidelity was prioritized over risk mitigation. For Columbia, entrenched bureaucratic norms and leadership confidence in historical success delayed responsive action. These scenarios reveal how powerful organizational interests—public or corporate—can produce environments where safety is perceived as negotiable.

Safety Climate, The Normalization of Deviance, and the Collingridge Dilemma

While originally applied to the public sector through NASA leading up to the Challenger disaster, I propose that workplace pressure is a constant regardless of private or public service, and that therefore Vaughan's framework is applicable to the corporate world. The Normalization of Deviance does not occur abruptly—it arises incrementally, as minor violations become routine and are retroactively justified by the absence of immediate negative consequences (Vaughan, 1996). For Challenger, prior launches had shown signs of O-ring erosion, yet no failures had occurred, leading management to conclude that these anomalies were within operational norms. Similarly, for Columbia, previous strikes to the shuttle had not caused catastrophic outcomes, reinforcing a perception that such impacts were benign. These cases underscore how organizations, public or private, can become desensitized to risk when success appears to validate flawed assumptions.

The Collingridge Dilemma further underscores the regulatory challenges that accompany complex technological systems. In the early stages of a program—such as NASA's reusable shuttle—risks are often poorly understood, making proactive regulation difficult. But once routines are established and systems become operationally entrenched, meaningful intervention becomes politically and economically burdensome. After Challenger's explosion, NASA undertook major design overhauls to restore confidence. Following Columbia's failure, although the shuttle program continued for several more years, its vulnerabilities prompted a decision to phase it out, culminating in retirement in 2011 (Adler, 2023). In both cases, the cost of reform was steep—highlighting the core dilemma: early action is constrained by uncertainty, while later action is impeded by institutional inertia.

These dynamics mirror those in the corporate world, where safety concerns are often deprioritized until public scrutiny or disaster forces reform. Regulatory capture, stakeholder pressure, and internal silos can all contribute to environments where known risks are tolerated until crisis strikes. The influence of operational/corporate interests on regulatory responsiveness exacerbates the Collingridge Dilemma, delaying necessary change and allowing deviant practices to take root.

The Normalization of Deviance, compounded by the Collingridge Dilemma, explains how even technically advanced organizations can make fatally flawed decisions. Understanding these disasters through these frameworks encourages a critical reevaluation of how high-risk industries balance safety with operational priorities.

Intersectionality and Safety Prioritization Theory

The complexities of safety in aerospace engineering cannot be reduced to isolated frameworks or single-dimensional causes. Rather, safety prioritization emerges from the *intersection* of safety culture, safety climate, technological evolution, and historical precedent. Culture and climate are not interchangeable, rather they are dimensions of safety that are mutually reinforcing. Within this interplay, I propose a framework called *Safety Prioritization Theory*, which offers a temporal model to trace how safety transforms from a post-crisis value into a background norm subject to erosion. Each stage—Idealization, Devaluation, Constriction, Rationalization, and Normalization—is informed by historical examples and grounded in the frameworks of Diane Vaughan's Normalization of Deviance and the Collingridge Dilemma.

Process	Climate or Culture Driven?	Impact of Low Experience/Oversight	Cascading Effect
Idealization	Climate	● Post-Accident, regulations and investigations rush to evaluate and analyze the problem ● Safety is prioritized, but measures of safety are not adapted to change with the space	● Safety regulations that are not reflective of the design space’s changes over time
Devaluation	Climate	● Safety measures are ill-fitting so much so that people see them more as a slough than a necessity ● Due to the measures “working”, safety is de-prioritized and seen as stifling innovation	● Increased pressure to remain competitive ● Cuts to “inefficient” programs
Constriction	Climate	● Lack of historical input for budget estimates for new technology ● Lack of knowledge of design space for new technology	● Budget Shortfalls ● Overly Optimistic Timelines
Rationalization	Culture	● Reliance on newer and more experimental models and simulations ● Incorrect transfer of applicability due to lack of historical data	● Reassurance based on faulty data ● Continued dismissal of failsafes
Normalization	Culture	● Instances of normalization fall through the cracks due to ill-fitting regulations ● Due to earlier constrictions the overseers are more likely to participate in Normalization of Deviance.	● Pushing limits and constraints beyond acceptability

Figure 2: A tabular description of the stages of Safety Prioritization Theory in chronological order

Idealization marks the organizational overcorrection that follows public failure. In this phase, safety is rhetorically elevated—codified through new procedures, technical review boards, and highly visible leadership engagement. These changes often represent a shift in the safety climate, but not necessarily culture. Reforms tend to be reactionary, targeting the specific failure rather than addressing broader organizational weaknesses. After the Challenger explosion, NASA implemented formal reporting mechanisms and restructured technical oversight, projecting a renewed commitment to safety (Presidential Commission, 1986). Yet as the Columbia Investigation Board later observed, this surge in reform created an “illusion of safety” based on the quantity—not the quality—of changes. This can be seen in chapter 5 of the Columbia Investigation report, which states “NASA made many changes to the Space Shuttle Program structure after Challenger. The fact that many changes had been made supported a belief in the safety of the system, the invincibility of organizational and technical systems, and ultimately, a sense that the foam problem was understood”. (Columbia Investigation Board, Volume 1, pg. 199).

Devaluation marks the stage where safety begins to be seen as a burden rather than a necessity. The climate shifts from urgency and vigilance to efficiency, cost-reduction, and routine. Safety measures, once implemented with conviction, are now viewed as mismatched to emerging challenges. Under pressure to meet deadlines, managers and engineers begin treating safety concerns as obstacles to progress. For Challenger, leadership downplayed O-ring concerns in favor of schedule adherence and public optics. For Columbia, foam strikes were considered “acceptable” due to the team planning for ‘light’ debris falling on the orbiter, reinforcing a climate where risk was tolerated for the sake of continuity. This reflects Vaughan’s Normalization of Deviance: risk signals are repeatedly ignored, normalized by success rather than resolved by action (Vaughan, 1996).

Constriction emerges when organizations begin operating in a design space that lacks sufficient historical data, leading to inaccurate budgeting and unrealistic timelines. Marked by a narrowing of foresight—constriction is not because of deliberate negligence, but due to epistemic gaps in technological understanding. In these moments, the safety climate often grows overconfident, assuming that prior successes can be extrapolated to novel contexts. However, because the safety culture of the organization has not yet adapted to account for this new technological uncertainty, early-stage warning signs are frequently misinterpreted or overlooked.

For Challenger, engineers had minimal data on how low temperatures affected O-rings, yet were expected to certify launch readiness. For Columbia, engineers lacked the tools to fully assess foam strike damage, yet operational confidence remained unchanged. Because the organization was moving into uncharted technical territory without revising its safety expectations accordingly, planning assumptions remained rooted in outdated models. This stage reflects the Collingridge Dilemma—early in the adoption of new technology, organizations lack the empirical basis to make informed safety interventions, but by the time risks become visible, it is often too late to change direction without significant cost or delay. Without a culture that anticipates these unknowns, constriction creates a fertile ground for the Normalization of Deviance, as overconfidence and urgency obscure the knowledge gaps that require deeper scrutiny.

Rationalization follows when organizations begin to justify or explain away emerging risks through internal logic or insufficient data. In this phase, the safety climate becomes increasingly distorted—leadership may still express rhetorical commitment to safety, but operational decisions favor assumptions over facts. For Challenger, erosion of the primary O-ring was rationalized due to the presence of a backup seal, with engineers neglecting the fact that the backup seal was also compromised. For Columbia, flawed simulations suggested foam damage was negligible, and further imaging was denied. These rationalizations eroded the safety climate, sending the message that risk is manageable if it can be explained away. Meanwhile, the culture becomes overconfident in its processes, reinforcing a dangerous feedback loop of unverified trust in emerging tools. This directly reflects Vaughan's theory: deviations from protocol are framed as acceptable, even reasonable, when organizational success becomes the measuring stick (Vaughan, 1996).

Normalization is the final stage, where deviant behavior has become institutionalized and unremarkable. The safety climate no longer registers specific concerns as urgent because they have been integrated into operational expectations. Employees may no longer report safety issues because they assume nothing will change—or because risk has been reinterpreted as routine. For Challenger, concerns about launch temperatures were seen as non-critical because prior launches had succeeded under marginal conditions. For Columbia, the fatal foam strike was normalized as "acceptable," even though the consequences of the unchecked damage was catastrophic and could be seen as such if taken seriously from the ground. The safety culture at this point has internalized deviance, embedding it into unofficial policies, review processes, and leadership norms. Here, Vaughan’s theory reaches its full expression: risk is no longer an external hazard to be managed, but an internalized part of the system. Combined with the inflexibility highlighted in the Collingridge Dilemma, normalization makes meaningful reform nearly impossible until after failure occurs.

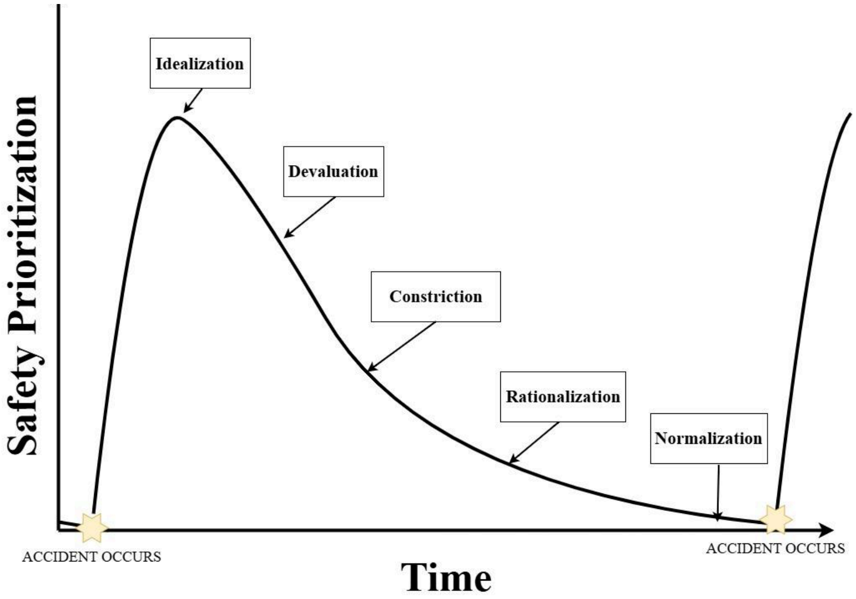

Figure 3: A cyclical visual of the stages of Safety Prioritization Theory

The Safety Prioritization Theory, then, is more than a conceptual timeline—it is a recursive model showing how shifts in climate inform behaviors and how culture sustains them. Each phase builds on the last, demonstrating how risk becomes reinterpreted, downgraded, and absorbed into organizational life. The Challenger and Columbia disasters serve as cautionary case studies for how these stages unfold in practice—and how safety, once deprioritized, can vanish from decision-making entirely. Understanding these patterns is essential not only for diagnosing past failures but for designing future systems that resist complacency and support adaptive, resilient safety cultures.

Conclusion

Aerospace safety is not a fixed attribute but a dynamic organizational priority—constantly shaped by technological change, economic pressure, and institutional culture. Through the lens of Safety Prioritization Theory, this paper has shown how well-intentioned safety reforms can gradually erode under systemic strain, leading to the eventual normalization of risk. The Challenger and Columbia disasters are not just historical tragedies—they are structural case studies in how deviance becomes routine when short-term imperatives outweigh long-term vigilance.

Integrating frameworks such as the Normalization of Deviance and the Collingridge Dilemma allows us to more clearly identify the conditions under which safety breaks down—not suddenly, but incrementally. At the core of this analysis lies the relationship between safety culture and safety climate, which must be continuously evaluated, not assumed. As Richard Feynman warned in the wake of Challenger, “They [erosion and blow-by] are warnings that something is wrong. The equipment is not operating as expected, and therefore there is a danger that it can operate with even wider deviations in this unexpected and not thoroughly understood way. The fact that this danger did not lead to a catastrophe before is no guarantee that it will not the next time, unless it is completely understood." (Feynman, 1986).

This insight remains as relevant today as it was then. To avoid repeating the same failures, high-risk industries must resist the drift toward complacency, remain critical of their own assumptions, and design cultures that treat small anomalies not as tolerable noise—but as early signals that something is deeply wrong. It is only by recognizing how safety fades—not catastrophically, but quietly—that we can hope to prevent history from repeating itself.

References

Adler, D. (2023, May 18). Why did NASA retire the space shuttle? Astronomy Magazine. https://www.astronomy.com/space-exploration/why-did-nasa-retire-the-space-shuttle/

Besti, F., & Samorè, F. (2018). The Collinridge Dilemma [Graph]. Retrieved from https://selfdrivingsociety.fondazionebassetti.org/wp-content/uploads/2019/01/Responsibility-driven-design-for-the-future-self-driving-society.pdf

Collingridge, D. (1980). The Social Control of Technology. St. Martin's Press.

Feynman, R. P. (1988). What do you care what other people think: Further adventures of a curious character. W. W. Norton & Company.

Feynman, R. P. (1986). Volume 2: Appendix F - Personal Observations on Reliability of Shuttle. Presidential Commission on the Space Shuttle Challenger Accident. https://www.nasa.gov/history/rogersrep/v2appf.htm

Hofmann, D. A., & Morgeson, F. P. (1999). Safety-related behavior as a social exchange: The role of perceived organizational support and leader–member exchange. Journal of applied psychology, 84(2), 286.

Reason, J. (1997). Managing the Risks of Organizational Accidents. Ashgate.

United States. Columbia Accident Investigation Board. (2003). Columbia accident investigation board report: Volumes 1 - VI. National Aeronautics and Space Administration. https://sma.nasa.gov/SignificantIncidents/assets/columbia-accident-investigation-board-report-volume-1.pdf

United States. Presidential Commission on the Space Shuttle Challenger Accident. (1986). Report to the president by the Presidential Commission on the space shuttle Challenger accident. National Aeronautics and Space Administration. https://sma.nasa.gov/SignificantIncidents/assets/rogers_commission_report.pdf

Vaughan, D. (1996). The Challenger launch decision: Risky technology, culture, and deviance at NASA. University of Chicago Press.

Zimbardo, P. (2008). The Lucifer effect: Understanding how good people turn evil. Random House Trade Paperbacks.

Zohar, D. (1980). Safety climate in industrial organizations: Theoretical and applied implications. Journal of Applied Psychology, 65(1), 96-102. doi:10.1037//0021-9010.65.1.96