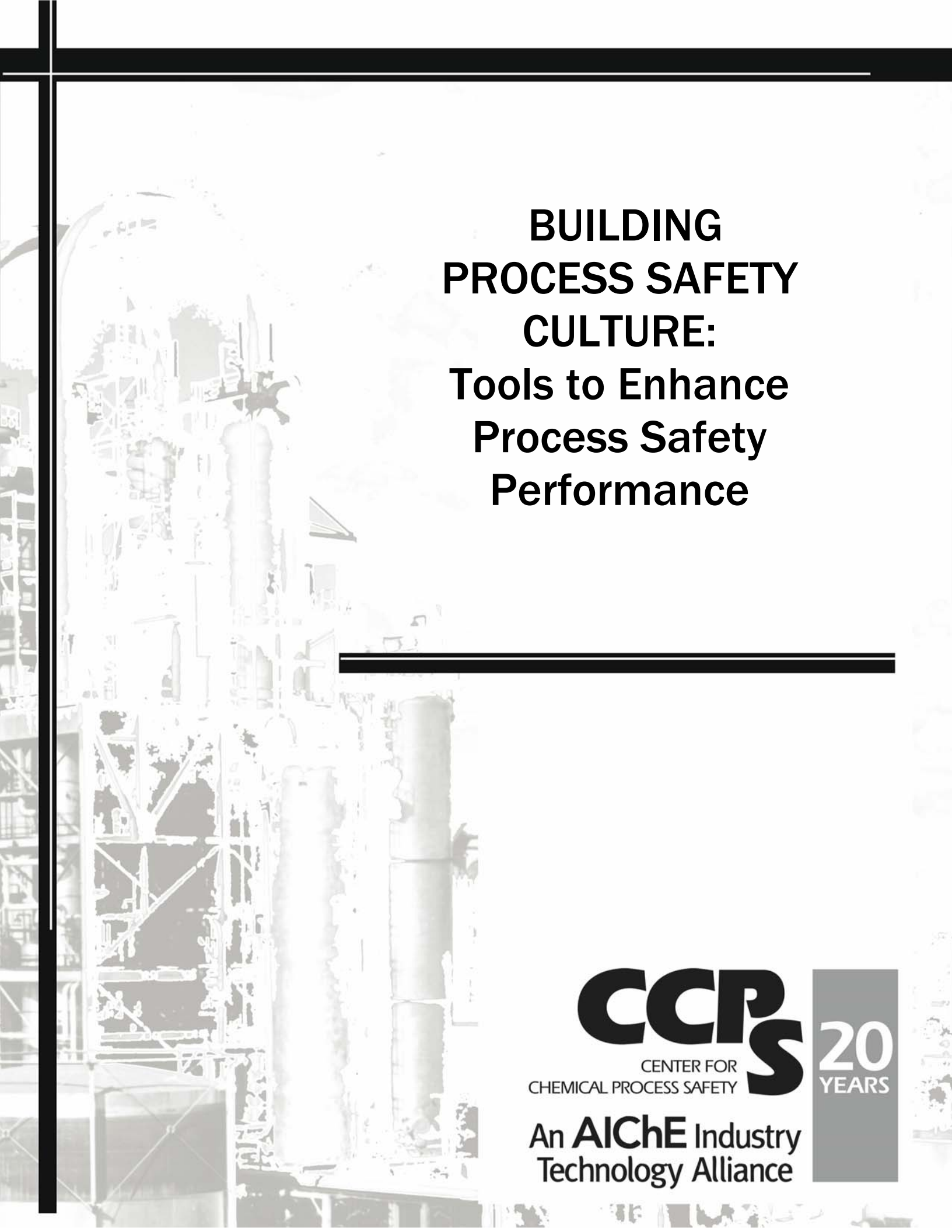


BUILDING PROCESS SAFETY CULTURE: Tools to Enhance Process Safety Performance

CCPS
CENTER FOR CHEMICAL PROCESS SAFETY
20 YEARS
An AIChE Industry Technology Alliance

Process Safety Culture Toolkit

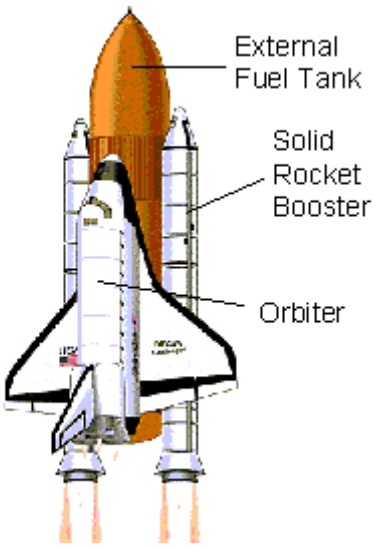
ISBN # 0-8169-0999-7

It is sincerely hoped that the information presented in this document will lead to an even more impressive safety record for the entire industry; however, neither the American Institute of Chemical Engineers, its consultants, CCPS Technical Steering Committee and Subcommittee members, their employers, their employers' officers and directors, warrant or represent, expressly or by implication, the correctness or accuracy of the content of the information presented in this document. As between (1) American Institute of Chemical Engineers, its consultants, CCPS Technical Steering Committee and Subcommittee members, their employers, and their employers' officers and directors, and (2) the user of this document, the user accepts any legal liability or responsibility whatsoever for the consequence of its use or misuse.

Challenger Case History

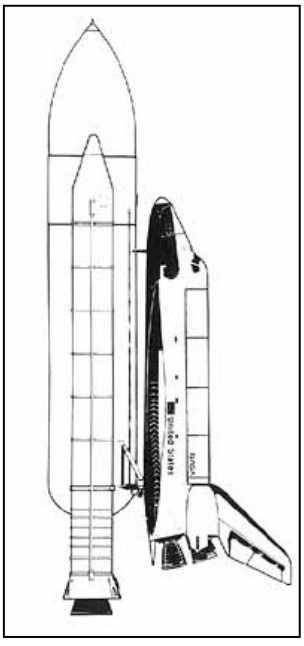
[The following information has been taken from the US government publication *Report of the Presidential Commission on the Space Shuttle Challenger Accident* (the Rogers Commission report).]

The Challenger space shuttle lifted off from launch pad 39B at Cape Kennedy at 11:38 a.m. EST, January 28, 1986. Aboard were seven crewmembers, including schoolteacher Christa McCaulliffe. 73 seconds later, the shuttle was destroyed in a catastrophic explosion, killing all seven astronauts.



Just 0.7 seconds after ignition of the solid fuel booster rockets, even before the shuttle had cleared the launch tower, a field assembly joint in the right-hand solid rocket booster (SRB) began to fail, leaking hot combustion gases from the booster. Subsequent examination of photos taken during lift-off revealed a series of puffs of dark smoke discharging from the joint.

Neither the shuttle crew nor the ground crew was aware of the problem. Even had they been aware, there would have been no means of aborting the take-off, or rescuing the astronauts, during the launch. Once the solid rocket boosters are ignited, there is no way of turning them off.



The leak from the booster rocket field joint continued to grow, impinging upon the lower portion of the external fuel tank. The external fuel tank contained (in separate vessels) the liquid hydrogen and liquid oxygen fuel that powered the shuttle's main engines. At about 65 seconds into the mission, the liquid hydrogen tank began to leak.

At about 73 seconds, the hydrogen tank failed catastrophically, and the liquid oxygen tank failed shortly thereafter. Within milliseconds, the explosively burning hydrogen and oxygen enveloped Challenger. Challenger broke into several large sections (photo on next page). The solid rocket boosters broke free and erratically flew about until Ground Control issued the remote destruct command. The main engine/tail section (with engines still burning), one wing, and the forward fuselage could be identified as they exited the fireball. It is believed that the crew module remained intact until it slammed into the sea.

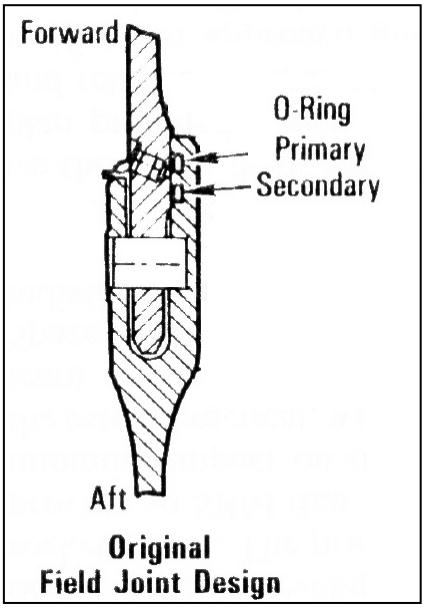
The costs of the incident were enormous:

- All seven astronauts were killed.
- A 3 billion dollar spacecraft was destroyed.
- The space shuttle program was interrupted for nearly three years until the cause of the incident could be investigated and necessary shuttle design modifications, and management system changes, could be implemented.

The subsequent investigation revealed the following:

- Concerns about the integrity of the field joint arose as early as 1982, and actual erosion of field joint O-rings, originally limited to the primary O-ring, had first been detected over two years prior to the last launch of Challenger. While erosion of the primary O-ring was initially viewed with concern by both NASA managers, and the staff of the SRB manufacturer (Thiokol), pressures placed upon maintaining mission schedules resulted in a gradual acceptance of primary O-ring erosion as an "acceptable risk". This risk acceptance was due, in part, to the confidence placed in the secondary O-ring to prevent releases from the joint.
- Later missions experienced erosion of both the primary and secondary O-rings. Erosion of the secondary O-rings rekindled concern on the part of engineers at Thiokol. However, NASA and Thiokol management grew to regard some erosion of both O-rings as being "routine," since no serious equipment damage had yet resulted, and no mission had been impacted, by the degree of O-ring erosion observed up to that time.
- In effect, a pattern arose where the degree of "acceptable" O-ring erosion gradually increased as more severe O-ring erosion was observed. More severe erosion, in the absence of general damage to the SRB, became a "success" that warranted broadening the tolerable degree of erosion. (Another author, writing about the Challenger disaster, described this pattern as “the normalization of deviance.”)
- Unusually cold weather had been experienced at Cape Kennedy on the night prior to the launch. The temperature at the launch pad, on the morning of the launch, was 36 ^{o}F, 17 ^{o}F colder than for any prior launch.
- Thiokol engineers had correlated lower launch temperatures with more severe erosion of both O-rings, and had a basic understanding of why this was the case, based upon the lowered resilience of the elastomer O-rings at lower temperatures. As the pressure inside the SRB increased during launch, the gaps in the field joint increased, and the O-rings were less capable of sealing the widening gaps at lower temperatures. This resulted in combustion gas blow-by, leading to erosion of the O-rings.

- It spite of the above knowledge, no criteria had been established for minimum temperature at launch. A conference call between Thiokol staff and the various NASA offices involved in approving the launch was held the night before the launch. During this call, Thiokol engineers advised delaying the launch until later in the day. In the face of pressure from NASA managers, Thiokol managers overruled their engineers and approved the launch on the original schedule.
- The top administrators at NASA were unaware of the issues related to the technical issues related to the performance of the joint at lower temperatures. NASA site managers did not pass information about Thiokol's concerns up the line within the NASA organization. The Commission concluded that it was likely that NASA management would not have gone forward with the launch if the "had known all the facts."



A number of organizational factors contributed to the failure of communications evident between the technical and management staffs, and the quality of decision-making within the NASA organization. These included, but were not limited to:

- The NASA culture discouraged engineers from reporting concerns to management beyond their immediate supervisor. Thus, a single individual, intentionally or unintentionally, could become a "bad news buffer."
- Managers tended to try to contain problems, attempting to solve them locally without having to report them up the line.
- An atmosphere had developed where many managers perceived the engineers as "crying wolf" while the engineers regarded the managers as being disinterested in their concerns.
- The safety role expected from the Thiokol engineers had been transformed form one where they had to prove the safety of the launch to one where they had to prove that the launch would be unsafe in order to prevent it.
- Pressures to demonstrate that the shuttle was an "operational," as opposed to "experimental," system and, consequently, an unrealistic launch schedule (2 launches per month were scheduled for 1986) resulted in the rationalization of ever-riskier decisions. The Challenger launch, originally scheduled for the summer of 1985, had already been delayed or rescheduled a half dozen times.
- NASA's history of successes in the space program had lulled decision-makers into a false sense of security or invincibility. The "can do" attitude in the organization reduced the awareness, or at least the consideration, of the potential for failure.

- The Commission concluded that NASA's safety system had been "silent" and was characterized by "a lack of problem reporting requirements, inadequate trend analysis, misrepresentation of criticality [of known safety problems], and lack of involvement in critical discussions."