

The Most Dangerous Launch Risk Is the Problem Everyone Has Learned to Work Around

Repeated survival is not proof of safety; it may be evidence that the organization has normalized the warning.

The most dangerous launch risk is often not the defect that failed dramatically.

It is the defect everyone has learned to work around.

Before Challenger, recurring O-ring erosion and blow-by had been treated as acceptable flight risk. The system had survived previous launches, so survival gradually became evidence-wrongly-that the underlying problem was tolerable.

The Commission's lesson is highly relevant to any founder preparing for a consequential product launch: a technical problem becomes more dangerous when the organization stops experiencing it as a problem.

This does not mean every workaround requires delaying launch. It means you need to distinguish manageable debt from accumulated fragility.

A useful way to do that is to examine five signals:

1. Has the workaround become part of the operating model?

If support, implementation, QA, or customers must remember a special sequence to avoid failure, the product may be relying on human compensation for a design weakness. The Shuttle joint was sensitive to multiple interacting conditions-temperature, dimensions, materials, reuse, processing, and dynamic loading. Fragility often hides behind a process that works only when several conditions remain favorable.

2. Is there a pattern in the anomalies?

The Commission found that every flight at or below 63°F showed O-ring distress, while only three of twenty flights at 66°F or above did. The warning was present in the history; the organization failed to perform the trend analysis that would have made it difficult to dismiss.

For your launch, do not ask only, "Has this caused a catastrophic failure?" Ask:

- Which incidents cluster around the same condition?
- Which fixes keep recurring?
- Which alerts, timeouts, data inconsistencies, or manual interventions are increasing?
- What has not failed yet only because someone catches it by hand?

3. Are engineers raising concerns-and can those concerns survive the approval process?

Before Challenger, Thiokol engineering recommended not launching below 53°F. During the final debate, engineers continued to oppose launch, but management reversed the recommendation under pressure.

That is not an argument for treating every engineering objection as decisive. It is an argument for making dissent specific, documented, and visible: What failure mode is being described? Under what conditions? What evidence supports it? What would make the objection go away?

If concerns disappear as they move upward, your process is not reducing risk. It is reducing visibility.

4. What information is missing from the launch decision?

The Commission found that critical information never reached key decisionmakers, and that launch constraints and waivers were not visible across management levels.

Before approving launch, create a plain-language record of known defects, workarounds, unresolved anomalies, owners, conditions that increase risk, and the evidence supporting the decision. A waiver should make risk more explicit-not make it disappear.

5. What happens when the first serious failure occurs?

The Shuttle had no effective way to save the crew after a Solid Rocket Booster failure during first-stage ascent. That made prevention and launch discipline especially important.

Your equivalent question is: if this failure occurs under real customer pressure, can the team detect it, contain it, communicate it, and recover? Or does the launch assume that the system will simply continue behaving as it has during demonstrations?

The Commission ultimately called for redesign, realistic testing, independent technical oversight, formal escalation of dissent, and a flight rate consistent with available resources.

That is the practical standard for your launch too: do not merely ask whether the product works. Ask whether the design has margin, whether the evidence covers realistic conditions, whether dissent is preserved, and whether the team has enough capacity to respond.

Repeated survival is not proof of safety. Sometimes it is proof that the warning has been normalized.