

# Memo: Deciding Whether Reliability Debt Is Launchable

**Repeated survival is not evidence of safety: if known failures, workarounds, and exceptions are becoming normal, the launch decision is already a risk-governance decision-not merely a scheduling decision.**

To: Founder Subject: Deciding whether known reliability problems are tolerable launch debt or launch-threatening fragility Purpose: Establish a disciplined launch decision before schedule pressure turns recurring warnings into accepted risk.

## Bottom line

Do not approve the launch solely because the product demonstrates value and no prior defect has caused a catastrophic failure. The relevant question is whether known problems remain bounded, understood, observable, and recoverable-or whether the organization has begun treating repeated anomalies, workarounds, and temporary fixes as acceptable operating conditions.

The Challenger Commission found that the disaster was not explained by one isolated component failure. A flawed design, sensitivity to conditions, inadequate testing, ignored warning patterns, weakened safety oversight, communication failures, and schedule pressure interacted. The broader lesson is directly relevant to this launch: a system can appear to work until several individually tolerated weaknesses combine under demanding conditions.

## What should change the launch decision

### 1. Treat recurring anomalies as evidence, not background noise

The Commission found that O-ring erosion and blow-by had become accepted as unavoidable and acceptable, even though the historical record showed a strong relationship between distress and low temperature. No trend analysis was conducted that would have exposed the pattern clearly.

For this launch, require a written inventory of known reliability issues-not just open bugs. Include recurring incidents, manual workarounds, temporary fixes, failed recovery steps, and conditions under which each problem becomes more likely. For every item, record:

- What fails or degrades;
- How the team detects it;
- What customer or support impact follows;
- Whether recovery is tested and repeatable;
- Which conditions increase the risk; and
- Who has authority to accept the remaining exposure.

A problem that has repeatedly been survived is not thereby safe. Repetition without resolution may indicate normalization of deviance rather than acceptable performance.

## 2. Separate compliance from adequacy

The Commission found that launch-site activities generally followed approved procedures, yet the deeper design remained inadequate. Following the current process therefore did not prove that the system was safe.

Apply the same distinction here. Ask not only whether the team followed the release checklist, but whether the checklist tests the conditions that make the known failures worse. If a workaround is required, determine whether it is a controlled mitigation with clear ownership or simply a habit that has not yet been challenged.

A "temporary" fix should not remain temporary by default. It needs an explicit expiration, evidence that it works under realistic conditions, and a named decision-maker who accepts the residual risk.

## 3. Preserve dissent and escalate exceptions

Immediately before Challenger, Thiokol engineers recommended against launching below 53°F, and the Commission found that engineers continued to oppose launch while management reversed the recommendation under customer and institutional pressure. Critical information also failed to reach the highest decision-makers because reporting channels contained and diluted it.

Before approving this launch, require the strongest technical objections to be presented directly and recorded without translation into softer language. The launch review should explicitly list:

- Every unresolved reliability concern;
- The engineer or team responsible for each concern;
- The evidence supporting launch and the evidence opposing it;

- Any waiver, exception, or unverified assumption; and
- The specific trigger that would stop or roll back the launch.

Disagreement is not proof that engineers are right. It is evidence that the decision needs better information and explicit judgment. Suppressing or informally resolving dissent removes information from the decision without reducing the underlying risk.

#### **4. Test the failure mechanism, not just the happy path**

The Commission concluded that the joint design was unacceptably sensitive to interacting factors such as temperature, dimensions, materials, reuse, processing, and dynamic loading. Tests showed that sealing was inconsistent under one combination of temperature and gap, and became consistent only at a materially warmer condition. The launch environment exposed a weakness that ordinary experience had not eliminated.

For the product, identify the combinations most likely to turn a manageable defect into a cascading customer failure: load, timing, dependency behavior, degraded infrastructure, unusual input, recovery, and repeated use. Test those conditions deliberately. Demonstrations of the normal path establish value; they do not establish resilience.

Also identify whether a local failure can propagate into loss of containment, widespread unavailability, corrupted customer state, or an inability to recover. Challenger's localized seal failure directed a flame plume onto the external tank and escalated into vehicle destruction. The launch review should similarly distinguish isolated inconvenience from failure modes that spread faster than the team can respond.

#### **Recommended decision rule**

Proceed only if the remaining defects are understood, their conditions and customer consequences are documented, mitigations are tested under realistic conditions, monitoring can detect deterioration early, and an accountable owner has explicitly accepted the residual risk.

Delay the launch-or reduce its scope-if any of the following is true:

- The team cannot explain why a recurring failure occurs or what conditions amplify it;
- A workaround depends on continuous expert intervention;
- A known issue has no tested recovery path;

- A waiver or exception is not visible to all decision-makers;
- Technical dissent is being treated as a request for perfection rather than evidence about uncertainty; or
- Schedule pressure is preventing analysis of existing incidents before the next release decision.

The Commission recommended redesigning a faulty joint, validating the replacement under realistic conditions, providing independent technical oversight, formally documenting constraints and dissent, and setting operating demands consistent with available resources. For this launch, the equivalent is not "fix everything." It is to remove or contain single-point failures, test the riskiest interactions, create an independent challenge to the release decision, and set a launch scope the team can support without relying on optimism.

The cost of delay is visible. The cost of normalizing a warning is harder to see until customers, employees, and credibility absorb it. Make the decision with the warnings fully visible.