

When "Good Enough" Becomes Fragile: A Launch Decision Framework

Repeated survival is not proof of safety; recurring defects can become accepted risks until one more demanding condition exposes the weakness.

Slide 1 - When "Good Enough" Becomes Fragile

A launch decision framework for known reliability problems

- The product works well enough to demonstrate value.
- Known defects, workarounds, and temporary fixes remain.
- The central question is not whether imperfections exist.
- It is whether the organization has begun treating warning signs as normal.

Slide 2 - The Decision You Actually Face

A launch is not simply a choice between:

- Perfect product
- Ship now

The real decision is whether the current system can:

- Operate under realistic launch conditions
- Detect and contain failures
- Respond without overwhelming the team
- Preserve customer and investor credibility
- Learn from anomalies before the next commitment

Slide 3 - What the Challenger Investigation Found

The immediate failure was specific: destruction of the seals in a Solid Rocket Motor joint.

But the catastrophe developed through interacting weaknesses:

- A design sensitive to temperature and other conditions
- Repeated damage treated as acceptable
- Weak trend analysis
- Critical information that did not reach decisionmakers
- Management and schedule pressure
- Insufficient independent safety oversight

Lesson: a visible failure may be local; the conditions that permit it are usually systemic.

Slide 4 - The Dangerous Pattern: "It Hasn't Failed Yet"

The Commission found that recurring O-ring erosion and blow-by had come to be treated as an acceptable flight risk.

The historical record contained a warning pattern:

- Every flight at or below 63°F showed O-ring thermal distress.
- Only three of twenty flights at 66°F or above did.
- No effective trend analysis exposed the growing danger.

For a product launch, repeated survival of a defect should trigger investigation-not automatic reassurance.

Slide 5 - A Failure Can Escalate Through the System

The Challenger sequence illustrates how a small initiating weakness can spread:

1. The seal failed.
2. Smoke appeared immediately after liftoff.
3. A flame became a continuous plume.
4. The plume weakened adjacent structure.
5. A localized problem became vehicle-wide destruction.

Ask of each known product defect:

- What does it directly affect?
- What can it affect next?

- What happens when conditions are worse than normal?
- Is there a recovery step, or does the failure become irreversible?

Slide 6 - Manageable Debt vs. Launch-Threatening Fragility

More likely manageable

- The behavior is understood.
- Its operating conditions are bounded.
- Detection is reliable and early.
- A workaround is documented and tested.
- Ownership and response are clear.
- The team can resolve the issue without disrupting core operations.

More likely launch-threatening

- The defect is sensitive to interacting conditions.
- The warning signal is ambiguous or arrives late.
- Workarounds depend on heroics or memory.
- Failures can cascade across customers or systems.
- The team has repeatedly waived the same concern.
- No one can state who decides when the risk becomes unacceptable.

Slide 7 - Technical Dissent Is Decision Evidence

Before Challenger launched, contractor engineers recommended not launching below 53°F. Engineers continued to oppose launch during the final discussion, but management reversed the recommendation under pressure.

The relevant question is not:

> "Are the engineers being too cautious?"

It is:

> "What evidence would prove them wrong, and has that evidence been gathered?"

A launch decision should preserve dissent, not convert it into an informal waiver.

Slide 8 - Do Not Let Risk Disappear in the Reporting Chain

The Commission found that crucial information never reached top launch decisionmakers. It also found no system that made launch constraints and waivers visible across management levels.

For this launch, require a single decision record containing:

- Known reliability issues and current severity
- Conditions that increase failure likelihood
- Customer and operational consequences
- Workarounds, owners, and response limits
- Open dissent and unresolved objections
- Explicit waivers, expiry dates, and escalation triggers

If a concern matters enough to discuss, it matters enough to document.

Slide 9 - Schedule Pressure Changes What the Organization Can See

The Commission found that an accelerated flight schedule strained training, maintenance, analysis, and logistics. The system could not fully analyze all flight data before subsequent launches.

The product equivalent is a launch cadence that leaves no time to:

- Investigate incidents and near-misses
- Analyze recurring defects
- Validate fixes under realistic conditions
- Prepare support and operational response
- Restore capacity after an emergency

A faster launch is not faster if it prevents the organization from learning between releases.

Slide 10 - The Governance Safeguards to Put in Place

Before launch:

- Assign an independent technical reviewer or review group.
- Make reliability, quality, and incident trends visible to the final decisionmaker.

- Require formal documentation of launch constraints and waivers.
- Include the people responsible for operating and supporting the product.
- Test the replacement or fix under realistic conditions-not only ideal ones.
- Set a launch threshold tied to available team capacity.

These controls are not a demand for perfection. They are protection against information loss and normalized risk.

Slide 11 - The Founder's Launch Gate

Proceed only when you can answer "yes" to the following:

- Do we understand the known failure modes?
- Have we tested the product under the conditions most likely to expose them?
- Can we detect failure before customers bear the full consequence?
- Are workarounds reliable, documented, and staffed?
- Has dissent reached the actual decisionmaker?
- Are waivers explicit rather than implicit?
- Can the team respond without exhausting its ability to operate?

If the answer is "no," the issue is not merely technical debt. It is decision risk.

Slide 12 - Final Principle

The Challenger Commission's broader lesson was not that one component failed.

It was that design weakness, recurring anomalies, communication failures, organizational pressure, and schedule demands interacted until a known problem became catastrophic.

For this launch:

> Do not ask whether the product has survived its known defects. Ask whether the organization has built a credible way to detect, contain, learn from, and govern them.

That is the difference between a calculated launch and a normalized gamble.