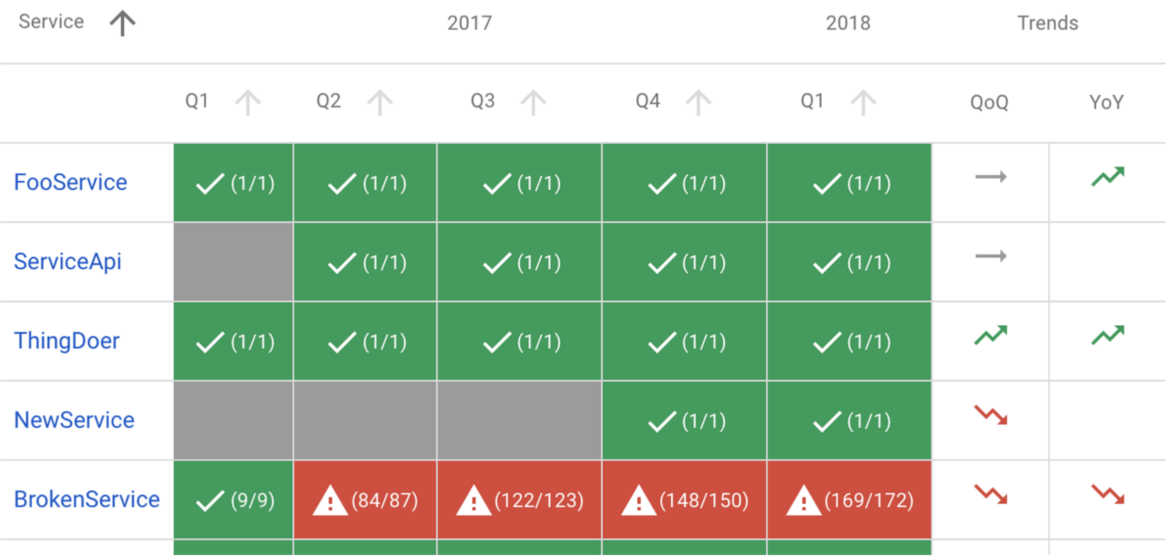
STPA at Google

Tim Falzone (Google), John Thomas (MIT)

This work was made possible through a partnership between Google and SES

Existing tools: Service-level Reliability vs Safety



Service ↑	2017				2018	Trends	
	Q1 ↑	Q2 ↑	Q3 ↑	Q4 ↑	Q1 ↑	QoQ	YoY
FooService	✓ (1/1)	✓ (1/1)	✓ (1/1)	✓ (1/1)	✓ (1/1)	→	↗
ServiceApi		✓ (1/1)	✓ (1/1)	✓ (1/1)	✓ (1/1)	→	
ThingDoer	✓ (1/1)	✓ (1/1)	✓ (1/1)	✓ (1/1)	✓ (1/1)	↗	↗
NewService				✓ (1/1)	✓ (1/1)	↘	
BrokenService	✓ (9/9)	⚠ (84/87)	⚠ (122/123)	⚠ (148/150)	⚠ (169/172)	↘	↘

Google’s need for STPA

Our current hazard analysis technique:

- Models of concrete implementations of system (RPC diagrams, etc.)
- Accident causality often explained by linear cause and effect ("root cause of an outage")
- Search for general safety requirements by studying specific events
- Focussed on *feasibility* ahead of *effectiveness*
- Quality of the result depends on the experience level of the engineers and their knowledge of the system

What we want:

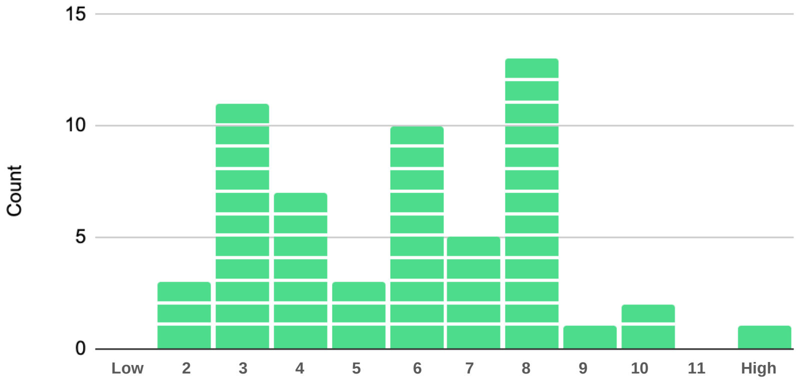
- Proactively find risks
- Comprehensive system scope
- Tuned for high complexity systems, with a holistic approach to identifying risks - especially in the seams between services
- Can be applied to *new* and *existing* systems
- Decouple hazard identification from solutions
- Teachable, reusable framework

Project Motivation

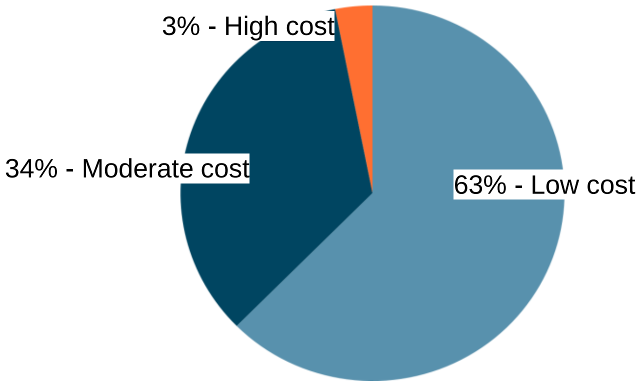
Can STPA provide relevant information and insights to **prevent** losses at Google?

STPA Study Results

- Time-constrained: 2 engineers worked for 5 weeks part-time on STPA analysis (with support)
- 30+ major subsystems analyzed, 10+ teams of engineers interacting across the system
- STPA identified **56 causal scenarios** that demonstrated weaknesses in the system
- The STPA scenarios and identified weaknesses were compared to past events, **especially one major incident**
- STPA found all of the defects that were identified in the post-incident report, and would likely have prevented **at least 4 other major incidents** (and many moderate & minor incidents)



Severity of STPA Scenarios

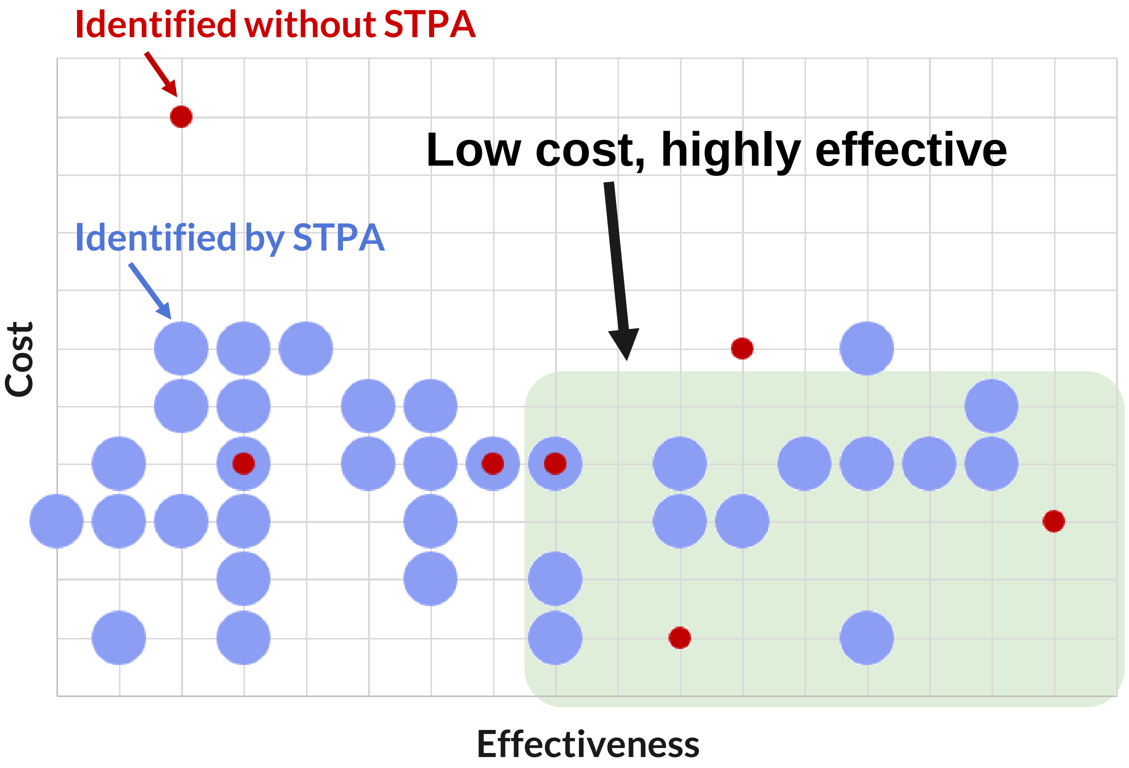


Cost to address STPA Scenarios

Effective solutions and recommendations

STPA found 7 of the 9 solutions identified in the original incident review.

In addition, STPA found a much larger number of solutions, many of which are low cost and highly effective.

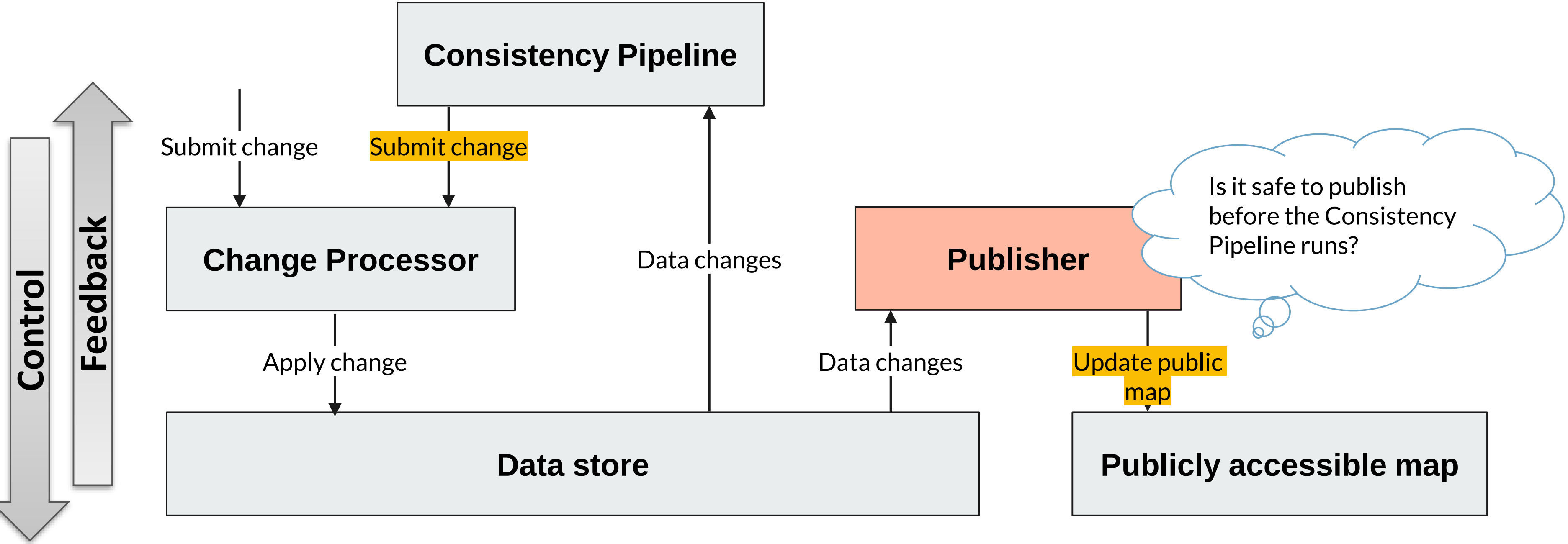


Google engineers estimated cost and effectiveness based on experience and the number of scenarios they would prevent

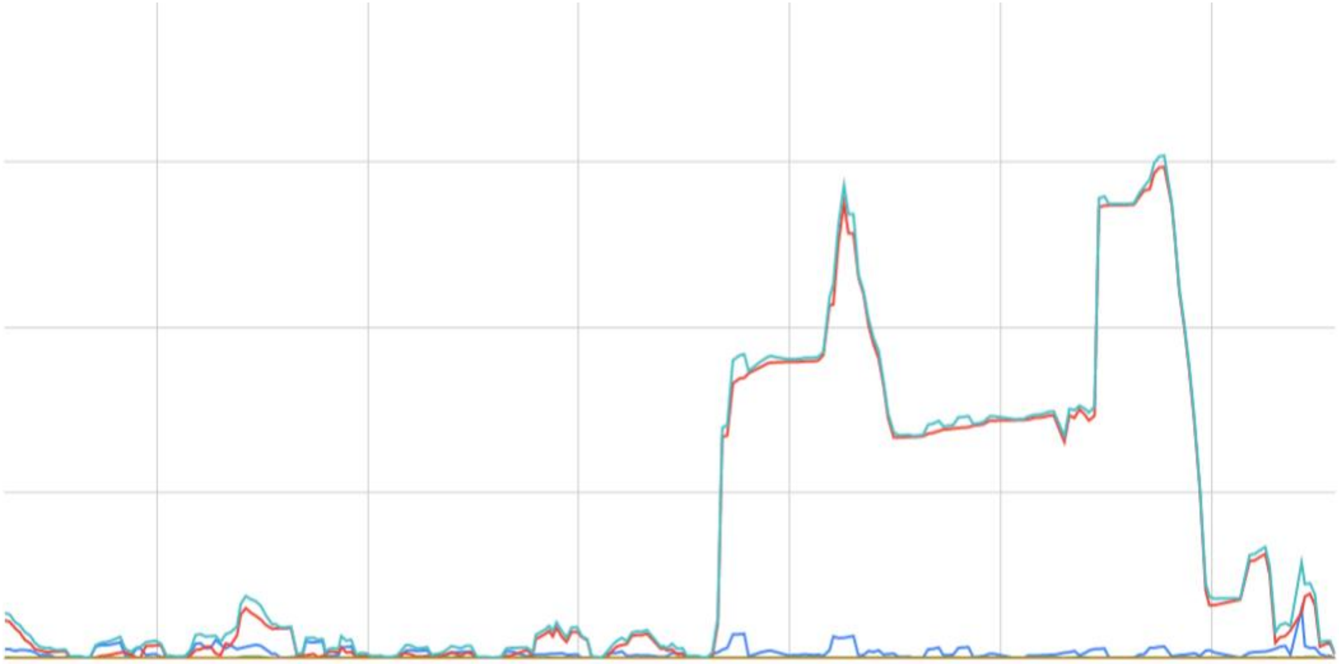
Examples of STPA Insights

Disclaimer: The full analysis is not releasable.
The following has been simplified for public release.

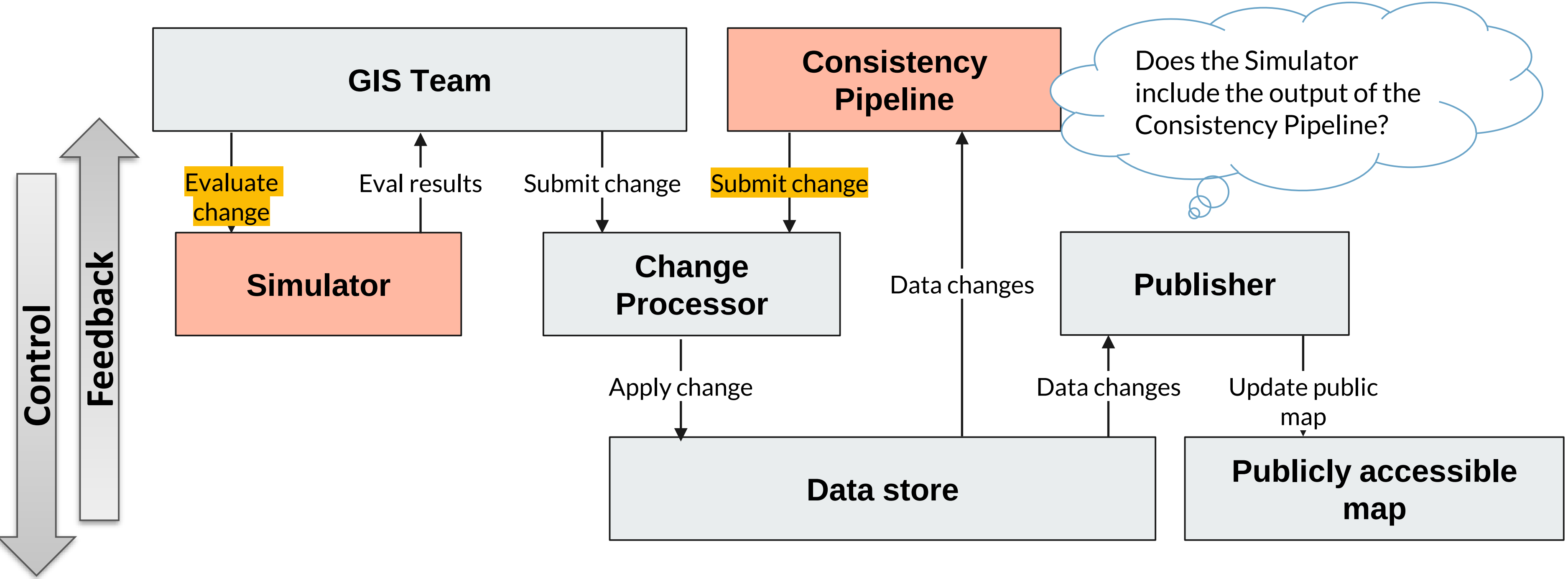
Control Loop Insights: Automated control loops



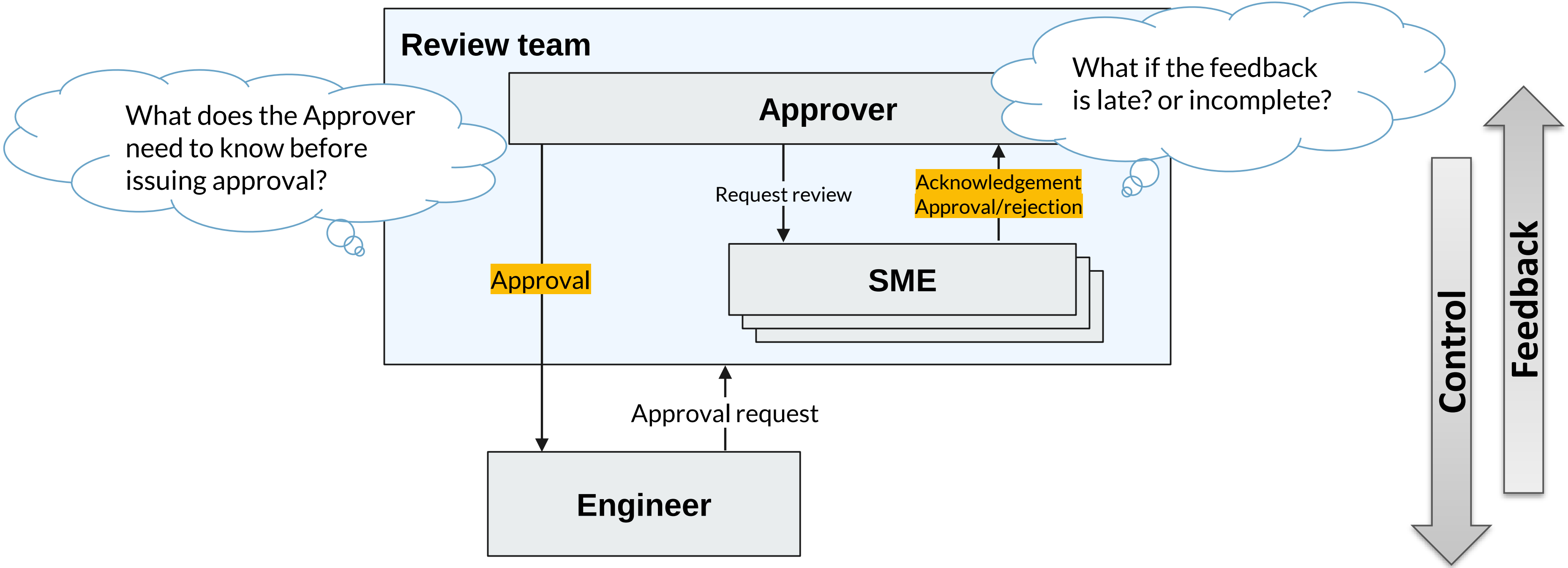
Inconsistency levels vary over time



Control Loop Insights: Hybrid control loops



Control Loop Insights: Human control loops



New solutions enabled by STPA

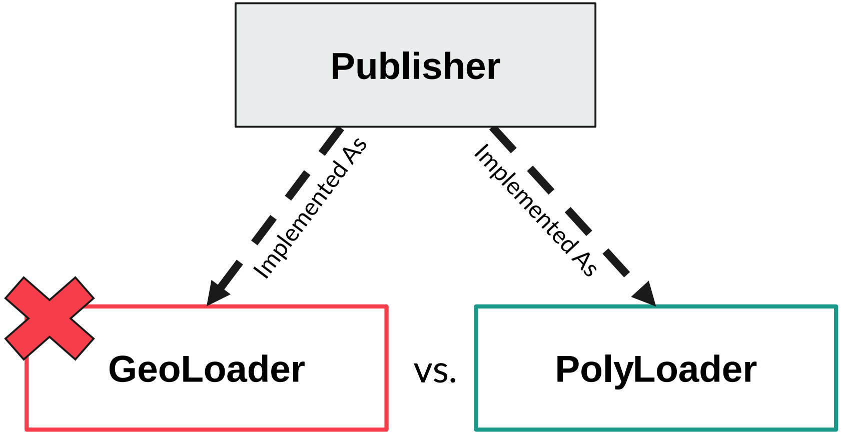
Analysis results led to prioritized engineering projects to address safety problems:

- Elimination of the Consistency Pipeline altogether
- Improvements to the approval process
- Investment in better methods of simulation and experimentation
- Different (more useful) quality measurements

Generalizability of STPA Results

Is the STPA analysis still relevant when the implementation of the Publisher changes?

Yes! The Publisher responsibilities were simply moved to a new software module.



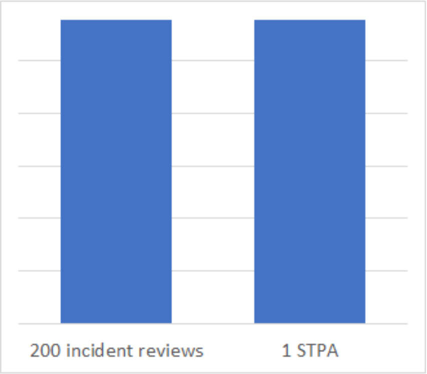
Rate of Learning

Before trying STPA, most learning came from incidents (post-facto).

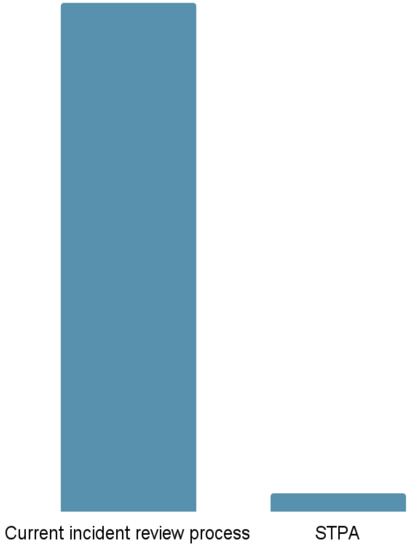
This project provides the evidence that learning can occur beforehand using STPA at a **much lower cost**.

STPA also generated more recommendations per incident than our current incident review process.

Value from the insights generated

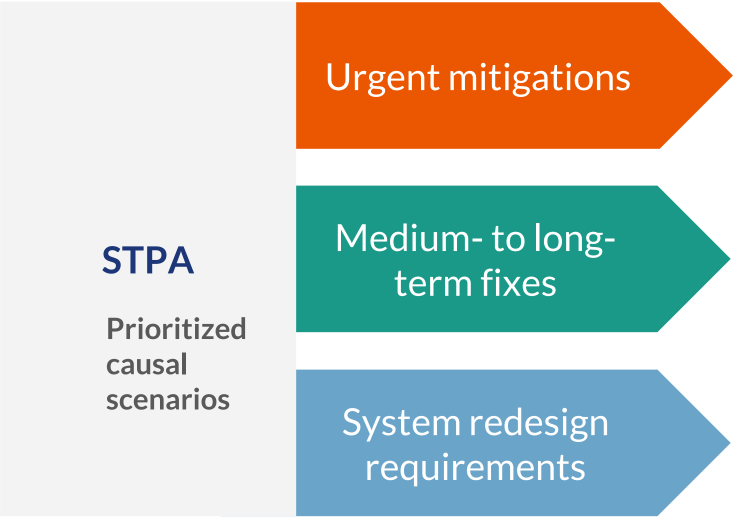


Cost to analyze 200 incidents



Google engineers evaluated insights, information content, and value based on their experience

STPA produced a variety of solutions



STPA

Prioritized causal scenarios

Urgent mitigations

Manual process changes, immediate patches, etc.

Often captured as the high priority action items in a post-incident investigation.

Medium- to long-term fixes

Process automation, monitoring and software changes, etc.

System redesign requirements

Large-scale redesign to dissolve safety problems.

STPA provides the system safety requirements.

Insights about STPA

Process insights

Start with the control structure, and think through how decisions are made in the system.

Hazards in the system are the anti-goals of the system -- get people thinking about the system goals. This was immediately useful.

The things at the top of the hierarchy have the broadest view of the safety requirements of the system. We had a hard time explaining control actions to non-STPA folks until we put it in these terms.

Stakeholder insights

Make the value proposition very simple: prevent large incidents, including novel ones.

The methodology works well on both new systems that are being designed and existing systems.

Sharing insights

The abstraction in the model is hard for people -- they want to put every component of the system on the diagram. Get them thinking about decisions and goals instead of data flow.

One of the major values of STPA for us was the identification of system safety requirements. These requirements are valuable to engineering teams and can increase velocity by helping clarify problems.

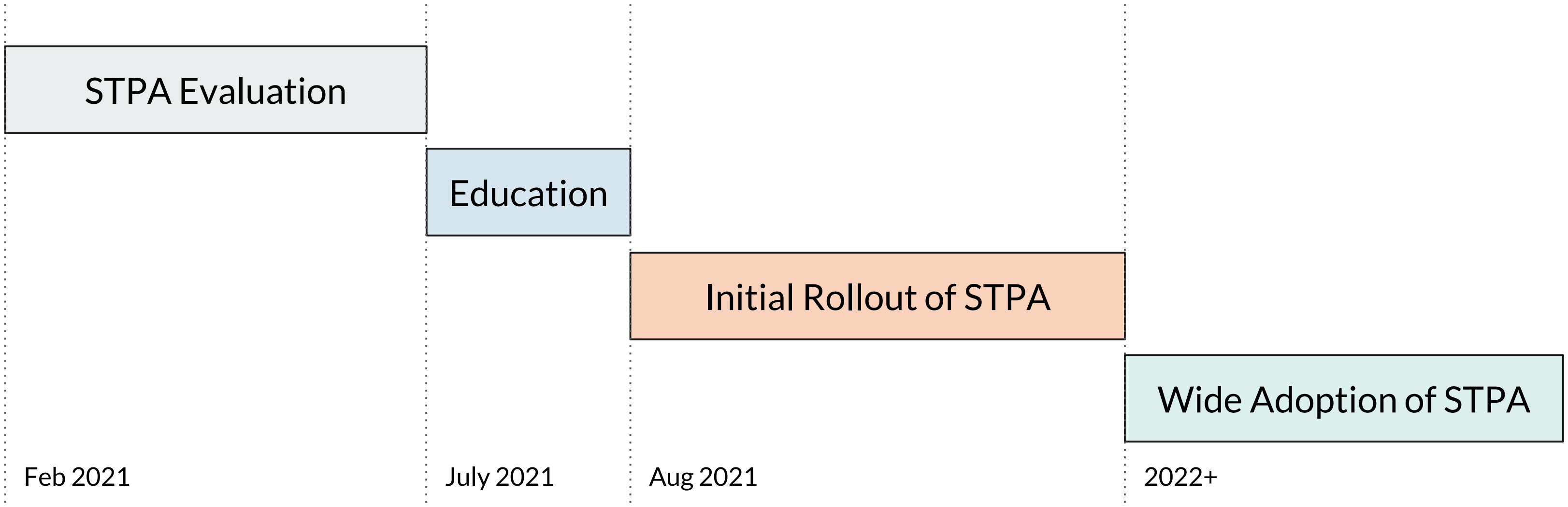
Comments

"My team is explicitly being given the scope of Data Reliability, among other items. I view [STPA] as fundamental to developing a long term strategy for keeping risk in check for the whole system and for data changes specifically."

"It's not that any one thing in this set of results is necessarily new to us. But we've never seen it all in one place before. It's scary to see it all at once."

Note: The STPA evaluation was limited and intended to study application suitability, not to produce new design insights. The fact that it did produce new conclusions and impacted real design decisions was beyond expectations for the limited initial pilot.

Google's next steps with STPA



STPA Evaluation

Education

Initial Rollout of STPA

Wide Adoption of STPA

Feb 2021

July 2021

Aug 2021

2022+