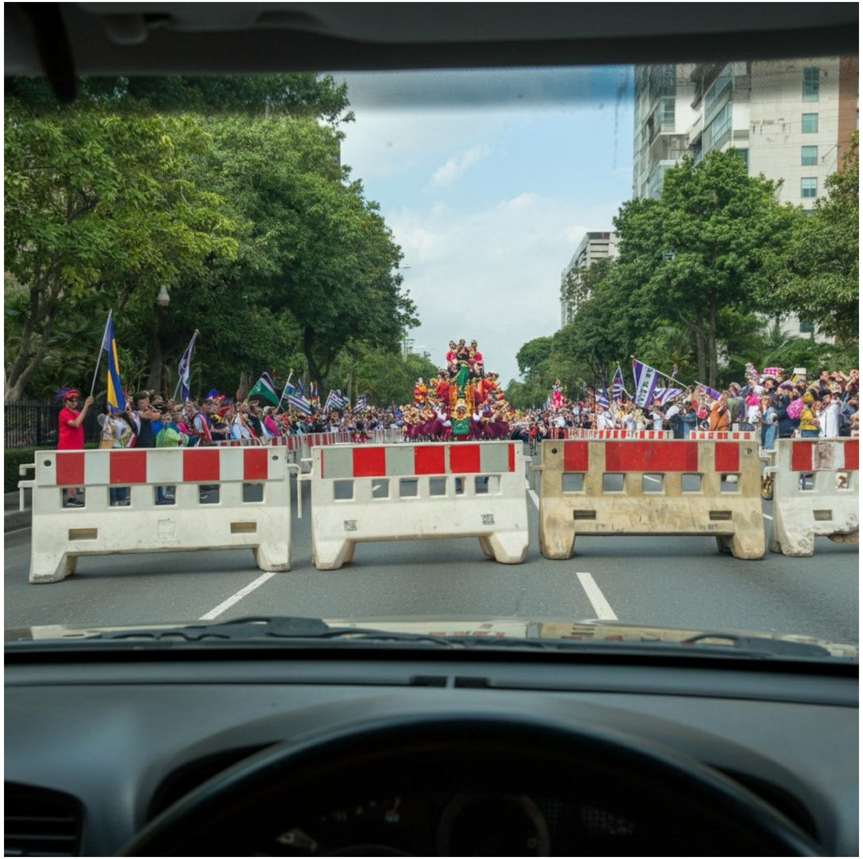
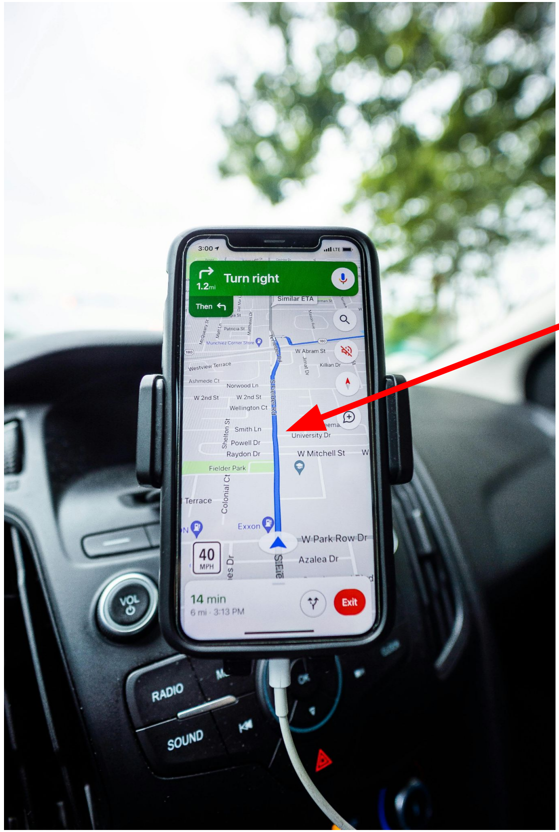
Mapping a Better Future with STPA

Geo Data SRE

Theo Klein (pikle@google.com)

SREcon, March 25 2025





Should be marked as closed, but isn't

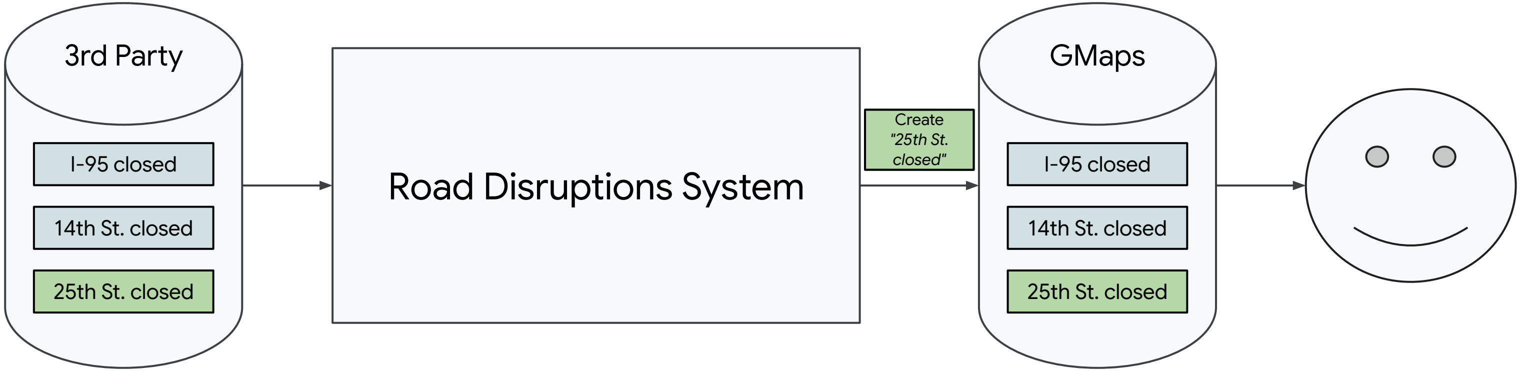
- Losses caused by component failures
  - Reliability problem

Traditional Focus

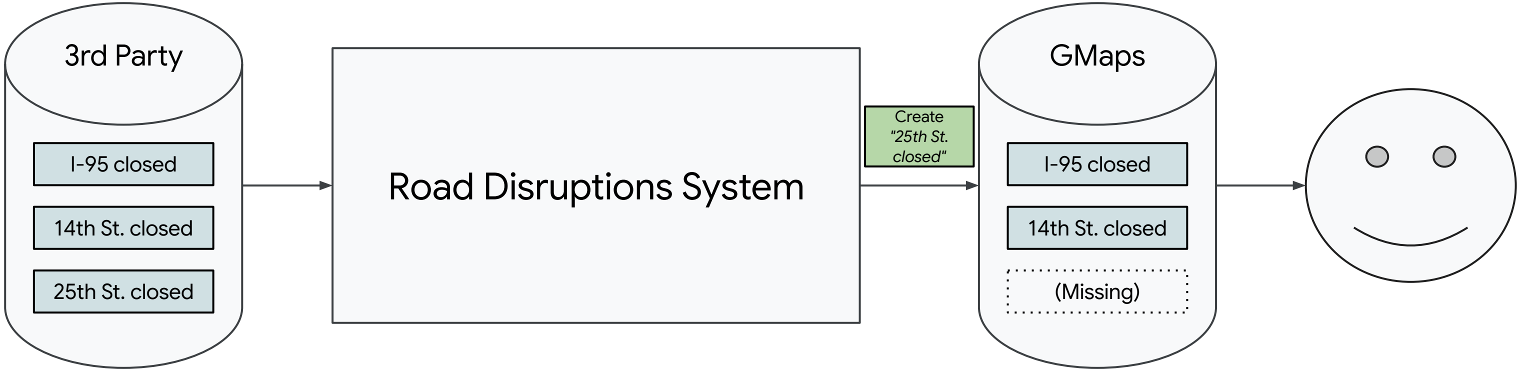
- Losses caused by component interactions
  - Often occur without component failures
  - Can be much more difficult to anticipate

Focus of new methods

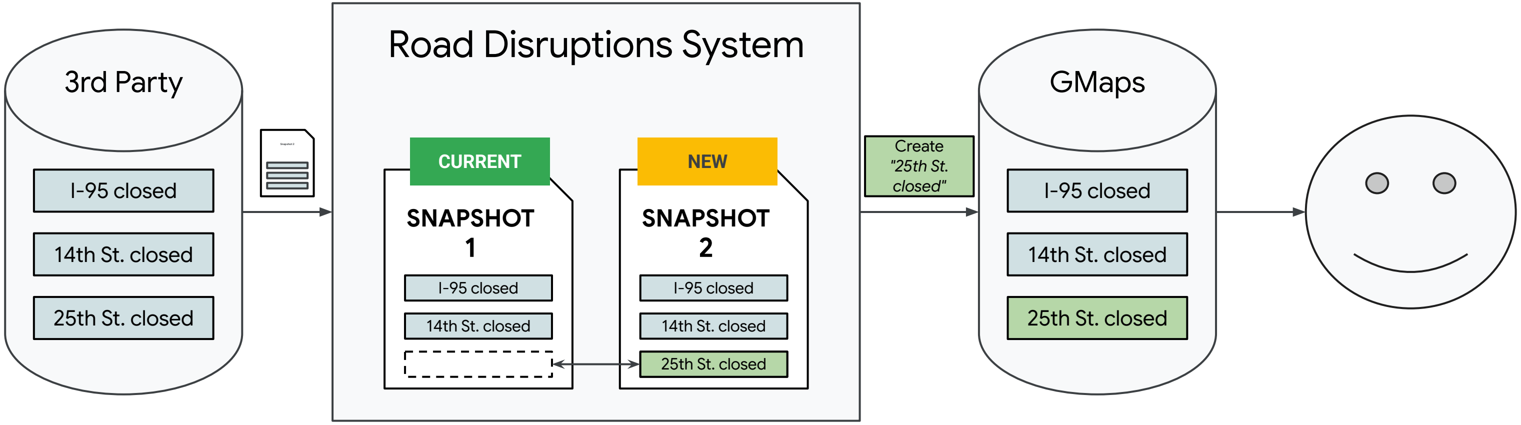
John Thomas, 2021, System Safety and STPA Class Materials


3rd Party
I-95 closed
14th St. closed
25th St. closed
Road Disruptions System
Create "25th St. closed"
GMaps
I-95 closed
14th St. closed
25th St. closed

Google



3rd Party
I-95 closed
14th St. closed
25th St. closed
Road Disruptions System
Create
"25th St. closed"
GMaps
I-95 closed
14th St. closed
(Missing)



3rd Party

I-95 closed

14th St. closed

25th St. closed

Road Disruptions System

CURRENT

SNAPSHOT 1

I-95 closed

14th St. closed

NEW

SNAPSHOT 2

I-95 closed

14th St. closed

25th St. closed

Create *"25th St. closed"*

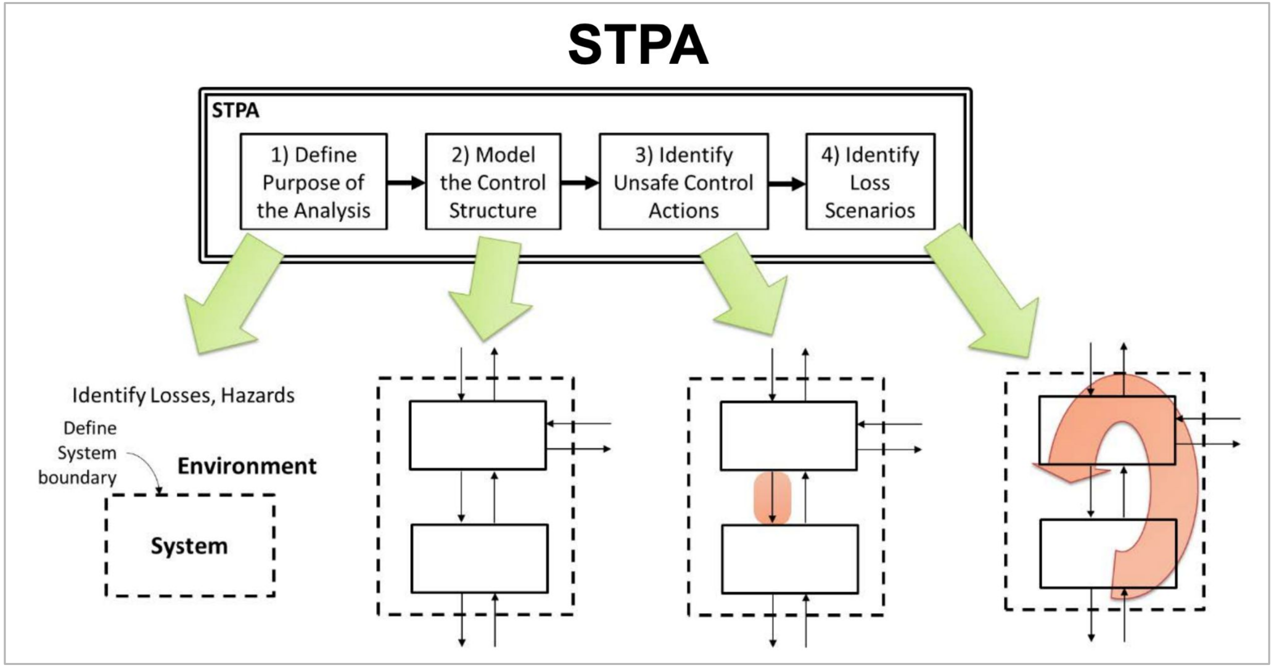
GMaps

I-95 closed

14th St. closed

25th St. closed

WARNING
STPA
AHEAD


STPA
STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
Identify Losses, Hazards
Define System boundary
Environment
System

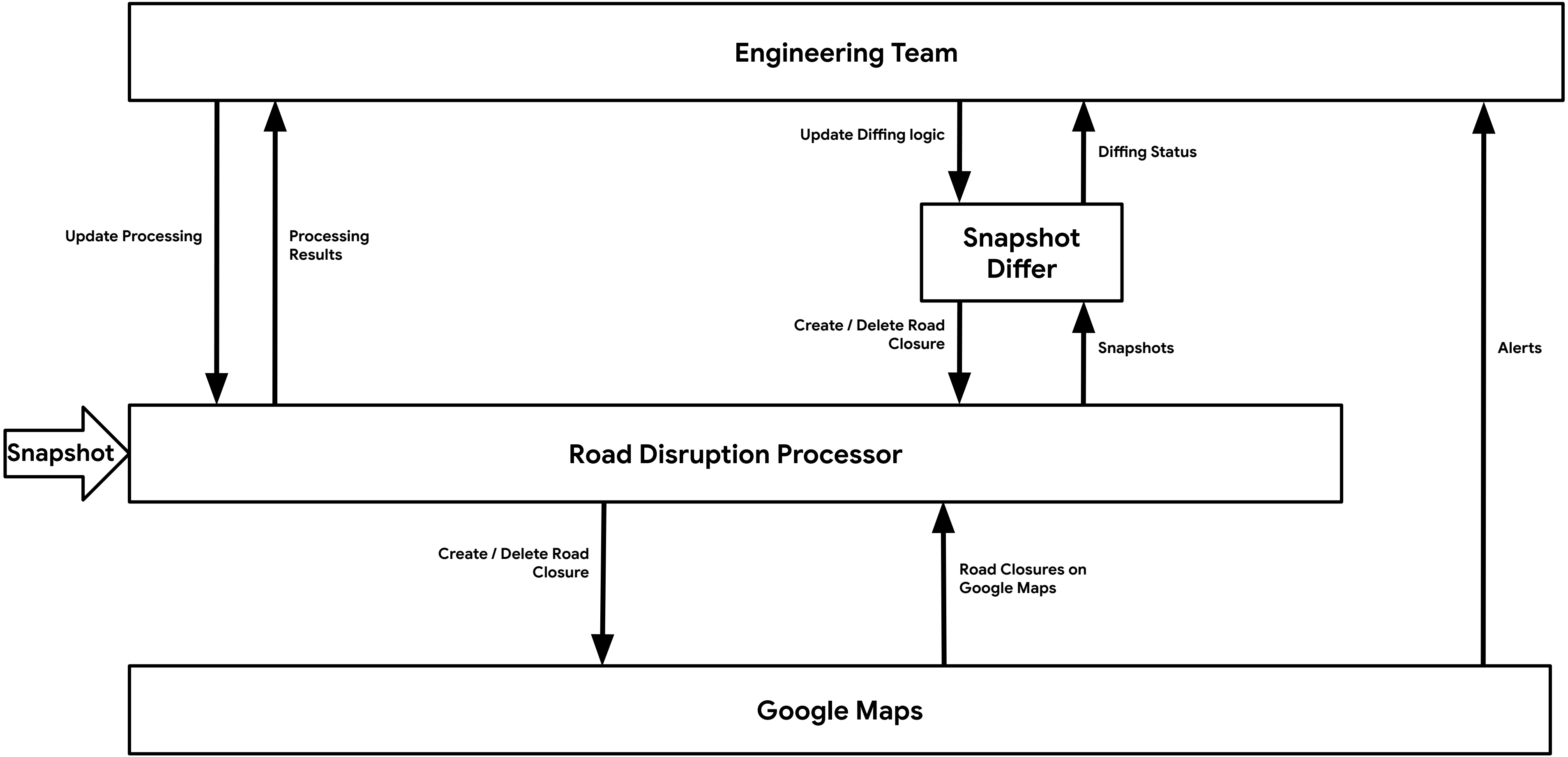
Step 1: Purpose of Analysis

Road Disruptions System

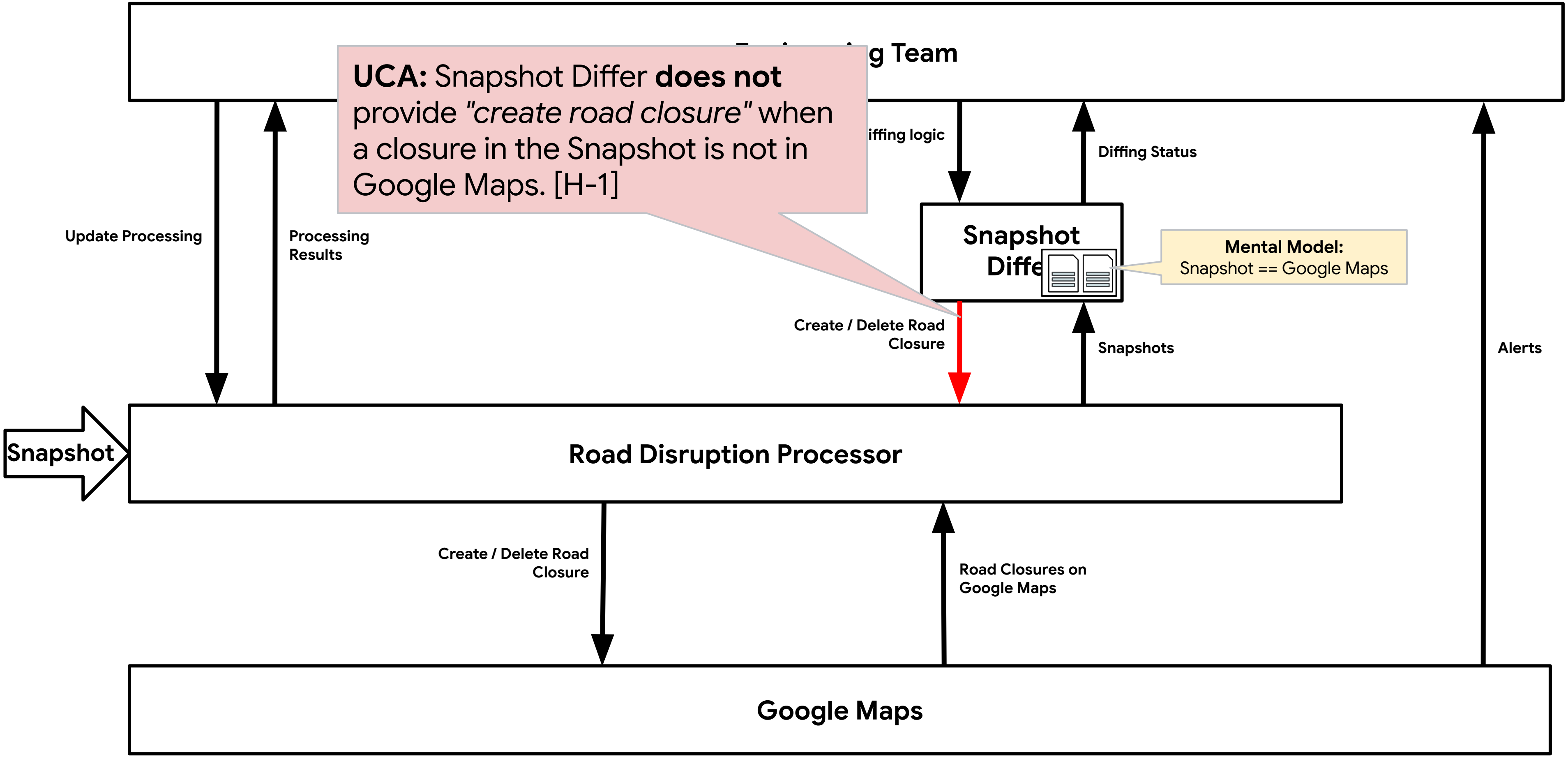
Goal	● Ensure that Google Maps contains the latest state of all 3rd Party Closures
Losses	● L-1: Loss of User Trust ● L-2: Loss of Mission ● L-3: Negative PR Events
Hazards	● H-1: Google Maps is out of sync with 3rd Party Closures. [L-1, L-2, L-3]
System Constraints	● SC-1: Google Maps must be in sync with 3rd Party Closures. [H-1] ● SC-1.1: If it is out of sync, then the system must provide the means to detect and correct this condition. [H-1]

Google

Step 2: Control Structure



Step 4: Loss Scenario



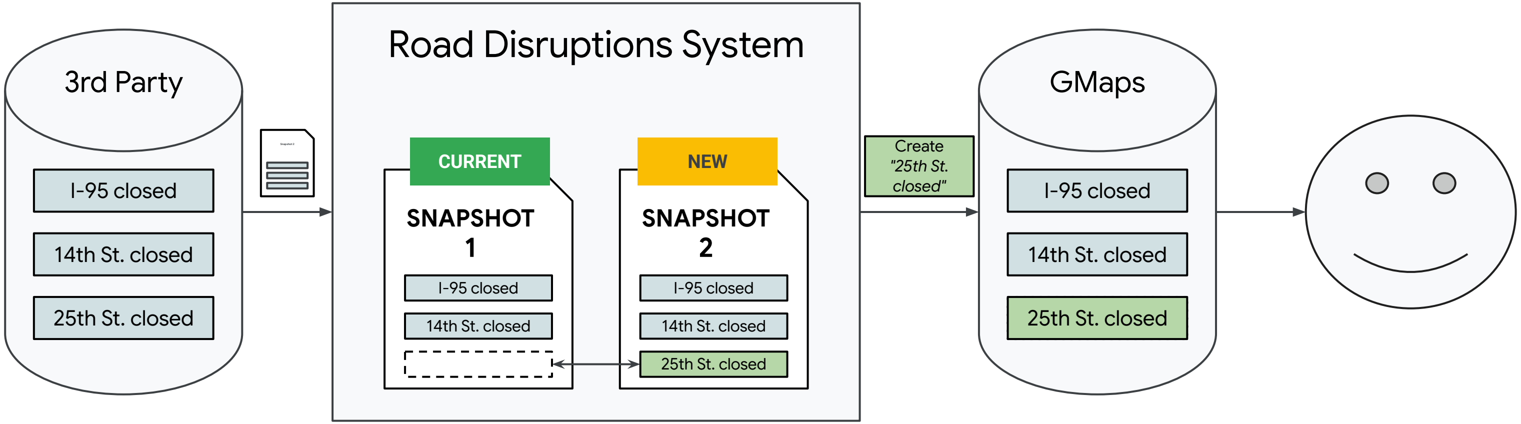
UCA: Snapshot Differ **does not** provide *"create road closure"* when a closure in the Snapshot is not in Google Maps. [H-1]

Mental Model:
Snapshot == Google Maps

Google

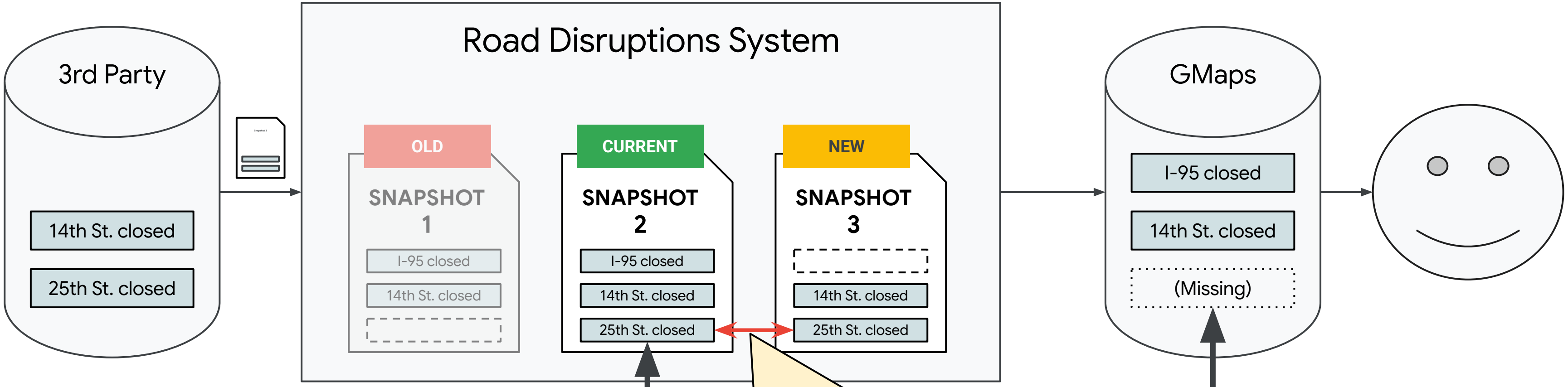
Step 4: Loss Scenario

UCA: *Snapshot Differ* ***does not*** *provide "create road closure" when a closure in the Snapshot is not in Google Maps.*



Step 4: Loss Scenario

UCA: *Snapshot Differ* ***does not*** *provide "create road closure" when a closure in the Snapshot is not in Google Maps.*

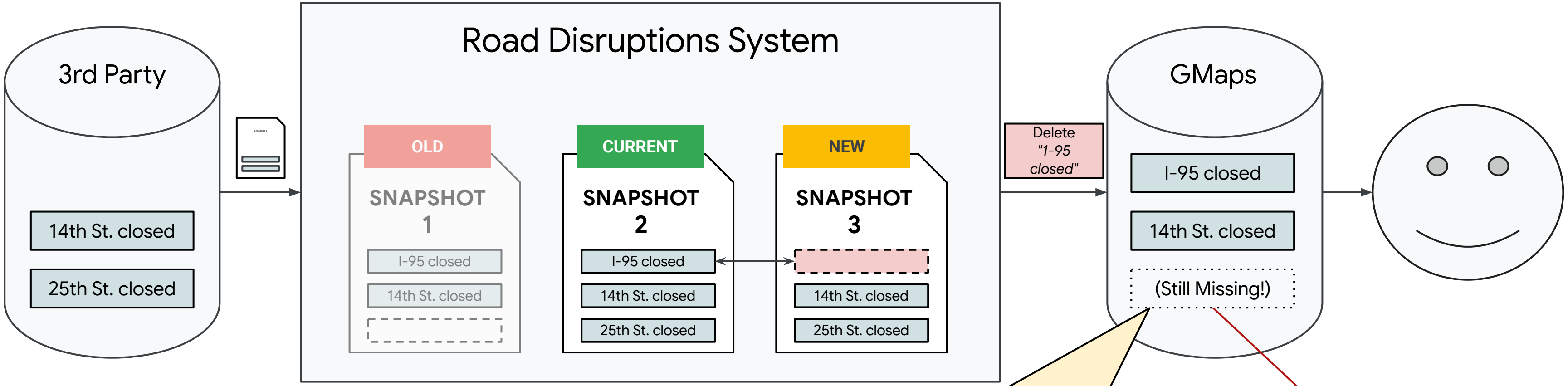


No diff for ***25th st. closure***!

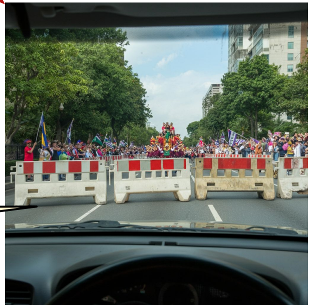
Road Disruptions System incorrectly assumes that the 25th street closure exists in Google Maps!

Step 4: Loss Scenario

***UCA:** Snapshot Differ **does not** provide "create road closure" when a closure in the Snapshot is not in Google Maps.*



Road Disruptions System will never re-attempt to close 25th street.

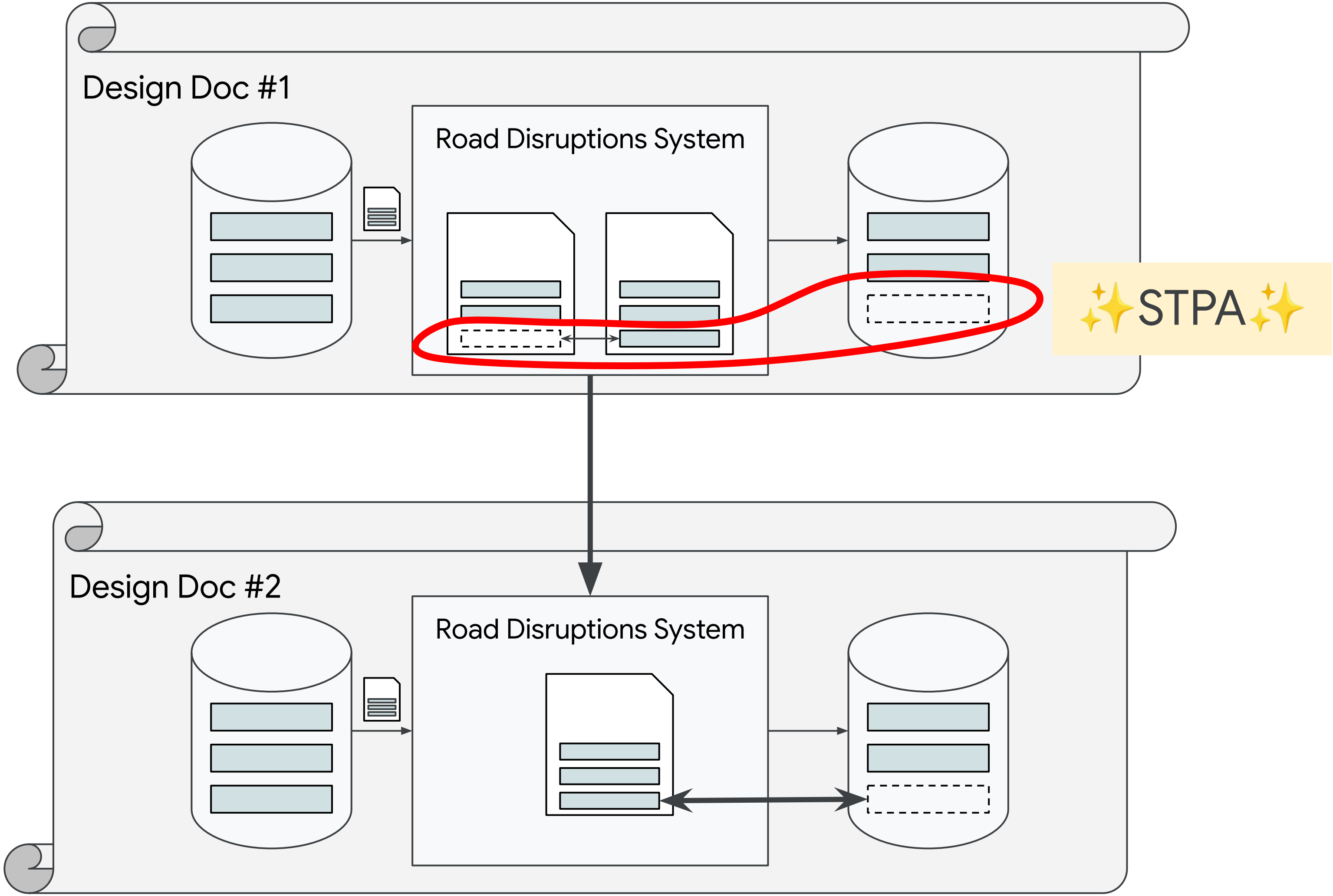


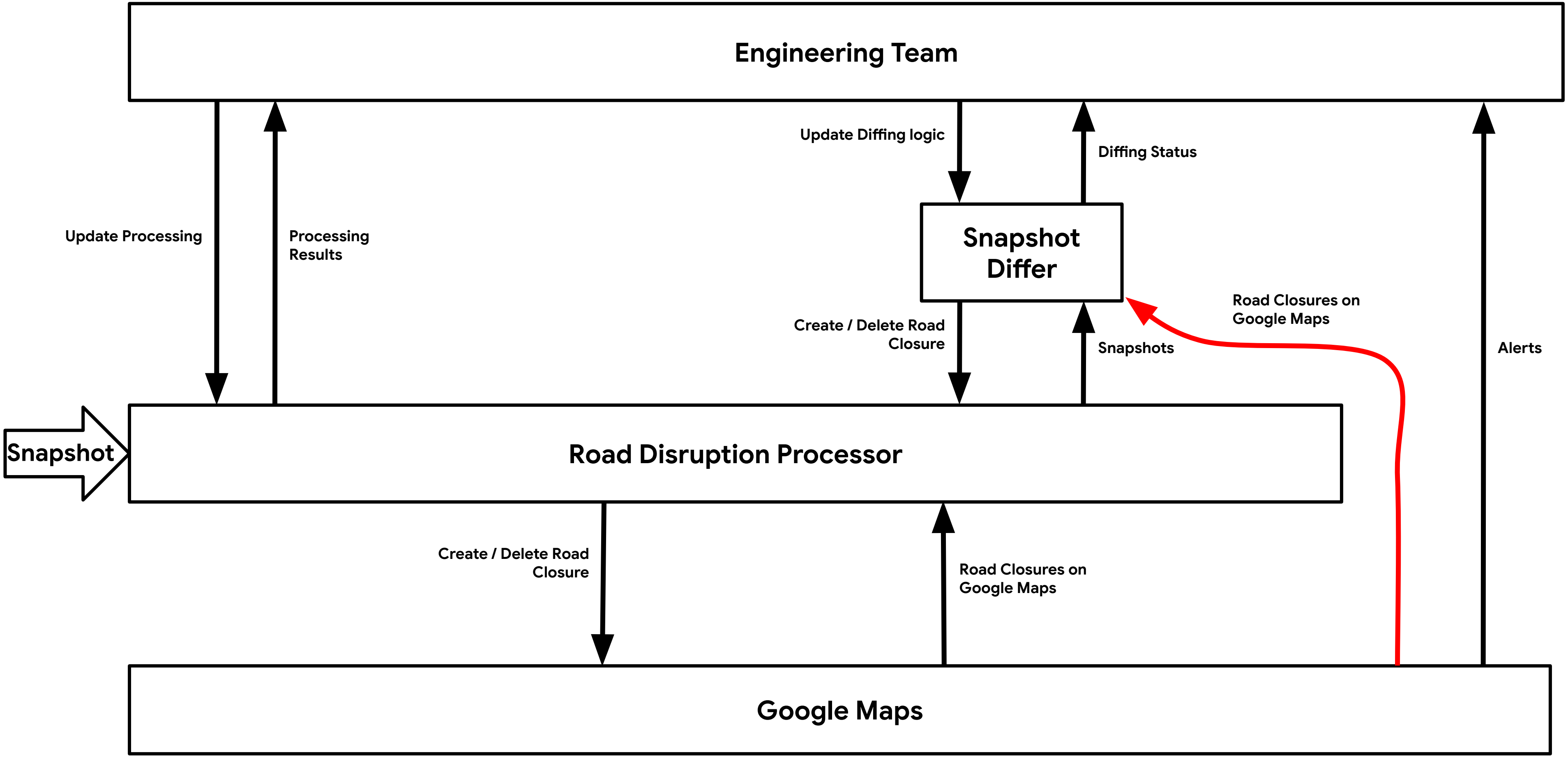
This is our loss.

No component failed.

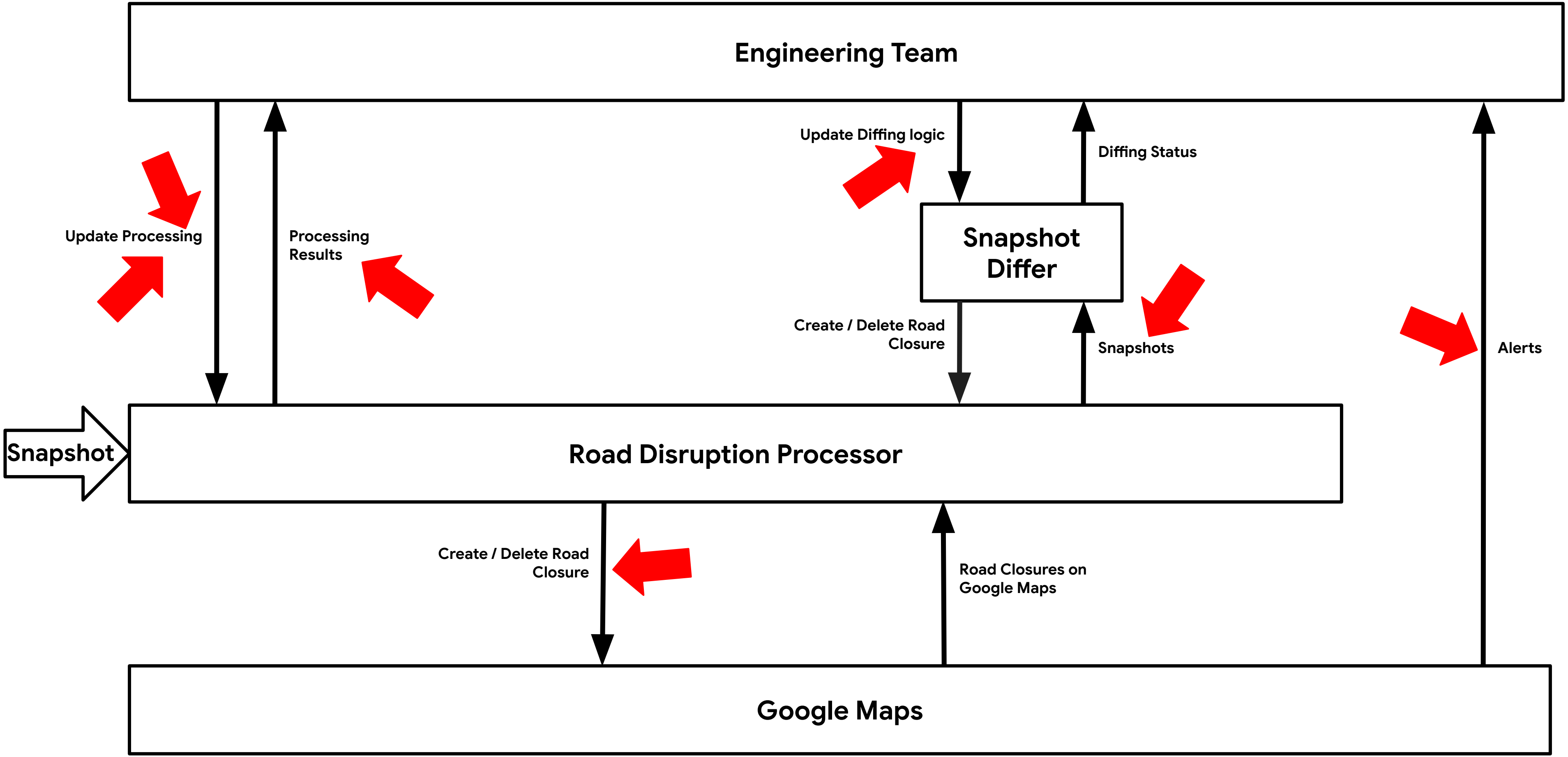
Every component operated as designed.

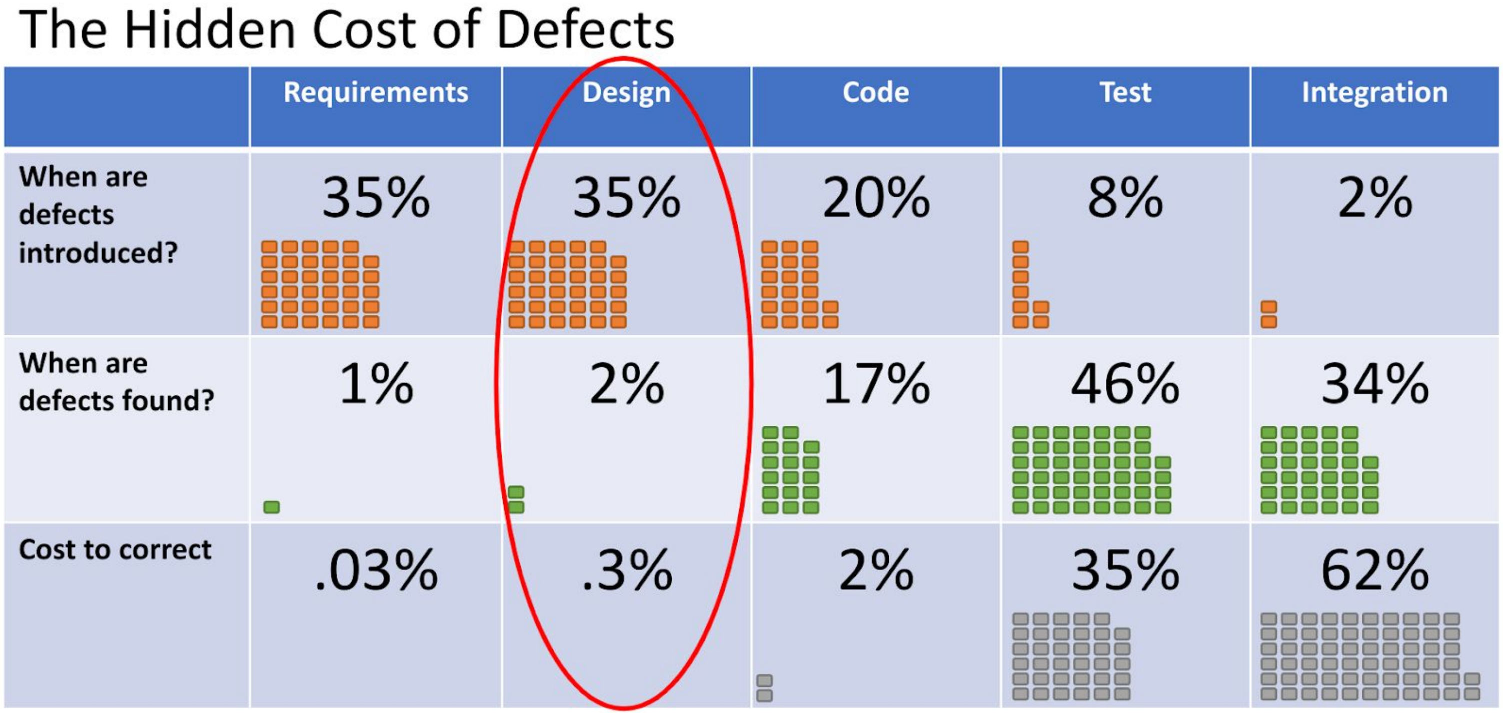
Problem: The system has a key design flaw.


Design Doc #1
Road Disruptions System
✨STPA✨
Design Doc #2
Road Disruptions System


Engineering Team
Update Processing
Processing Results
Update Diffing logic
Diffing Status
Snapshot Differ
Create / Delete Road Closure
Snapshots
Road Closures on Google Maps
Alerts
Snapshot
Road Disruption Processor
Create / Delete Road Closure
Road Closures on Google Maps
Google Maps

Google


Engineering Team
Update Processing
Processing Results
Update Diffing logic
Diffing Status
Snapshot Differ
Create / Delete Road Closure
Snapshots
Alerts
Snapshot
Road Disruption Processor
Create / Delete Road Closure
Road Closures on Google Maps
Google Maps



The Hidden Cost of Defects

	Requirements	Design	Code	Test	Integration
When are defects introduced?	35%	35%	20%	8%	2%
When are defects found?	1%	2%	17%	46%	34%
Cost to correct	.03%	.3%	2%	35%	62%

John Thomas, 2021, System Safety and STPA Class Materials

Data from “ROI Analysis of the System Architecture Virtual Integration Initiative”, SEI, 2018

Key Takeaways

1. Software Systems are deeply complex.
2. SREs do not have the tools to interrogate the safety of complex systems.
3. When we apply STPA before we implement our systems, we have the opportunity to fix our problems at a fraction of the cost.

Further Reading

- Google Resources:
  - https://sre.google/resources/practices-and-processes/stpa/

- MIT Resources:
  - https://stamp-institute.com
  - https://psas.scripts.mit.edu/home/mit-stamp-workshop-tutorials/
  - https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf