Google

Mapping a Better Future with STPA

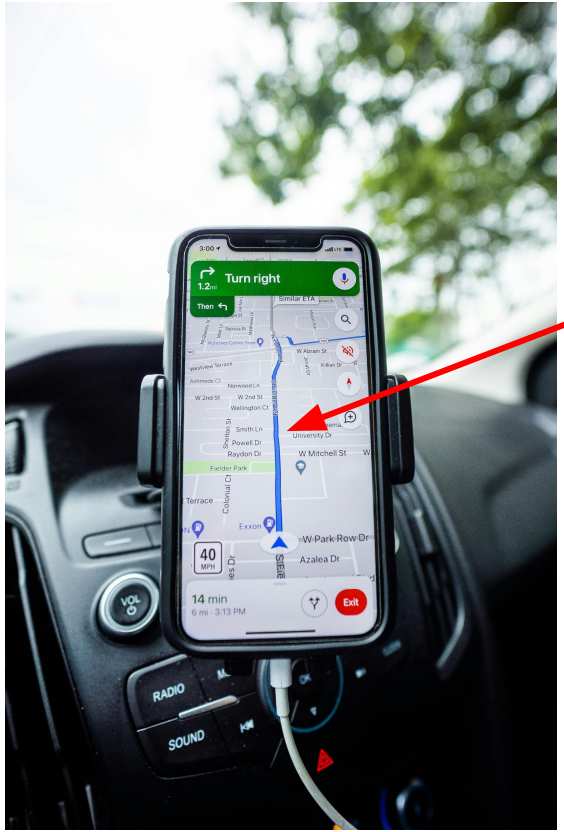
Geo Data SRE

Theo Klein (pikle@google.com)

MIT STAMP, March 26 2025

Google





Should be marked as closed, but isn't

Google

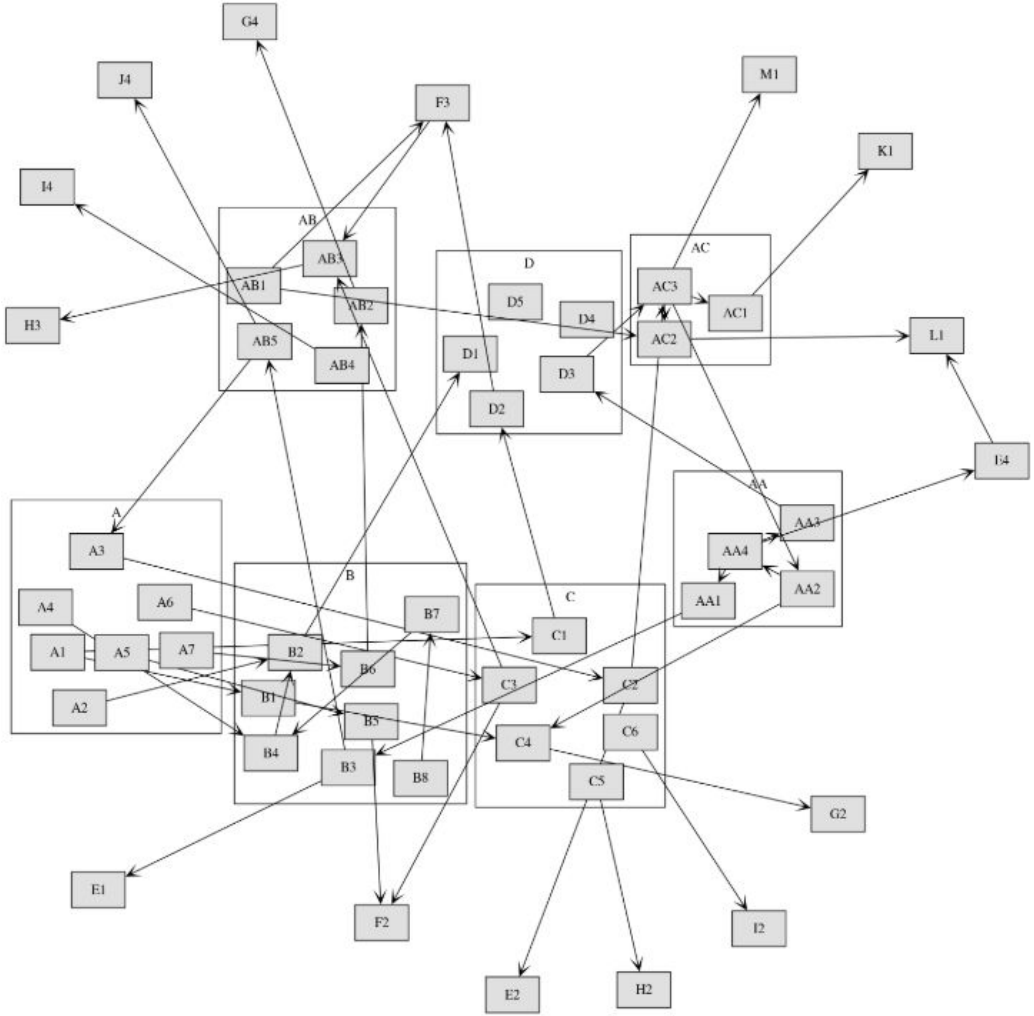
- Losses caused by component failures
  - Reliability problem

Traditional Focus

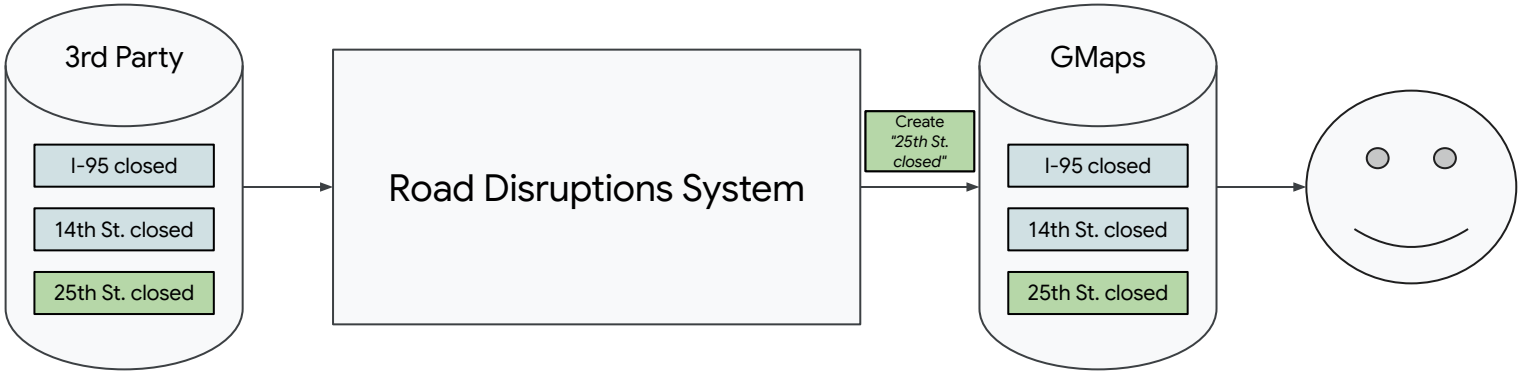
- Losses caused by component interactions
  - Often occur without component failures
  - Can be much more difficult to anticipate

Focus of new methods

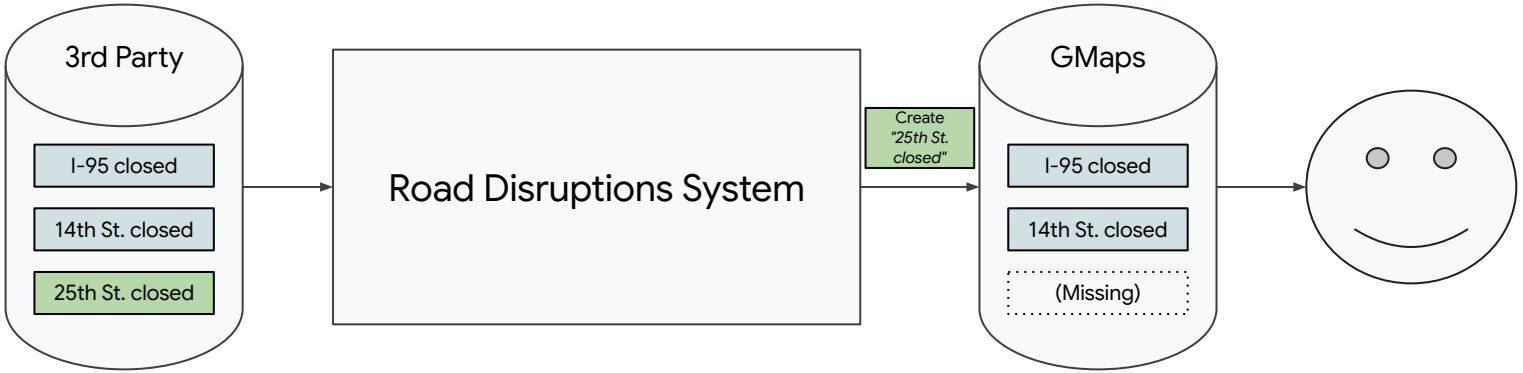
Google


G4
J4
F3
M1
K1
I4
AB
AB3
AB1
AB2
H3
AB5
AB4
D
D5
D4
D1
D3
D2
AC
AC3
AC1
AC2
L1
I4
AA
AA3
AA4
AA2
AA1
A
A3
A4
A6
A1
A5
A7
A2
B
B7
B2
B6
B1
B5
B4
B3
B8
C
C1
C3
C2
C6
C4
C5
G2
E1
F2
I2
E2
H2

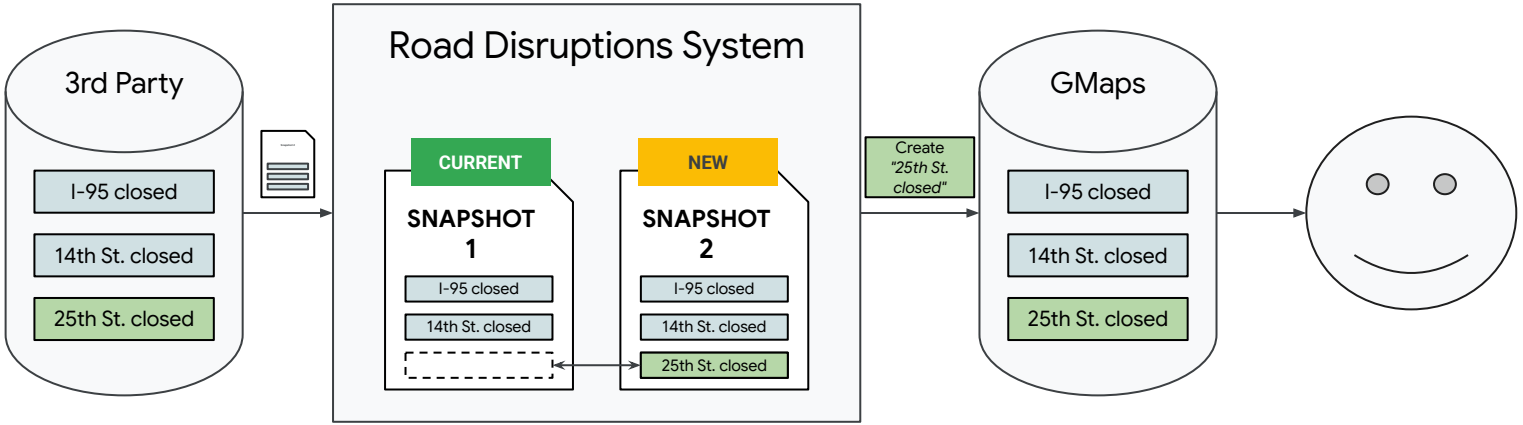
Google


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
25th St. closed

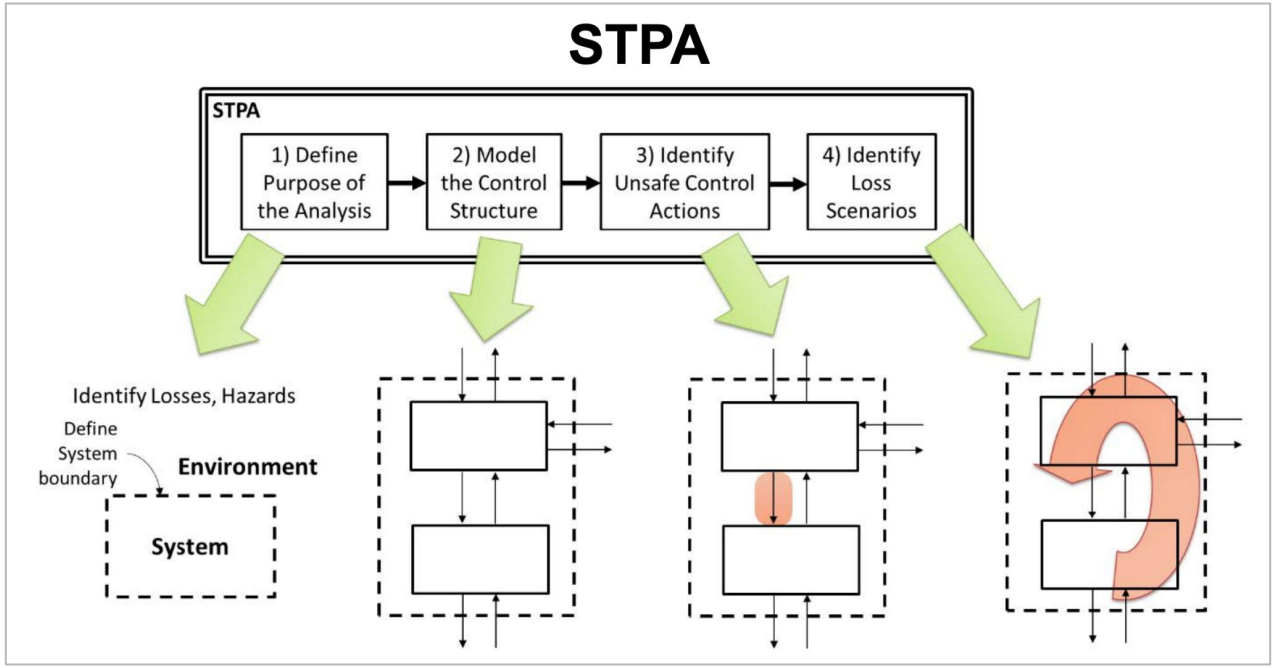
Google


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)

Google


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

Google


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

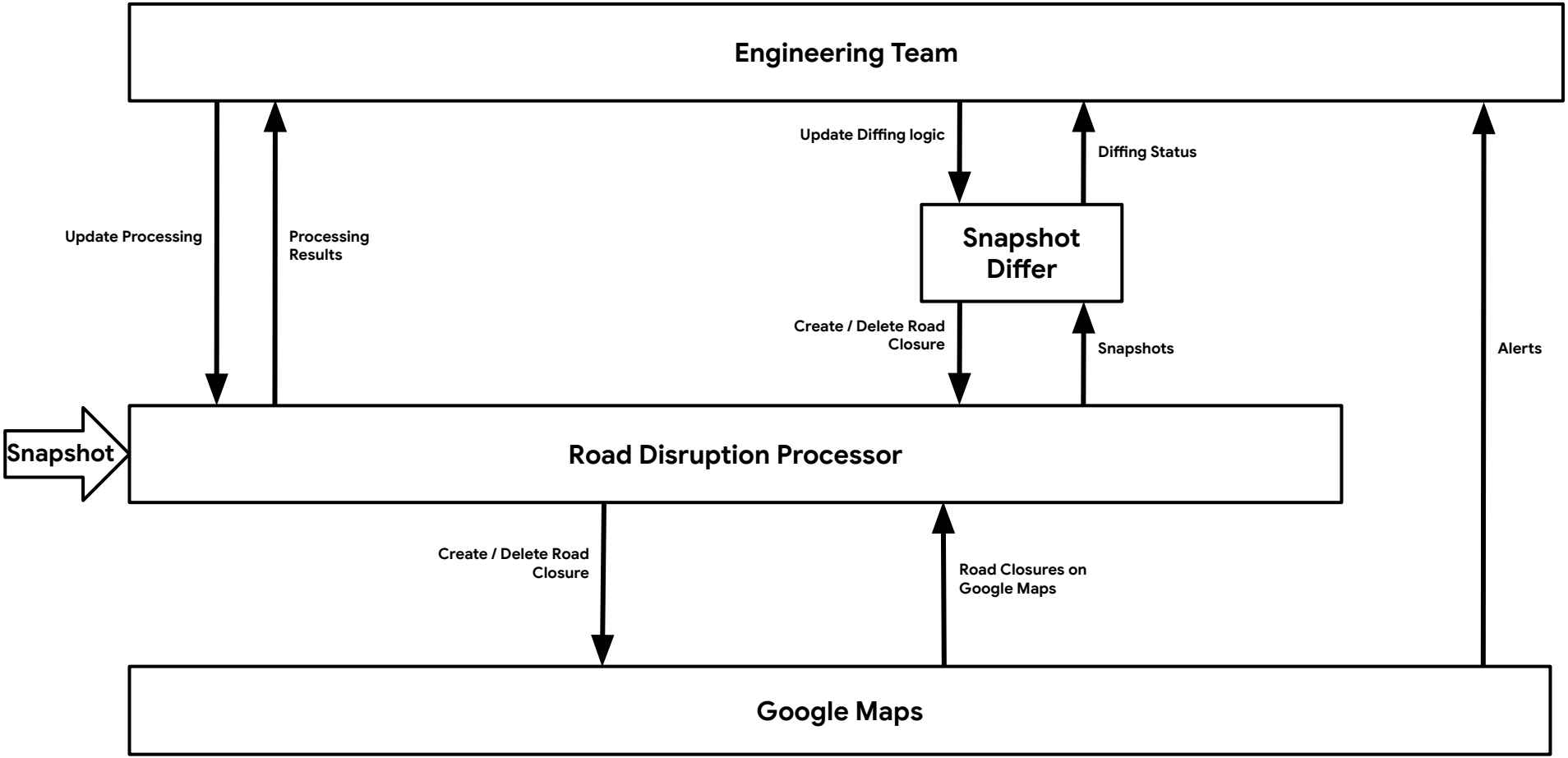
Google

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]

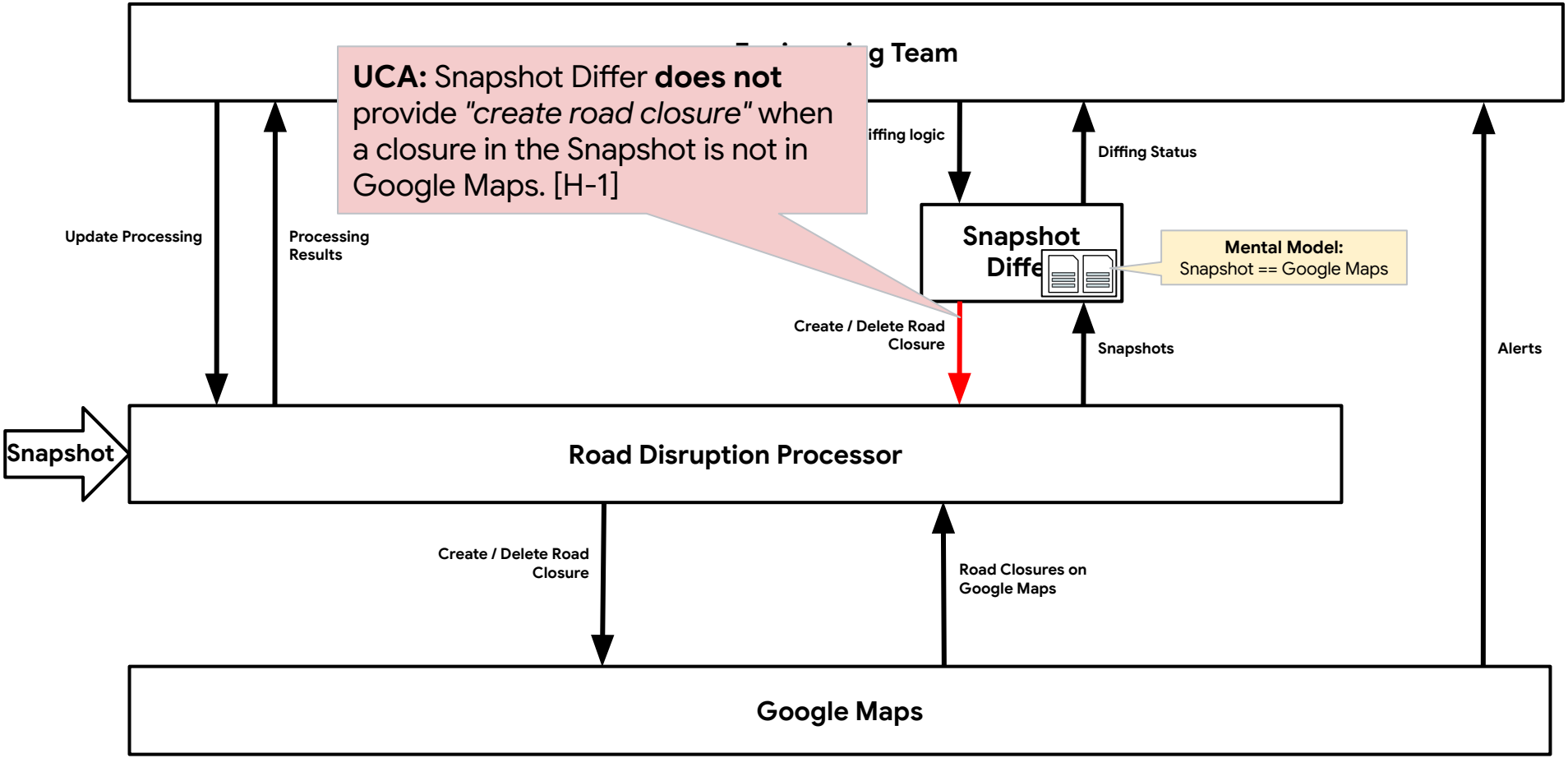
Google

Step 2: Control Structure



Google

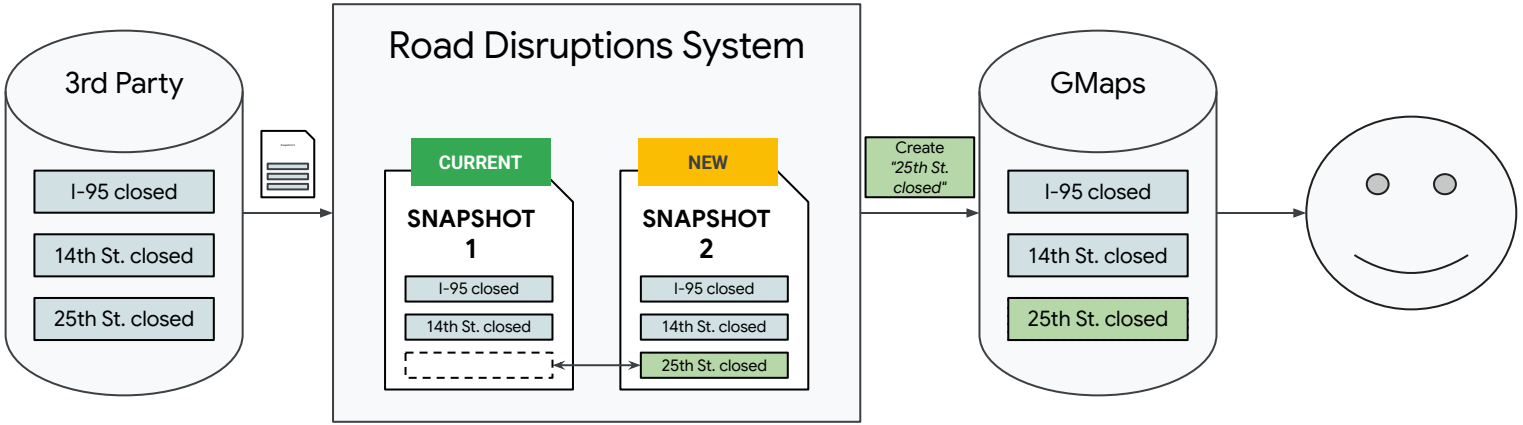
Step 3: Identify UCAs



Google

Step 4: Loss Scenario

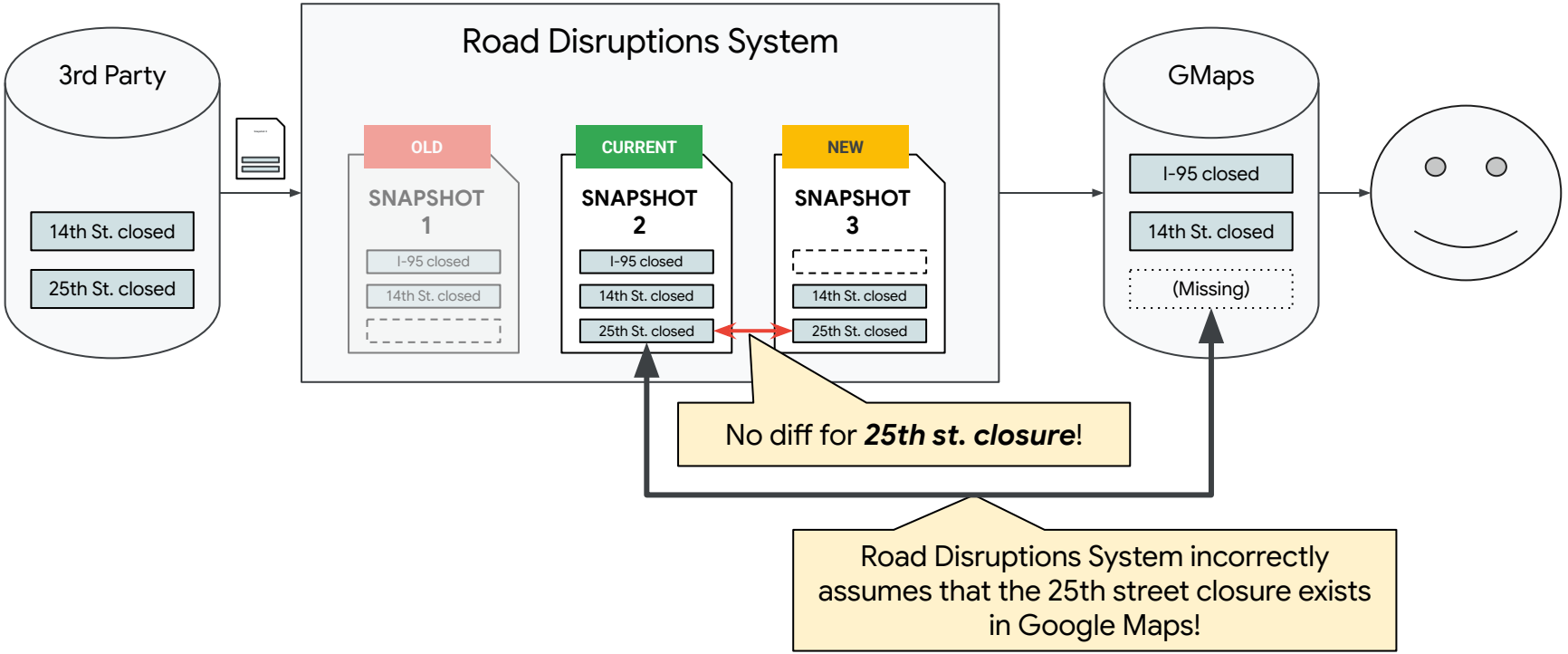
UCA: *Snapshot Differ* ***does not*** *provide "create road closure" when a closure in the Snapshot is not in Google Maps.*



Google

Step 4: Loss Scenario

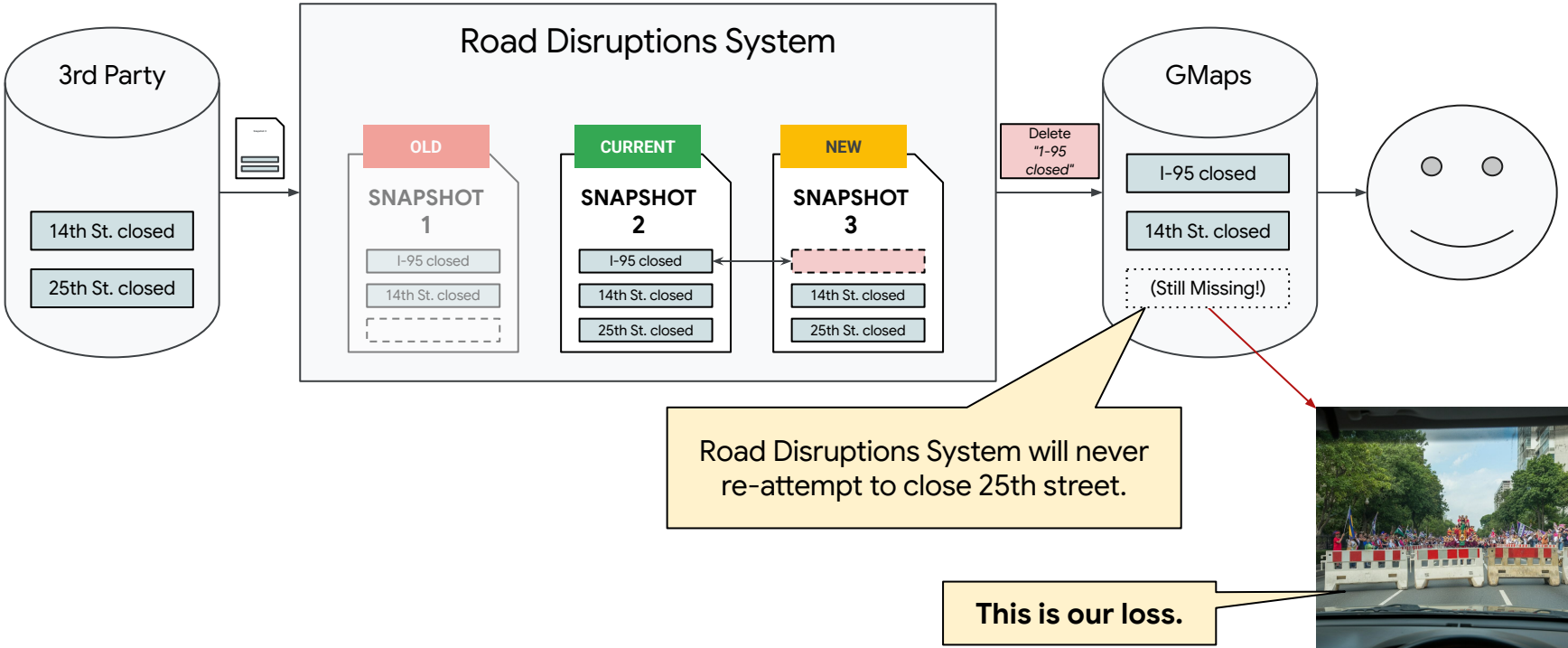
UCA: *Snapshot Differ* ***does not*** *provide "create road closure" when a closure in the Snapshot is not in Google Maps.*



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.*



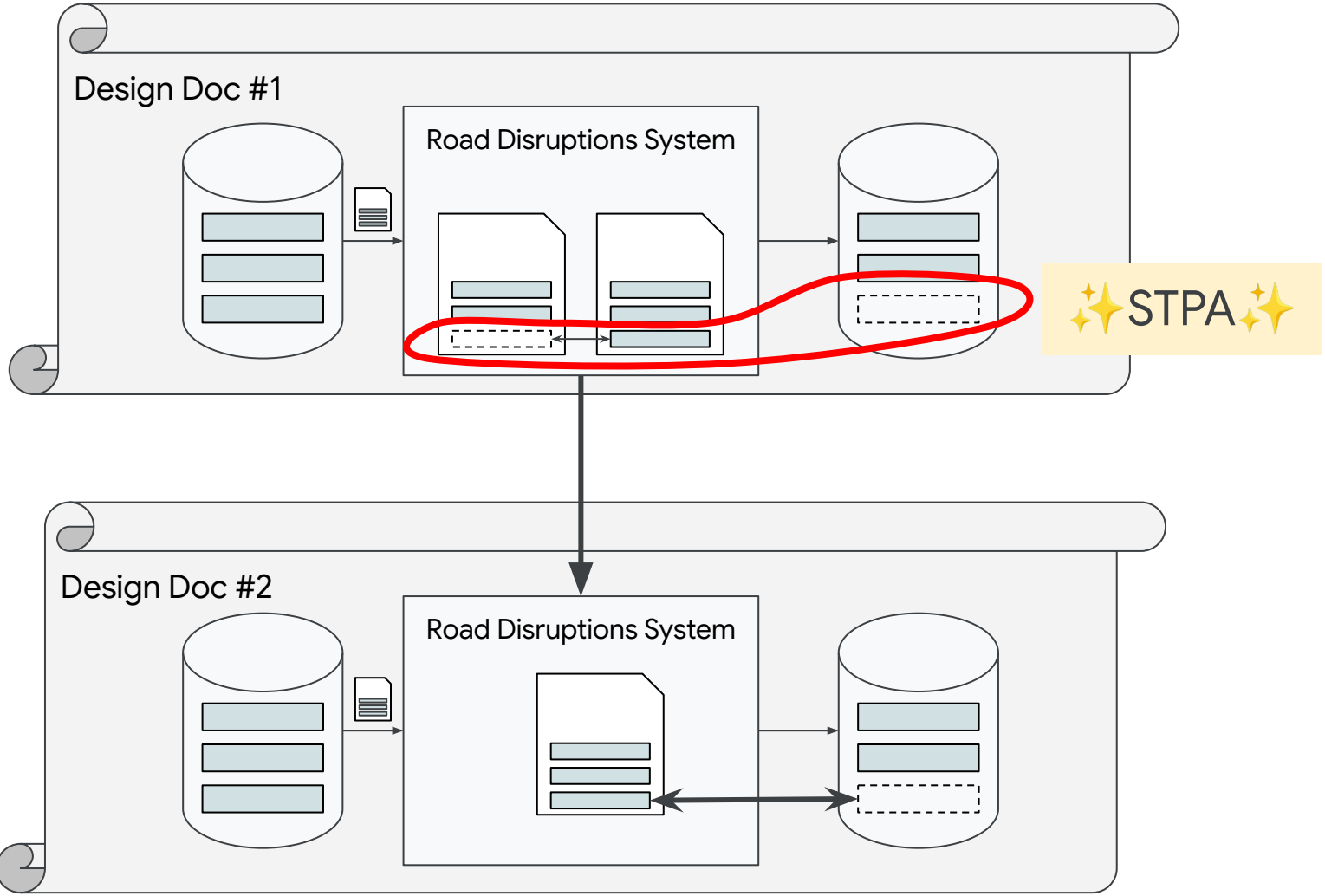
Google

No component failed.

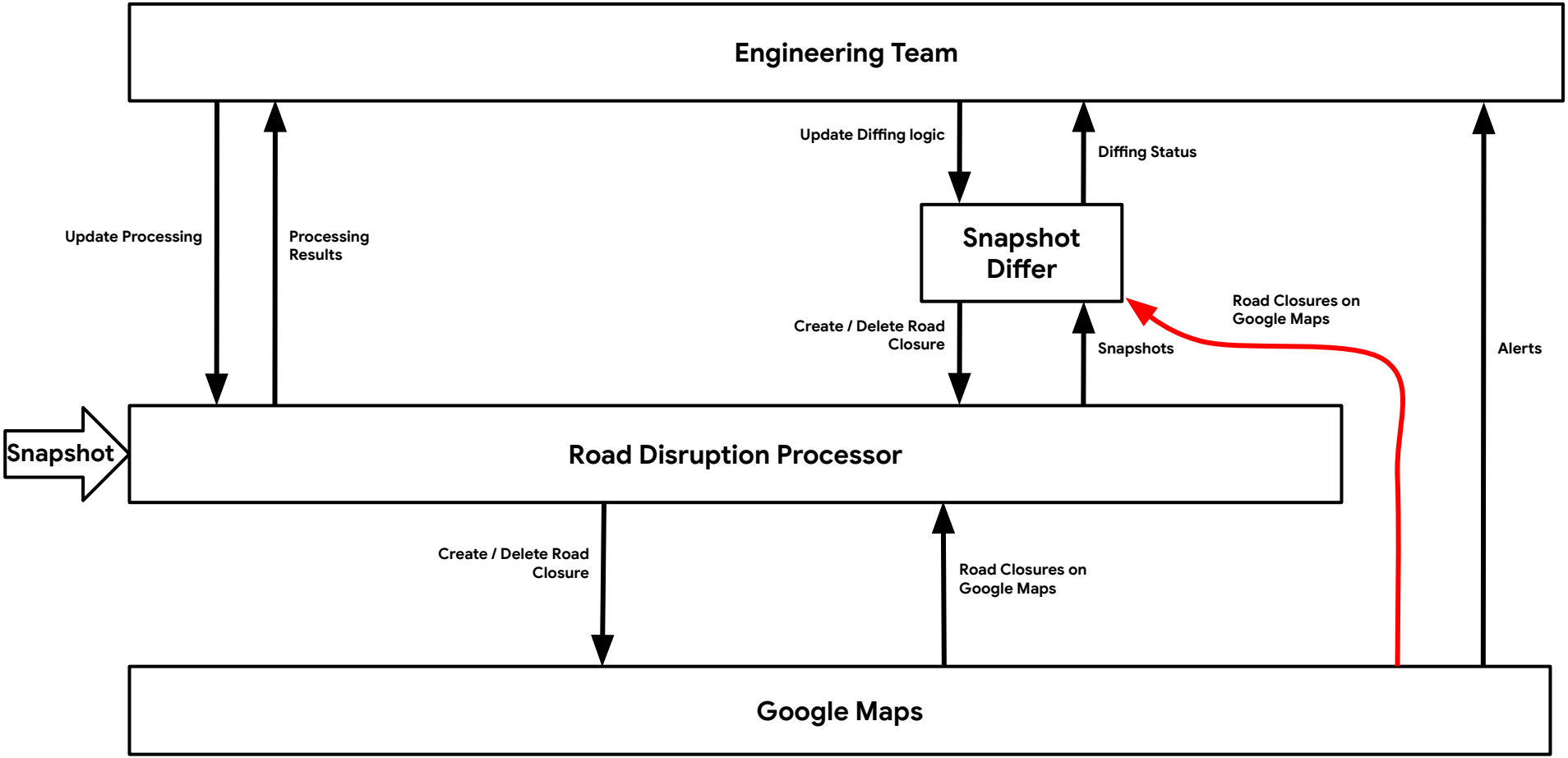
Every component operated as designed.

Problem: The system has a key design flaw.

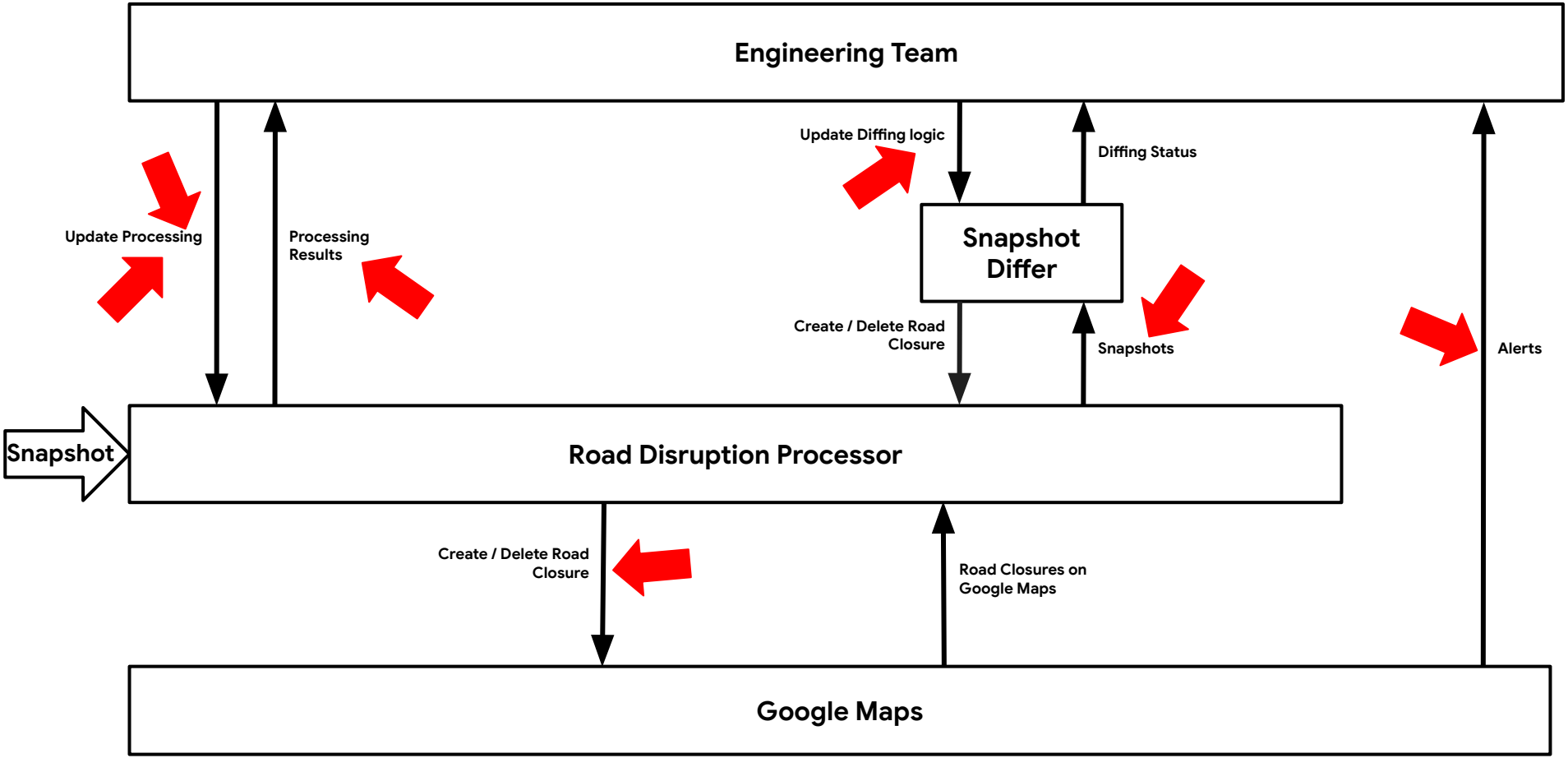
Google


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

Google


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

Google

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

Google

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.