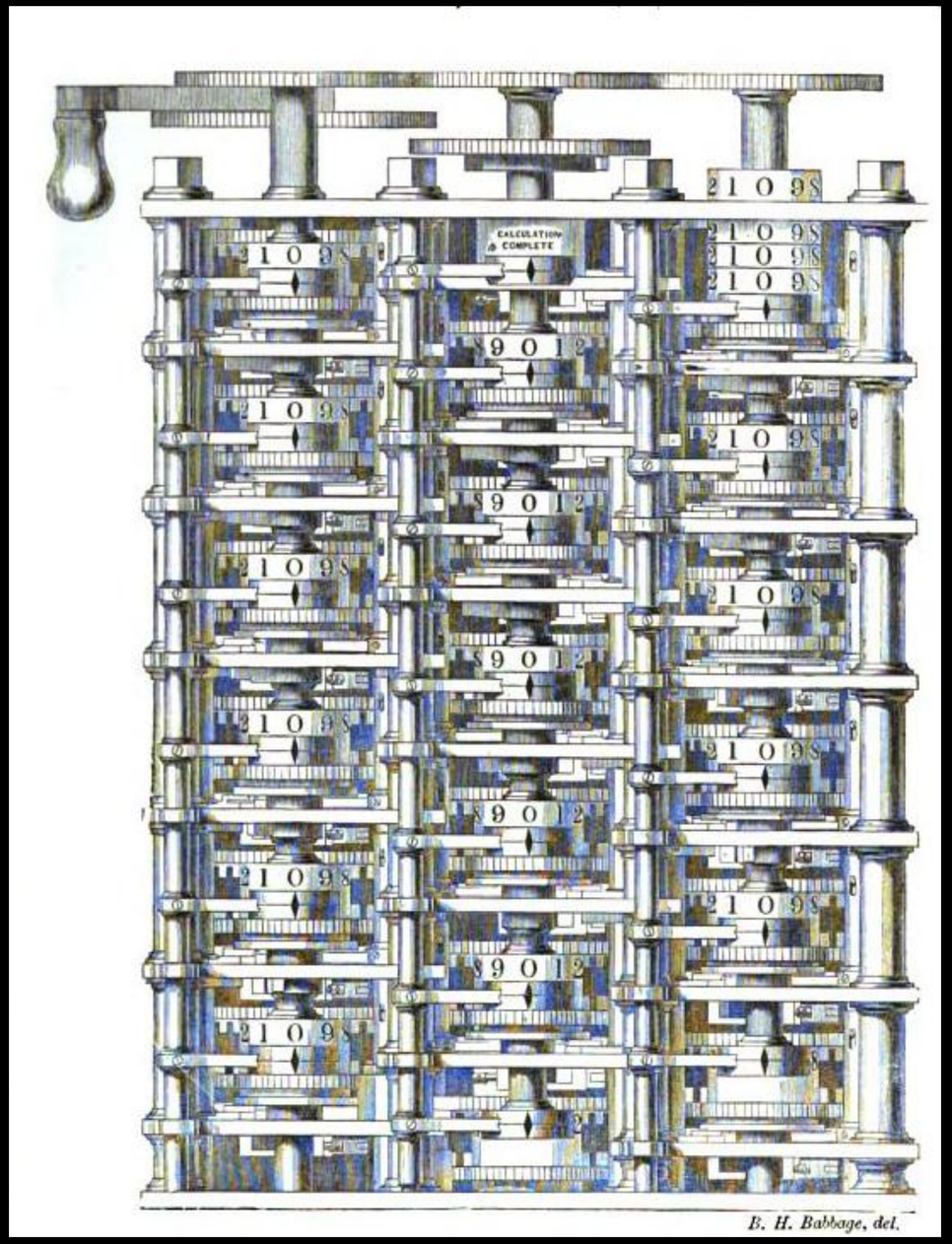
Freezing The Firehose

Forensic Engineering In The Age Of OpenTelemetry

Cail Young (he/him) - SRECon EMEA 2026 - @cail.bsky.social - https://linkedin.com/in/cailyoung

Babbage


CALCULATION
IS COMPLETE
B. H. Babbage, del.

In studying the evidence given upon the inquiries into the various lamentable accidents which have occurred upon railways, I have been much struck by the discordance of that evidence as to the speed with which the engines were travelling when they took place.

Even the best and most unbiassed judgment ought not to be trusted when mechanical evidence can be produced. The first rule I propose is, that —

Every engine should have mechanical self-registering means of recording its own velocity at every instant during the whole course of its journey

Charles Babbage, Passages from the life of a philosopher, 1864

The company put a disused second-class coach at [Babbage's] disposal and he converted it into what must have been the first example of a dynamometer car.

The car could be placed between an engine and a train, and it would record on a continuously moving roll of paper the tractive force of the engine. It would also record a plot showing the path of the centre of the carriage over the surface of the earth and the vertical shake of the carriage at three different points.

The company provided Babbage with full facilities for these experiments, including a locomotive with driver and fireman.

Wilkes, M. V. (2002). Charles Babbage and his world. Notes and Records of the Royal Society of London, 56(3), 353–365. https://doi.org/10.1098/rsnr.2002.0188

“The Black Box”



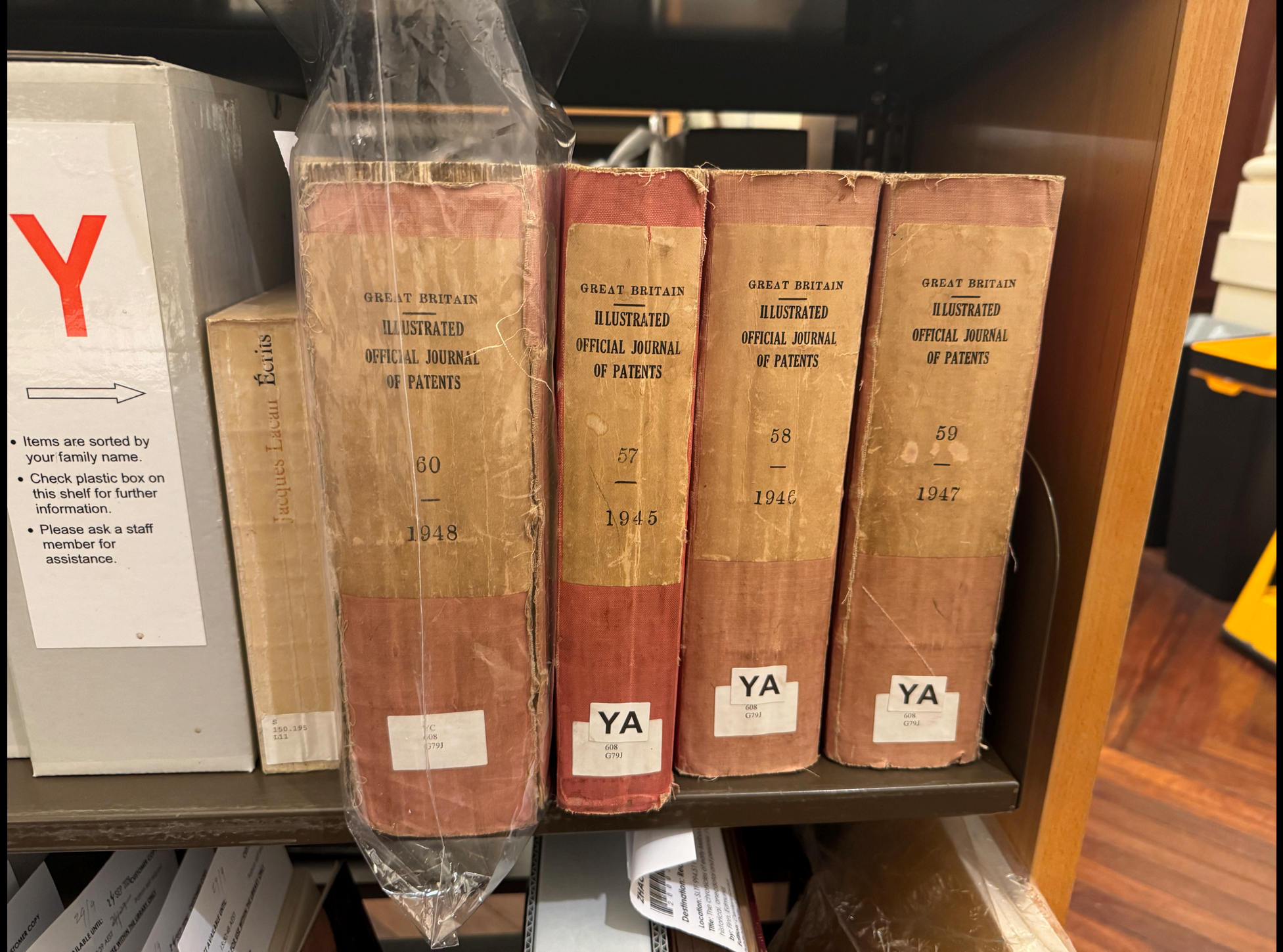
1939, Hussenot and Beaudouin, France

Image © User:Tiraden / Wikimedia Commons / CC-BY-SA-4.0

WW2 - Len Harrison & Vic Husband in the UK,
copper foil data recorder
first that survives where the crew cannot

[citation needed]

<photo permission not granted>


Y
• Items are sorted by your family name.
• Check plastic box on this shelf for further information.
• Please ask a staff member for assistance.
Jacques Lacan Écrits
GREAT BRITAIN
ILLUSTRATED
OFFICIAL JOURNAL
OF PATENTS
60
—
1948
GREAT BRITAIN
ILLUSTRATED
OFFICIAL JOURNAL
OF PATENTS
57
—
1945
YA
608
G79J
GREAT BRITAIN
ILLUSTRATED
OFFICIAL JOURNAL
OF PATENTS
58
—
1946
YA
608
G79J
GREAT BRITAIN
ILLUSTRATED
OFFICIAL JOURNAL
OF PATENTS
59
—
1947
YA
608
G79J



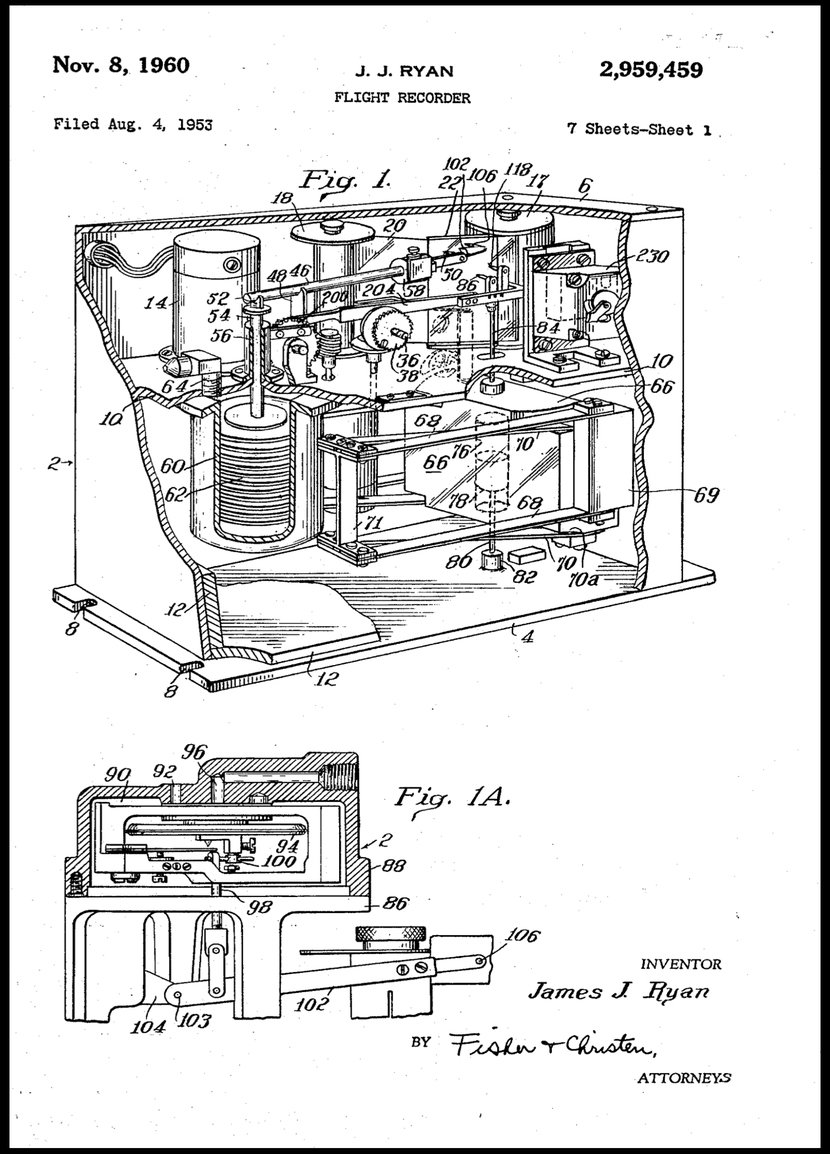
1942 - Veijo Hietala, Finland

Photo courtesy Museokeskus Vapriikki / CC-BY-2.0



Major Howard L. Nussbaum showing the magnetic wire recorder to Gen. Arnold, Commandant of the U. S. Army Air Forces.

1943 - USAAF pilots a cockpit voice recorder on magnetic wire



Nov. 8, 1960 J. J. RYAN 2,959,459

FLIGHT RECORDER

Filed Aug. 4, 1953 7 Sheets-Sheet 1

Fig. 1.

Fig. 1A.

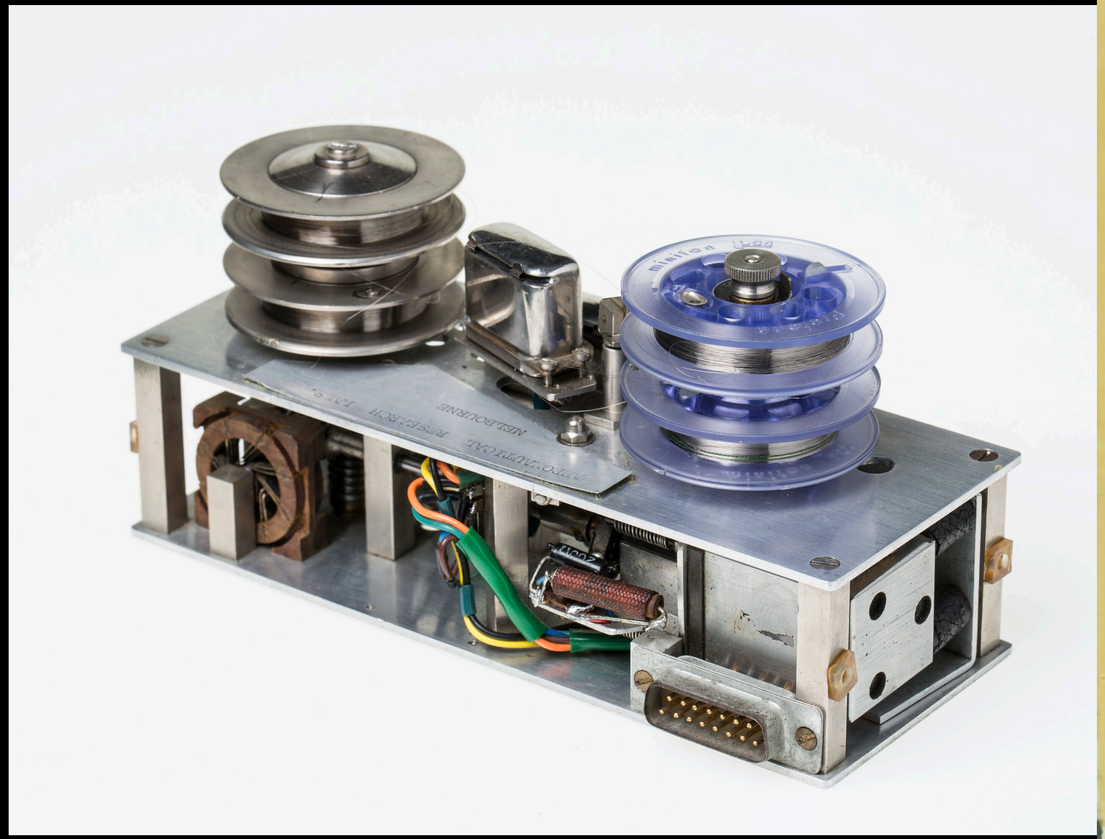
INVENTOR

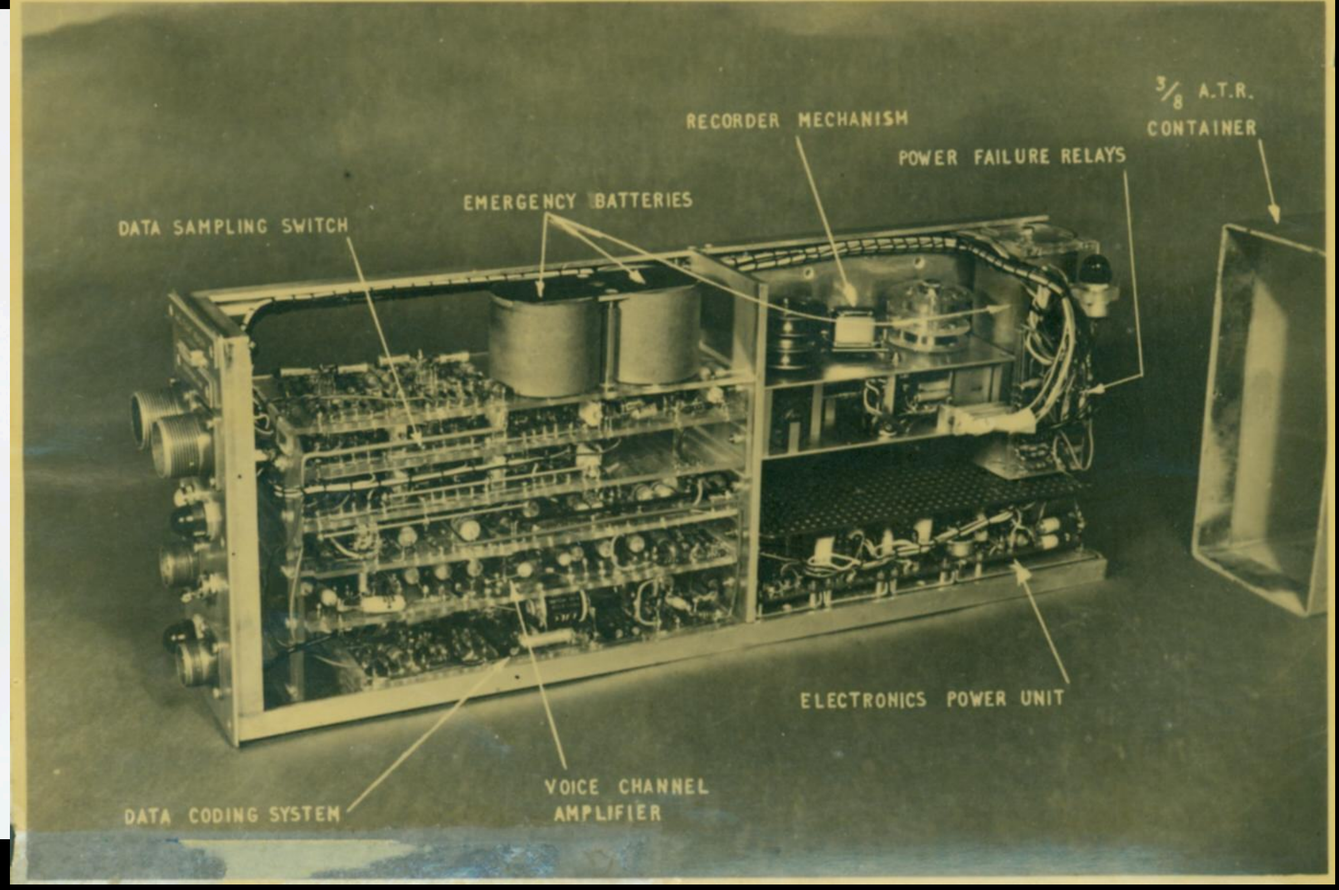
James J. Ryan

BY Fisher & Christen,

ATTORNEYS

1953-1960 - James Ryan gets a US patent for a flight recorder

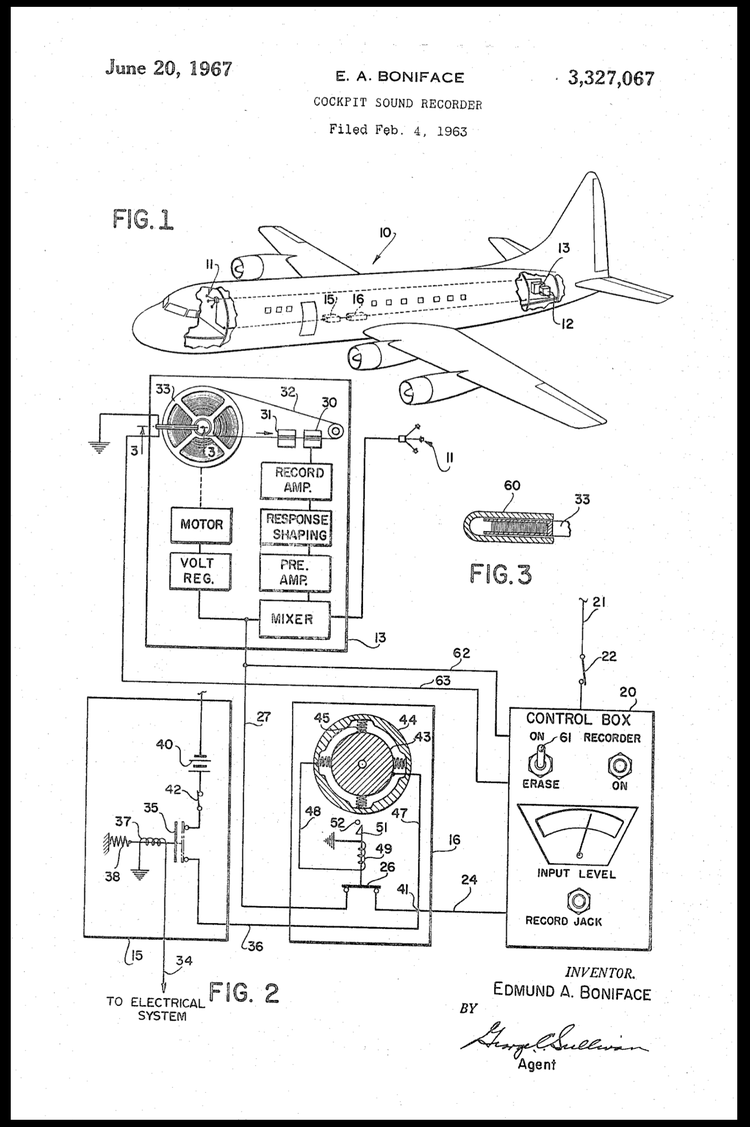




🇦🇺 1958 - David Warren at ARL in Australia 🇦🇺

Copyright Museums Victoria / CC BY
Photographer: John Broomfield
Museums Victoria

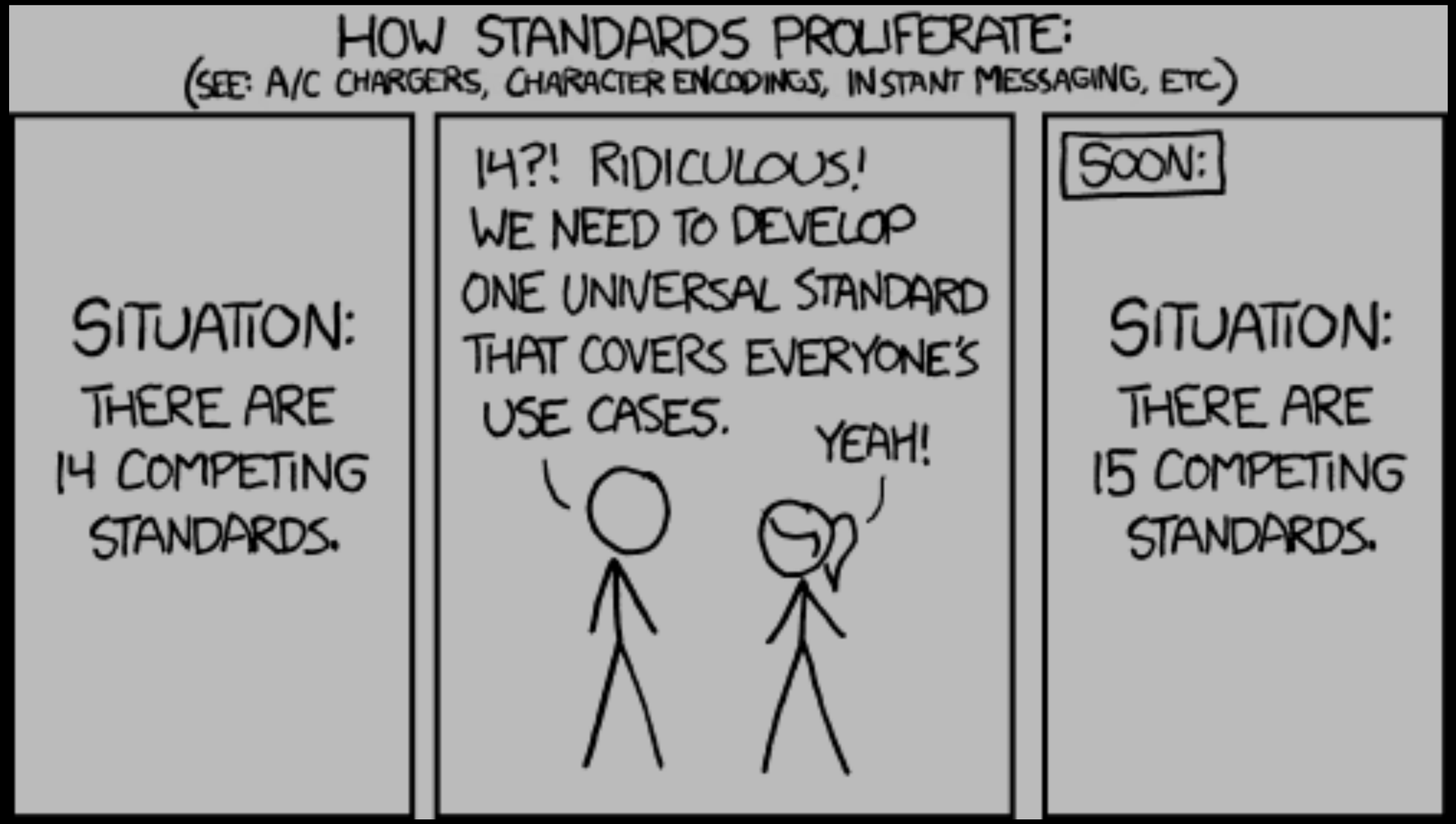
https://collections.museumsvictoria.com.au/items/393647
https://collections.museumsvictoria.com.au/items/405748



1961 - Edmund Boniface Jr at Lockheed

1960s - aviation regulators progressively make recorders mandatory around the world

Preventative v *Forensic*



https://xkcd.com/927

Courtesy Randall Munroe - CC-BY-NC-2.5 - https://creativecommons.org/licenses/by-nc/2.5/

We want to share!

Where To From Here

aka ‘the agenda’

- Telemetry Platform Design
- ‘Cold Replay’ Forensics Capability
- General Concerns About The Future
- If Time (And Patience) Permits, A Period Of Questions

2024: The year of spans on the desktop

Mission: Invent the Universe

Two main questions:
Where and What

I must not egress.
Egress is the budget-killer.

— Paul Atreides, SRE

Ingest charges

Decision:
Sample *in-region*,
then egress to a vendor

Initial customer:
Our own SaaS product



Q: Where?
A: 3x regions, Kubernetes in each

Side quest: Instrumentation

Tail sampling: *critical*

Q: What (that can tail sample)?

Multiple policies exist today and it is st ght forward to add more. Thes

- `always_sample` : Sample all trac
- `latency` : Sample based on th time, without taking into consi greater than `threshold_ms`
- `numeric_attribute` : Sam
- `probabilistic` : Sample
- `status_code` : Sample b
- `string_attribute` : Sampl supported
- `trace_state` : Sample based on TraceState valu
- `trace_flags` : Sample if the sampled trace flag was set on a
- `rate_limiting` : Sample based on the rate of spans per second.
- `bytes_limiting` : Sample based on the rate of bytes per second us golang.org/x/time/rate. This allows for burst traffic up to a configura bucket is refilled continuously at the specified rate and has a maxim
- `span_count` : Sample based on the minimum and/or maximum num the range threshold, the trace will not be sampled.
- `boolean_attribute` : Sample based on boolean attribute (resource
- `ottl_condition` : Sample based on given boolean OTTL condition
- multiple policies, creates an AND policy
- single policy, creates a

Each policy will result in a decision, and the processor

- When there's a "drop" decision, the trace is not s
- When there's an "inverted not sample" decision, t
- When there's a "sample" decision, the trace is sam
- When there's a "inverted sample" decision and no
- In all other cases, the trace is NOT sampled

```
  },
  {
    name: composite-policy-1,
    type: composite,
    composite:
      {
        max_total_spans_per_second: 1000,
        policy_order: [test-composite-policy-1, test-composite-policy-
        composite_sub_policy:
          [
            {
              name: test-composite-policy-1,
              type: numeric_attribute,
              numeric_attribute: {key: key1, min_value: 50}
            },
            {
              name: test-composite-policy-2,
              type: string_attribute,
              string_attribute: {key: key2, values: [value1, value2]}
            },
            {
              name: test-composite-policy-3,
              type: always_sample
            }
          ],
        rate_allocation:
          [
            {
              policy: test-composite-policy-1,
              percent: 50
            },
            {
              policy: test-composite-policy-2,
              percent: 25
            }
          ]
      }
  },
]
```

Enter: *Dynamic* sampling

“99.99% of Your Traces Are (Probably) Trash” - Paige Cruz

https://www.usenix.org/conference/srecon24americas/presentation/cruz

200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200
200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200
200 200 200 200 200 200 200 200 200 200 200 200 200 404 200 200
200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200
200 200 200 200 200 200 200 200 200 418 200 200 200 200 200 200
200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200
200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200
200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200
200 200 500 200 200 200 200 200 200 200 200 200 200 200 200 200 200
200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200

200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200
200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200
200 200 200 200 200 200 200 200 200 200 200 200 200 404 200 200
200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200
200 200 200 200 200 200 200 200 200 418 200 200 200 200 200 200
200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200
200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200
200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200
200 200 500 200 200 200 200 200 200 200 200 200 200 200 200 200 200
200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200 200



https://github.com/open-telemetry/opentelemetry-specification/issues/691

What about Refinery?

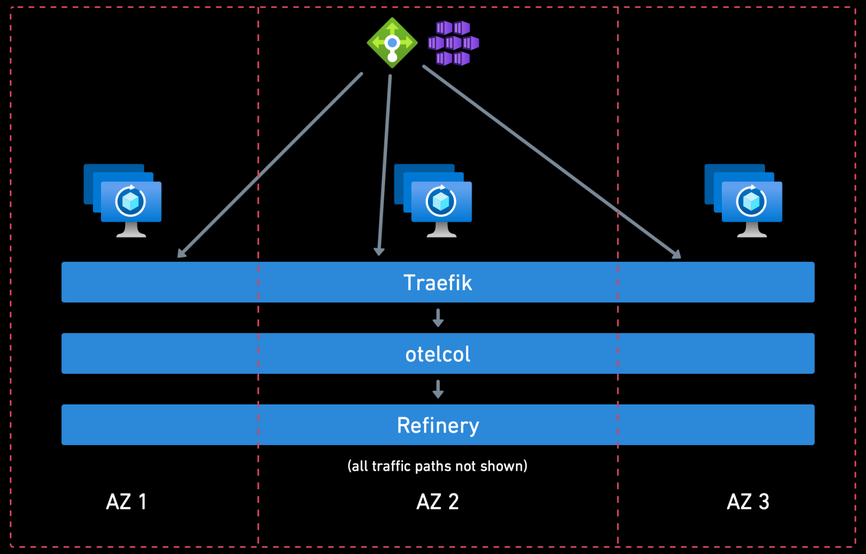
Q: Where? A: 3 Regions.

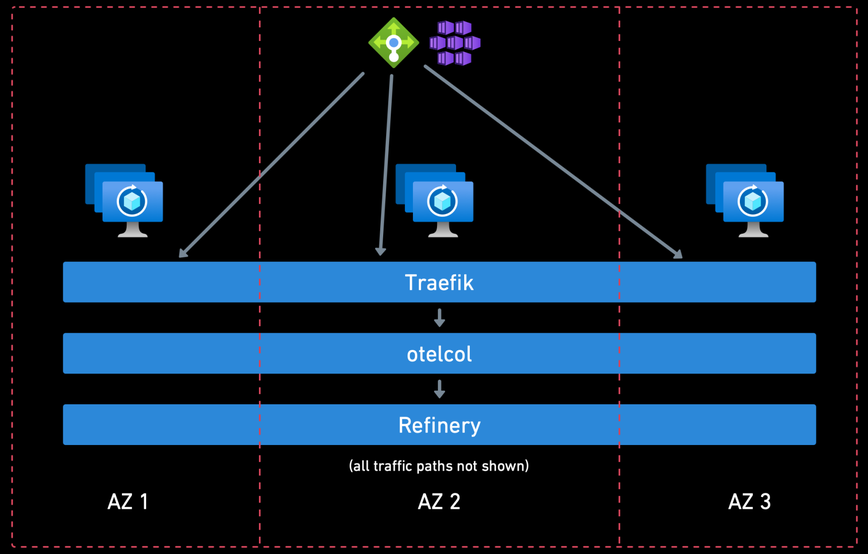
Q: What?: A: otelcol + refinery

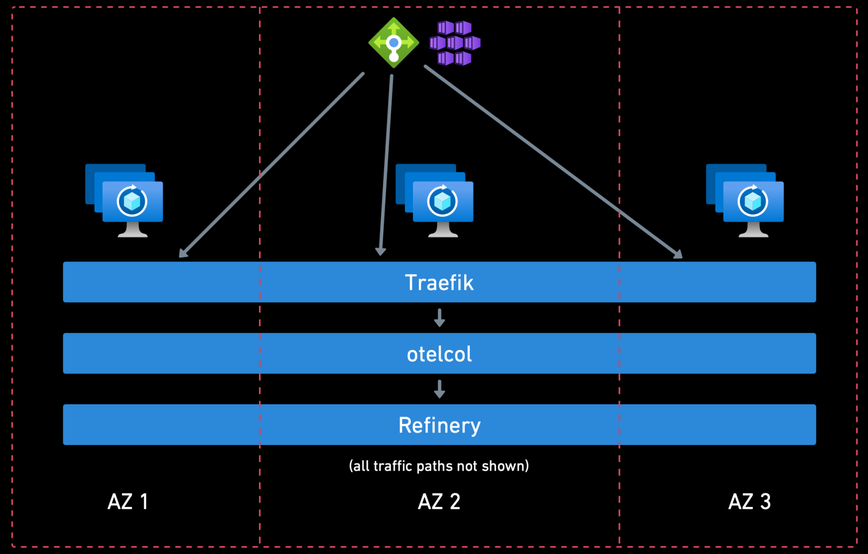
Q: Availability?

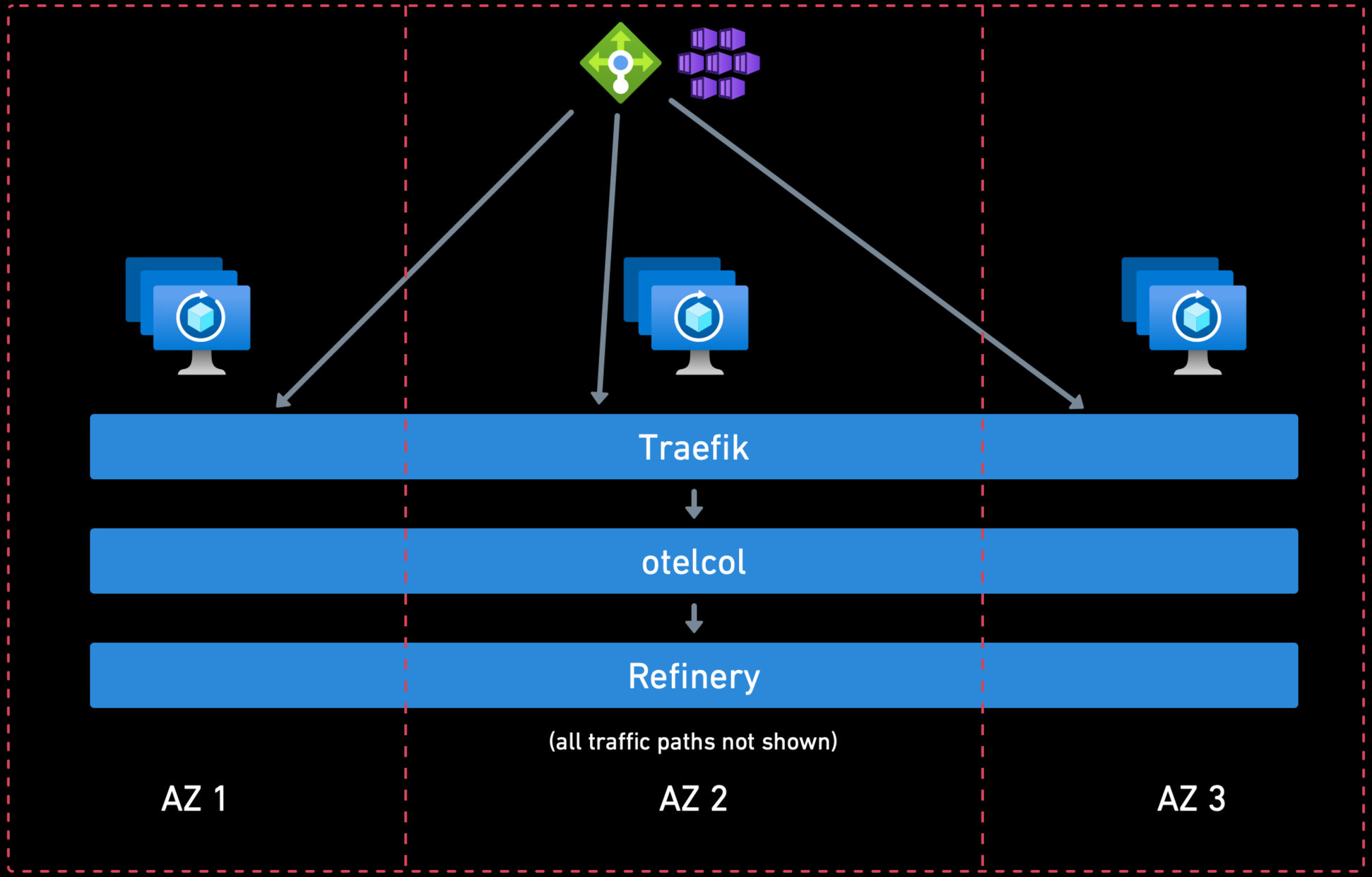
Replicable
Minimum 3
Zone-Balanced

traefik -> otelcol -> refinery


Traefik
otelcol
Refinery
(all traffic paths not shown)
AZ 1
AZ 2
AZ 3


Traefik
otelcol
Refinery
(all traffic paths not shown)
AZ 1
AZ 2
AZ 3


Traefik
otelcol
Refinery
(all traffic paths not shown)
AZ 1
AZ 2
AZ 3

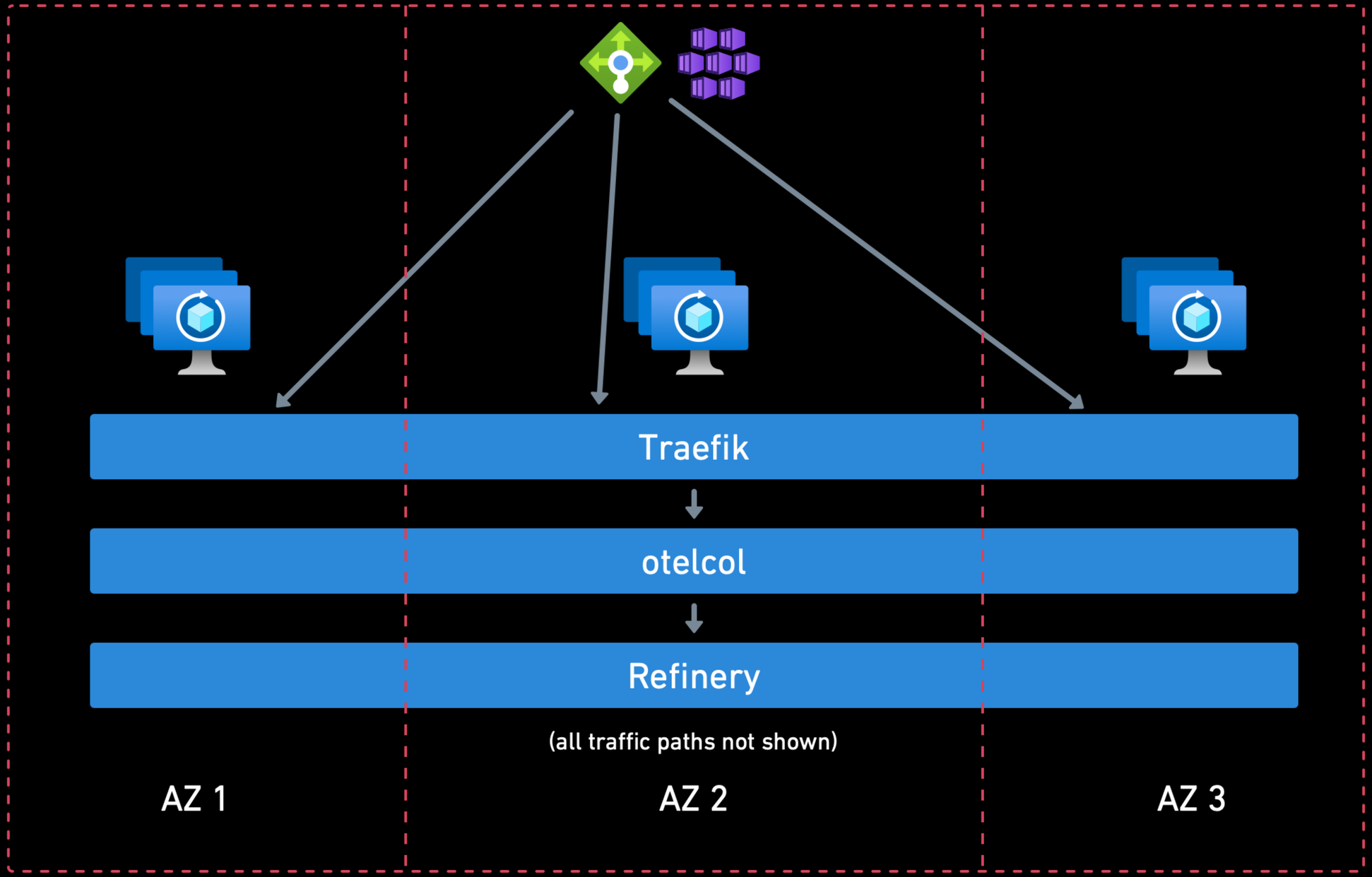

Traefik
otelcol
Refinery
(all traffic paths not shown)
AZ 1
AZ 2
AZ 3

```
    health_check
  pipelines:
    traces/preprocess:
      receivers:
          - otlp
      processors:
          - memory_limiter
          - resourcedetection
          - attributes/force-sample-from-header
          - transform/coerce-force-sample-to-bool
          - attributes/cloud-properties-for-frontend-spans
          - filter/not_staging_instance
      exporters:
          - routing
```

```yaml
connectors:
  routing:
    default_pipelines: [traces/sample_in_refinery]
    table:
      - context: span
        condition: attributes["force_sample"] == true
        pipelines: [traces/always_sample]
      - context: span
        condition: instrumentation_scope.name == "Octopus.ProcessExecution"
        pipelines: [traces/always_sample]
      - context: span
        condition: instrumentation_scope.name == "@honeycombio/instrumentation-web-vitals"
        pipelines: [traces/always_sample]
      - context: span
        condition: instrumentation_scope.name == "@opentelemetry/instrumentation-document-load"
        pipelines: [traces/always_sample]
```

```
# This pipeline is for spans that we always want to send thro
traces/always_sample:
  receivers:
    - routing
  processors:
    - memory_limiter
    - batch
  exporters:
    - otlphttp/honeycomb
```

```
traces/sample_in_refinery:
  receivers:
    - routing
  processors:
    - memory_limiter
    - filter/not_staging_instance
    - attributes/cloud-properties-for-frontend-spans
    - batch
  exporters:
    - otlphttp/localrefinery
```


Traefik
otelcol
Refinery
(all traffic paths not shown)
AZ 1
AZ 2
AZ 3

Getting It Right “At Scale”

Iterate &
Iterate &
Iterate &
Iterate &
Iterate &
Iterate &
Iterate &
Iterate &
Iterate &
Iterate &
Iterate &
Iterate &
Iterate &

v1.0 Done!

SLI: Minimum Throughput

`libhoney_upstream_messages_sent`

SLI: Data Loss

```
otelcol_exporter_send_failed_spans_total
otelcol_exporter_enqueue_failed_spans_total
otelcol_receiver_refused_spans_total
```

```
libhoney_upstream_send_errors
libhoney_peer_send_errors
incoming_router_dropped
peer_router_dropped
```

90.02%

Current SLI

95.0%

Target

0.0% (-8h21m)

Error Budget Remaining

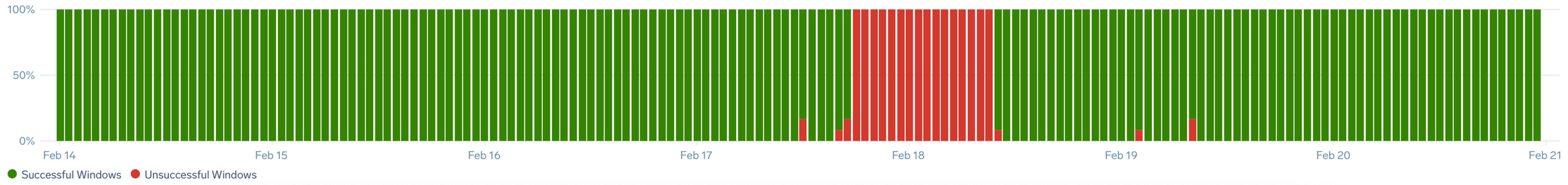
7d Rolling (14/2 to 20/2)

Compliance

Error Budget Burndown



Event History



Second customer:
Integration Tests

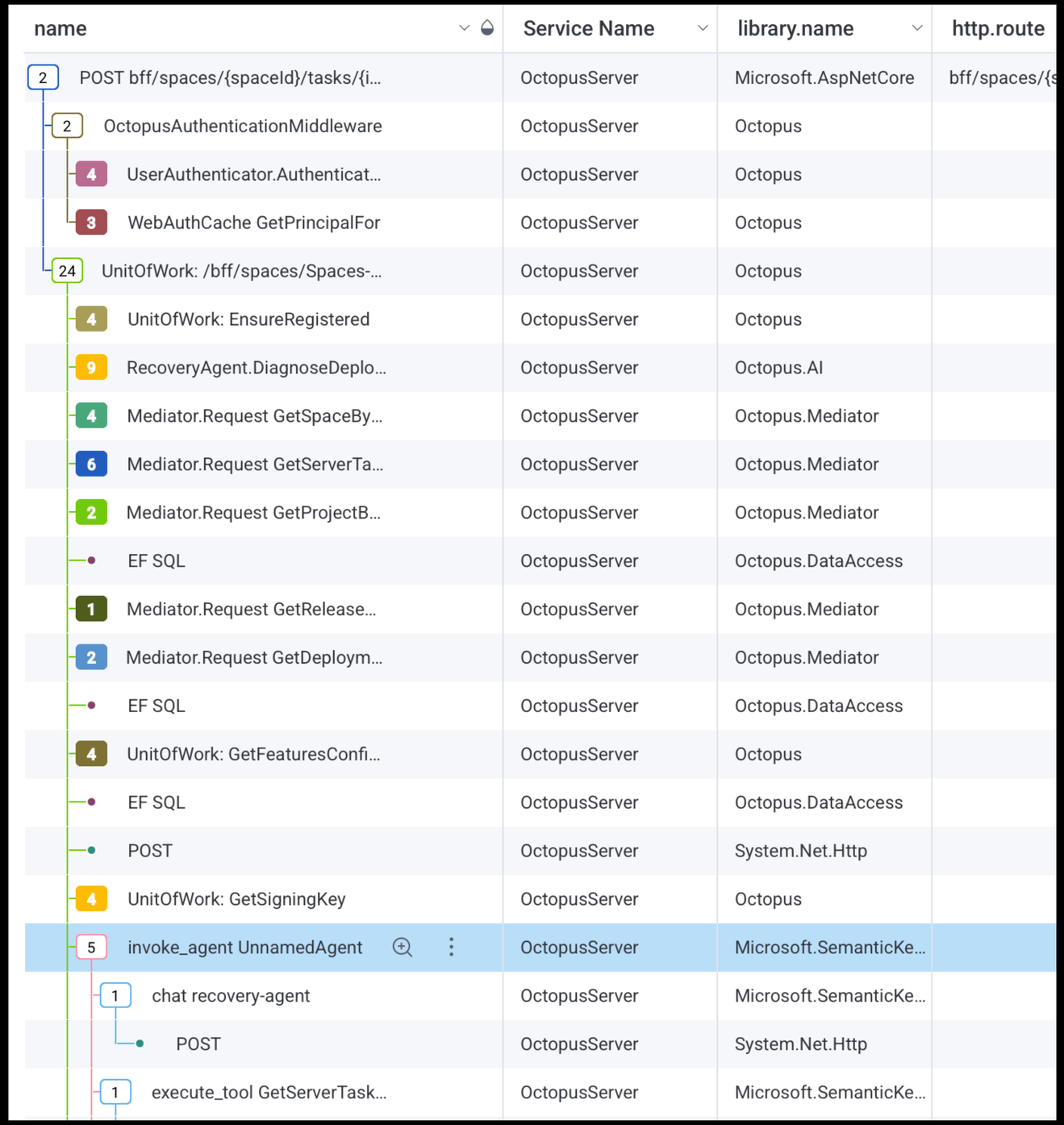
Path-based routing

```
  - path: /
    pathType: Prefix
    backend:
      service:
        name: server-cloud-loadbalancer-collector
        port:
          name: otlp-http

  - path: /services/servertests/ # make sure we configure
    pathType: Prefix
    backend:
      service:
        name: tests-collector-collector
        port:
          name: otlp-http
```

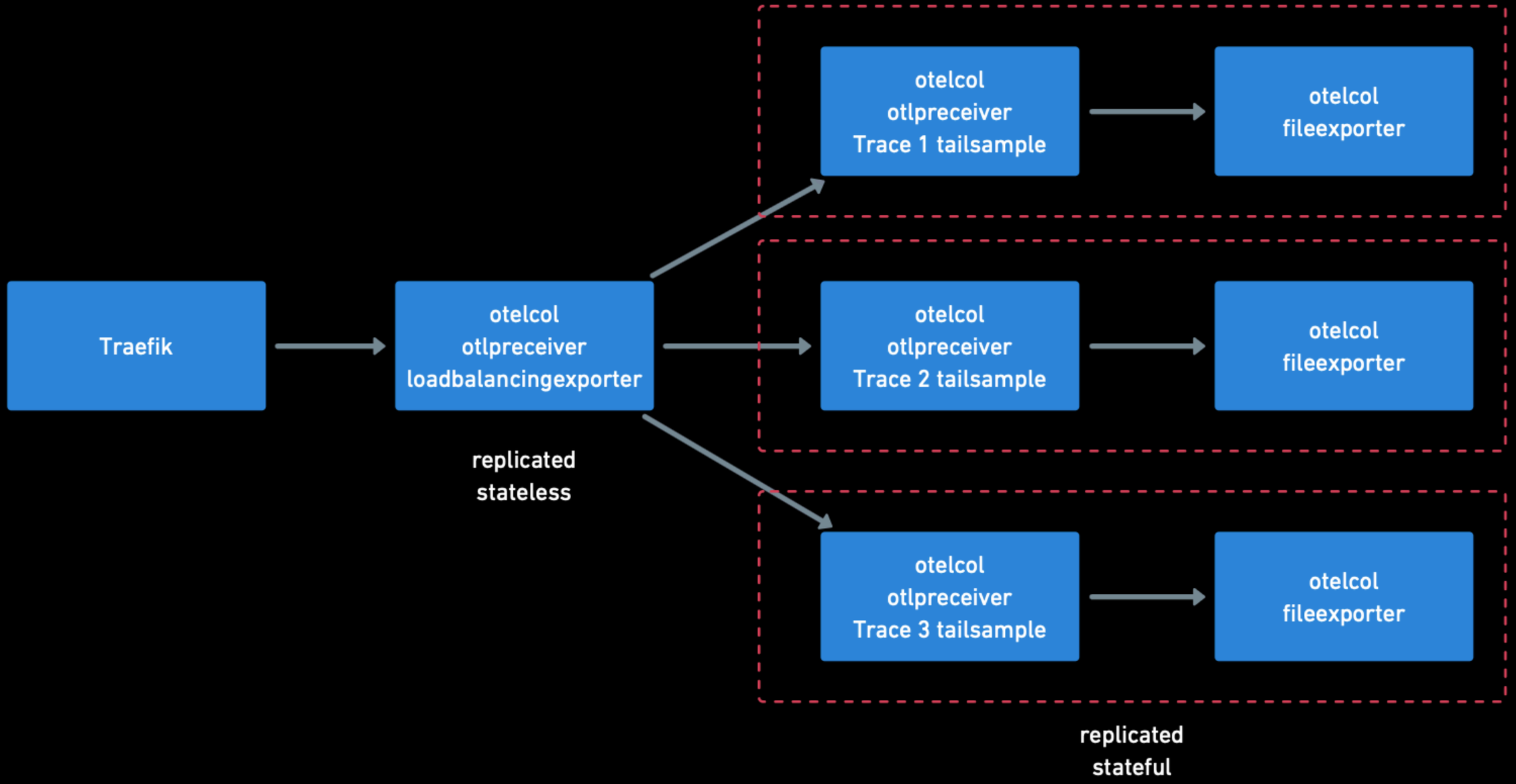
```
config:
  receivers:
    otlp:
      protocols:
        http:
          traces_url_path: /services/servertests/v1/traces
          endpoint: 0.0.0.0:4318
          include_metadata: true
          auth:
            authenticator: bearertokenauth
```

Third customer: AI Evals



name	Service Name	library.name	http.route
2 POST bff/spaces/{spaceId}/tasks/{i...	OctopusServer	Microsoft.AspNetCore	bff/spaces/{s
2 OctopusAuthenticationMiddleware	OctopusServer	Octopus	
4 UserAuthenticator.Authenticat...	OctopusServer	Octopus	
3 WebAuthCache GetPrincipalFor	OctopusServer	Octopus	
24 UnitOfWork: /bff/spaces/Spaces-...	OctopusServer	Octopus	
4 UnitOfWork: EnsureRegistered	OctopusServer	Octopus	
9 RecoveryAgent.DiagnoseDeplo...	OctopusServer	Octopus.AI	
4 Mediator.Request GetSpaceBy...	OctopusServer	Octopus.Mediator	
6 Mediator.Request GetServerTa...	OctopusServer	Octopus.Mediator	
2 Mediator.Request GetProjectB...	OctopusServer	Octopus.Mediator	
EF SQL	OctopusServer	Octopus.DataAccess	
1 Mediator.Request GetRelease...	OctopusServer	Octopus.Mediator	
2 Mediator.Request GetDeploym...	OctopusServer	Octopus.Mediator	
EF SQL	OctopusServer	Octopus.DataAccess	
4 UnitOfWork: GetFeaturesConfi...	OctopusServer	Octopus	
EF SQL	OctopusServer	Octopus.DataAccess	
POST	OctopusServer	System.Net.Http	
4 UnitOfWork: GetSigningKey	OctopusServer	Octopus	
5 invoke_agent UnnamedAgent	OctopusServer	Microsoft.SemanticKe...	
1 chat recovery-agent	OctopusServer	Microsoft.SemanticKe...	
POST	OctopusServer	System.Net.Http	
1 execute_tool GetServerTask...	OctopusServer	Microsoft.SemanticKe...	

Somehow, `tailsamplingprocessor` returned


Traefik
otelcol
otlpreceiver
loadbalancingexporter
replicated
stateless
otelcol
otlpreceiver
Trace 1 tailsample
otelcol
fileexporter
otelcol
otlpreceiver
Trace 2 tailsample
otelcol
fileexporter
otelcol
otlpreceiver
Trace 3 tailsample
otelcol
fileexporter
replicated
stateful

So much CrashLoopBackoff

Fourth Customer: Forensics

More Iteration More Furious

Iterate &
Iterate &
Iterate &
Iterate &
Iterate &
Iterate &
Iterate &
Iterate &
Iterate &
Iterate &
Iterate &

More Iteration More Furious

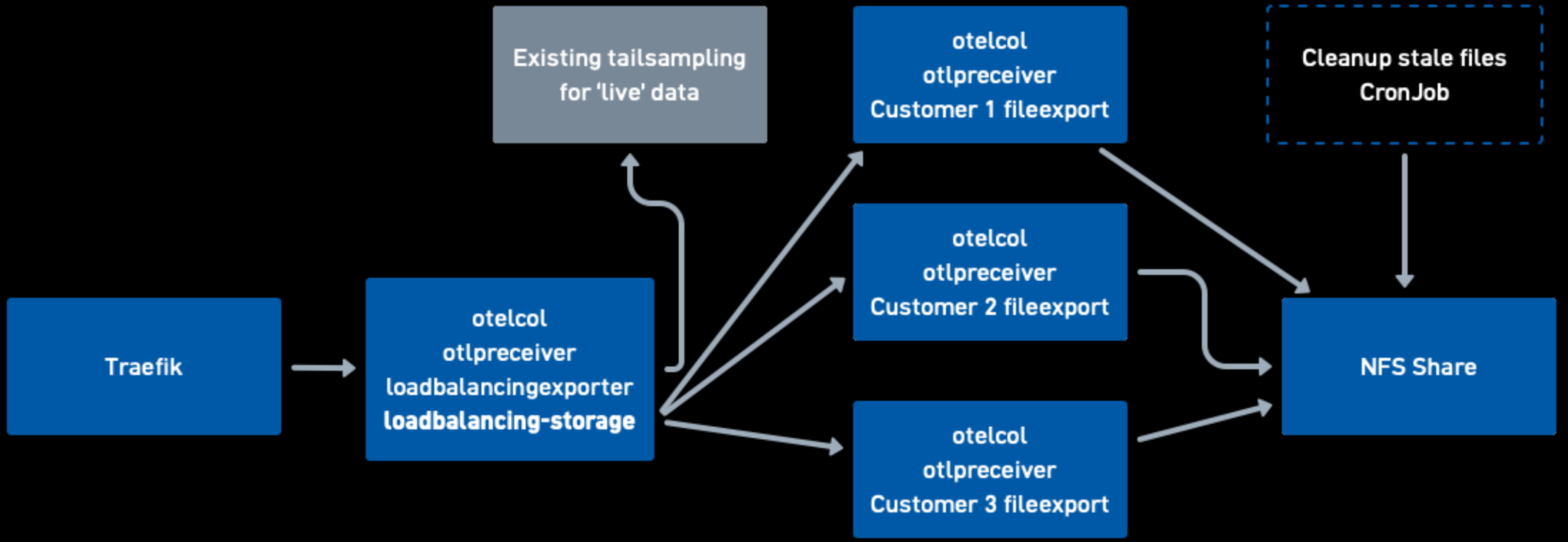
- Keep it *extremely* simple - no Kafka if we can avoid it
- Initial costing on SMB shares
  - Provisioned performance
  - Compression is a problem for “later”

More Iteration More Furious

- Challenges:
  - Memory accounting -> OOM -> nocache mountoption
  - Logrotation difficult due to non-POSIX -> NFS
  - Uneven load -> distribute load by customer ID

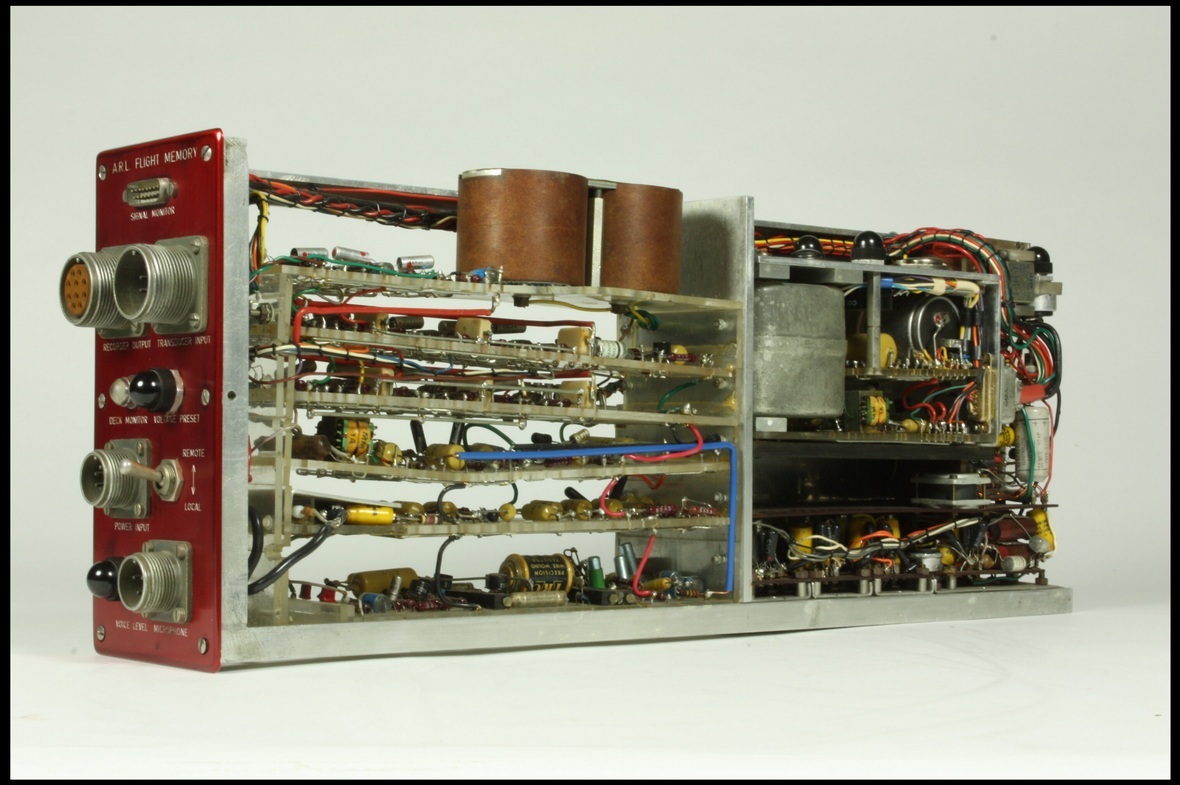
More Iteration More Furious

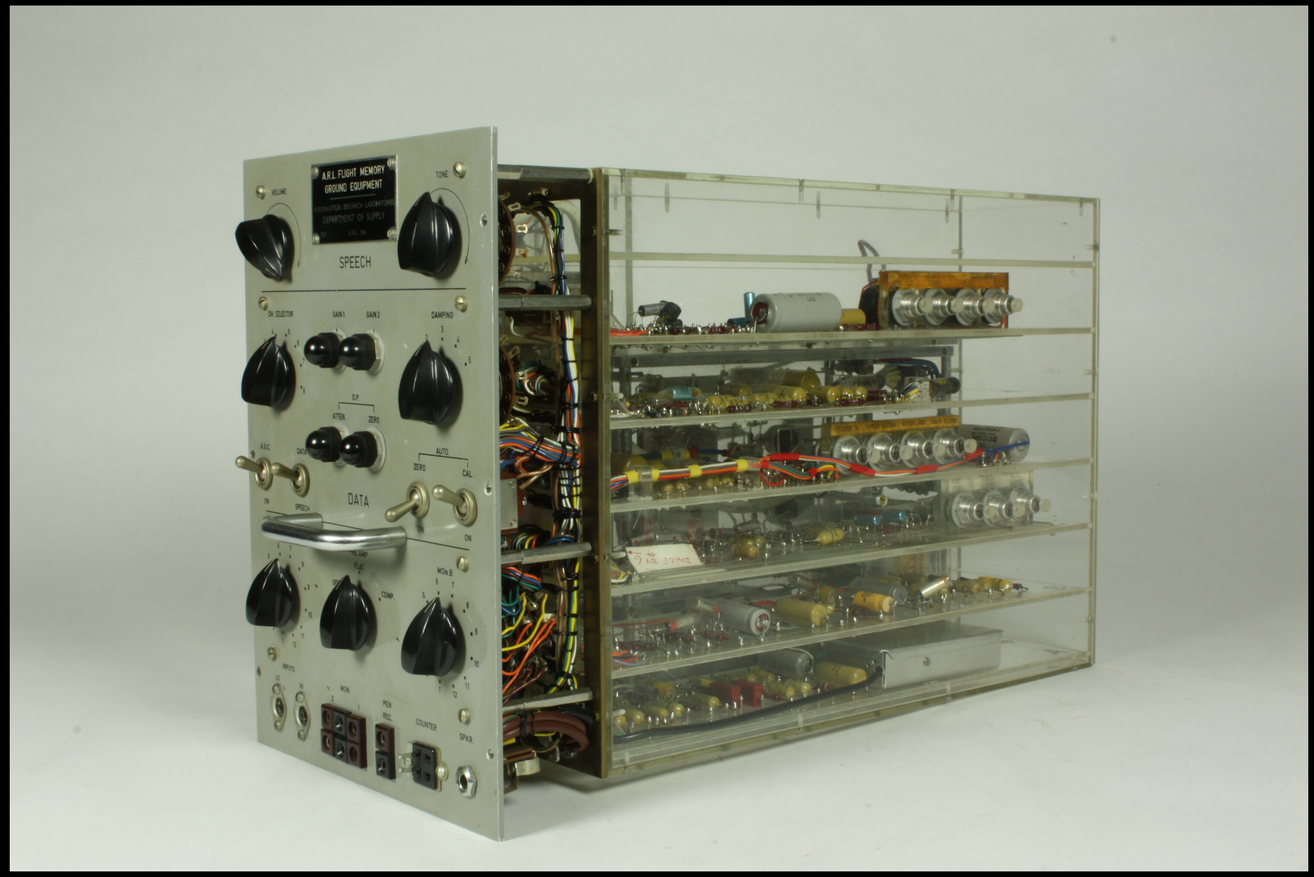
- Final tweaks:
  - Compression arrives as opt-in feature -> *way* cheaper on disk
  - Go GC tuning for predictable memory consumption
  - Fix racing for stale files cleanup


Existing tailsampling
for 'live' data
otelcol
otlpreceiver
Customer 1 fileexport
Cleanup stale files
CronJob
Traefik
otelcol
otlpreceiver
loadbalancingexporter
loadbalancing-storage
otelcol
otlpreceiver
Customer 2 fileexport
NFS Share
otelcol
otlpreceiver
Customer 3 fileexport

```yaml
exporters:
  file/cold_storage:
    path: /#{ColdStorageName}/traces/*.zst
    format: json
    compression: zstd
    compression_params:
      level: 1
    flush_interval: 1s
    group_by:
      enabled: true
      resource_attribute: cold_storage.path_segment # customer ID + replica name
    rotation:
      max_megabytes: 8 # this is approx 1 hr of traces for many cloud instances
      max_days: 7
      max_backups: 0 # unlimited
```

Replay





Copyright Museums Victoria / CC BY
Attribute this image
Photographer: David Thompson
Museums Victoria

https://collections.museumsvictoria.com.au/items/405748
https://collections.museumsvictoria.com.au/items/401038

Runbooks / Replay Traces

Run Replay Traces on PreProd

main -o- c7dfc9e

Task Summary | Task Log | Waterfall Preview | History | Details | Kubernetes

This task started 2 days ago and ran for 3 minutes

- Run Replay Traces on PreProd
  - The run completed successfully.
- Step 1: Validate inputs
- Acquire packages
- Step 2: Create ConfigMap for estimating replay
- Step 3: Deploy job to estimate replay size
- Step 4: Print replay estimate for review
  - binnacle-preprod-australiaeast

```
Extracting dependency '/octopus/Files/https_github.com_OctopusDeploy_Binnacle-OpenTelemetry.git@
Directories that will be replayed to Honeycomb
-------------------------------------------
8.1M      /cold-storage/traces/i071823/9-15-23
7.1M      /cold-storage/traces/i071823/9-16-0
---
Total (2 hours): 15.2M
Total estimate of Honeycomb Events consumed: 232,873
This is expected to consume 0.4% of the daily Honeycomb budget (58.3 million events per day)
This replay is expected to cost $0.9 USD. (4 USD per million events)
REPLAY_DIRS=i071823/9-15-23,i071823/9-16-0
DryRun: true. Traces will NOT be replayed to Honeycomb if you proceed.
```

Jul 20 2026 at 19:50:43 – Jul 31 2026 at 18:39:18 UTC+10:00 (Granularity: 30 min)



Overview | BubbleUp | Correlations | Traces | Explore Data

coldstorage.replay

true

elapsed query time: 441.545019ms examined 81,572,800 rows more details > copy

Summary

Summary

- Daunting task, but ultimately collaboration and low time pressure got us there
- Current operational burden low - automated maintenance FTW
- Self-service configuration changes - we are *not* gatekeepers
- 7 days of forensics at (nearly) no extra charge!

What can you apply?

Telemetry infrastructure and telemetry design are interdependent

Prepare to fail

Choose Boring Technology

Dan McKinley - https://boringtechnology.club/

Yes, `otelcol` is *boring*™

[laudatory]

$500/day

Observability or Forensics?
Why not both?

Who is the ‘ICAO’ of software?

ICAO: International Civil Aviation Organization

Acknowledgements

- Nick Travaglini - https://www.frctlflm.blog/blog/specious-historiography
- My team, especially Lindsay Bec
- My partner Clio
- Phil Rowlands
- You!

Cail Young

@cail.bsky.social

Bluesky, obviously. We don’t talk about the other place.

https://linkedin.com/in/cailyoung

Questions?