

AI generated image created by Gemini

STPA for Software Workshop - Handout

SREcon EMEA

Dublin, October 14th, 2026

SRECON EUROPE MIDDLE EAST AFRICA
DUBLIN, IRELAND
13–15 October, 2026



Specification: Rollout Manager

[D] Definitions

[D.1] Rollout Manager (RM): Commercial software solution by Safe State Systems, Inc. that monitors the in-house API endpoints. It manages both rollouts and rollbacks of production services.
[D.2] Service: Serves online HTTP traffic on one or more API endpoints.
[D.3] Attention set: The set of API endpoints monitored at one point in time.

[C] Configuration API

[C.1] Configuration files are submitted to RM via a Configuration API (HTTP/gRPC) or via the RM CLI tool (a wrapper around the API). The exact config files submitted by clients are called *configured attention sets*.
[C.2] Upon loading a configured attention set, the Configuration API internally computes an *effective attention set* using the following algorithm:

- [C.2.1] For each service (`service_id`) in the `include` section of the provided configured attention set, all of its `api_endpoints.name` (regexps) are matched against the API endpoint names returned by a call to the `discovery_service_url`.
- [C.2.2] The same is done for the `exclude` section, if that exists for the same `service_id`.
- [C.2.3] The Configuration API calculates the set difference between the included API endpoints and the excluded API endpoints. The resulting set of API endpoints are those that RM effectively monitors.

[C.3] Upon computing a new effective attention set, Configuration API caches it with a 30 min TTL.
[C.4] Configuration API limits (configurable) the total number of API endpoints being monitored.
[C.5] Access to the Configuration API is controlled by a set of read-write ACLs.
[C.6] RM limits the number of times per second the attention set can be submitted (global default: 10).
[C.7] RM provides a UI that displays the last configured attention set successfully loaded via the CLI tool.

[R] Runtime

[R.1] Rollout and rollback lifecycle is shown in Figure 1.
[R.2] After a new version of a service in the effective attention set is available, RM queues it for rollout to production.

- [R.2.1] The *rollout queue* (FIFO) is internal to RM and it accepts all rollouts and rollbacks.
- [R.2.2] The RM UI displays the state of all queued rollouts/rollbacks (QUEUED, RUNNING, PAUSED, FAILED, FINISHED)

[R.3] RM rolls back a service to its previous version if:

- [R.3.1] After a rollout of a new version, the error rate of any of the service API endpoints deviates upward from the error rate of the previous version; AND
- [R.3.2] The error rate of any of the service API endpoints exceeds its `error_rate_threshold`.

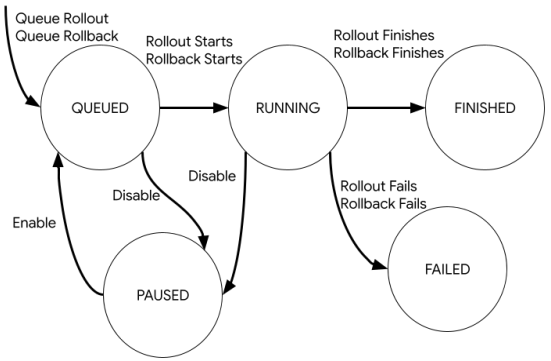


Figure 1: Rollout/Rollback Lifecycle States

[R.4] RM CLI tool allows *disabling* a service, resulting in stopping the monitoring of all its API endpoints. If the service is currently not in the configured attention set, then RM CLI tool returns an error.
[R.5] Disabling a service will pause (state: PAUSED) all rollouts and rollbacks for that service.
[R.6] RM CLI tool allows *enabling* a service, resulting in restarting the monitoring of all its API endpoints. If the service is currently not in the configured attention set, then RM CLI tool returns an error.
[R.7] Enabling a service will re-queue all PAUSED rollouts and rollbacks for that service, i.e. PAUSED->QUEUED.

Example Configuration

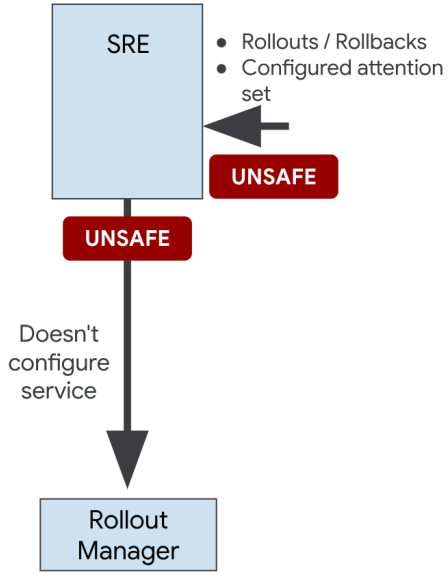
RM is configured via a text YAML file listing which API endpoints are monitored in the attention set. An example of YAML-based configuration:

```
# Managed Services Configuration
# Safe State Systems Rollout Manager (AIOps Automations
- Spec 2.1)

# Centralized naming service for dynamic endpoint
discovery
discovery_service_url:
"https://ns.internal.safestate.systems/v1/published_endpoints"

include:
 # --- Service 1: Authentication ---
 - service_id: "auth-v3-prod"
   service_name: "Global User Authentication Service"
   service_root_url: "https://auth.safestate.systems"
   api_endpoints:
     - name: "/api/v3/users/authenticate"
       error_rate_threshold: 5
     - name: "/api/v3/mfa/generate_code"
       error_rate_threshold: 2
     - name: "^/api/v3/profile/.*$"
       error_rate_threshold: 10

 # --- Service 2: AIOps Engine ---
 - service_id: "aiops-core-engine"
   service_name: "Core Telemetry Analysis Engine"
   service_root_url: "https://engine.internal.safestate.systems"
   api_endpoints:
     - name: "/engine/telemetry_ingest"
       error_rate_threshold: 50
     - name: "/engine/model/v[0-9]+/process"
       error_rate_threshold: 15

exclude:
 # --- Service 2 Overrides ---
 - service_id: "aiops-core-engine"
   service_name: "Core Telemetry Analysis Engine"
   service_root_url: "https://engine.internal.safestate.systems"
   api_endpoints:
     - name: ".*/metrics/experimental"
```

Activity 1: Loss Scenarios, Unsafe Feedback



UCA: Site Reliability Engineering **does NOT provide** Configure Service to Rollout Manager when Rollout Manager **is NOT** monitoring the API endpoint [H-1]



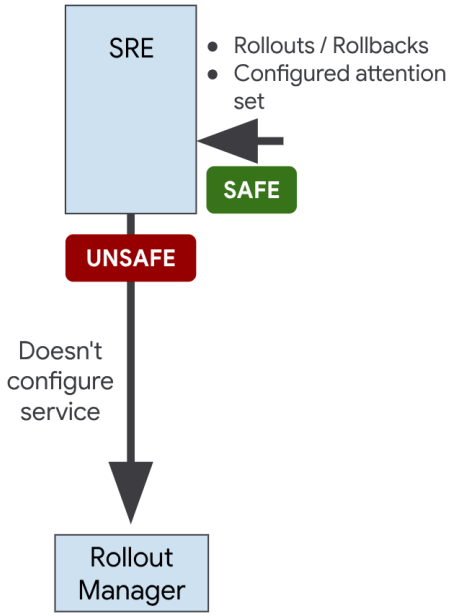
Question: How can you explain that:

1. **True state:** Rollout Manager **is NOT** monitoring the API endpoint
2. UNSAFE The feedback does **NOT** adequately indicate that the rollout manager is **NOT** monitoring the API endpoint
3. UNSAFE **Control action:** SRE **does NOT provide** Configure Service

Write out your unsafe feedback scenarios below:

Activity 2: Loss Scenarios, Unsafe Controller Behavior

UCA: Site Reliability Engineering **does NOT provide** Configure Service to Rollout Manager when Rollout Manager **is NOT** monitoring the API endpoint [H-1]



Question: How can you explain that:

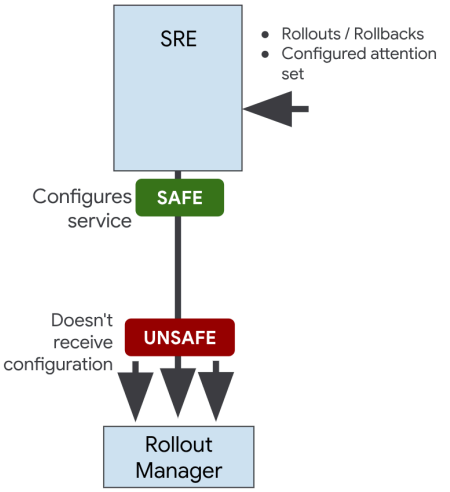
1. **True state:** Rollout Manager **is NOT** monitoring the API endpoint
2. SAFE The feedback **DOES** indicate that the rollout manager is **NOT** monitoring the API endpoint
3. UNSAFE **Control action:** SRE **does NOT provide** Configure Service

Write out your unsafe controller behavior scenarios below:

Activity 3: Loss Scenarios, Unsafe Control Path



UCA: Site Reliability Engineering **<u>does NOT provide</u>** Configure Service to Rollout Manager when Rollout Manager **<u>is NOT</u>** monitoring the API endpoint [H-1]



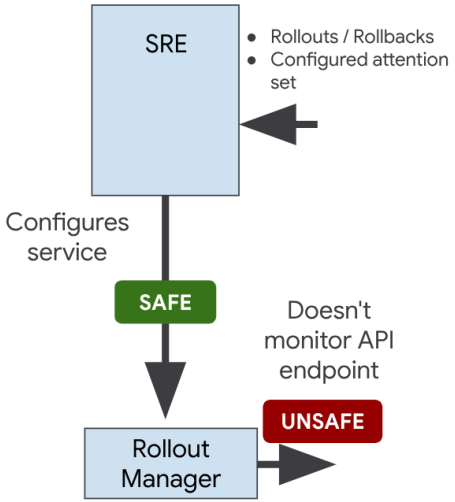
<u>Question:</u> How can you explain that:

1. **True state:** Rollout Manager **<u>is NOT</u>** monitoring the API endpoint
2. SAFE **Control action:** SRE provides Configure Service
3. UNSAFE Rollout Manager **<u>does NOT receive</u>** the configuration update

<u>Write</u> out your unsafe control path scenarios below:

Activity 4: Loss Scenarios, Unsafe Controlled Process Behavior

UCA: Site Reliability Engineering **does NOT provide** Configure Service to Rollout Manager when Rollout Manager **is NOT** monitoring the API endpoint [H-1]



Question: How can you explain that:

1. **True state:** Rollout Manager **is NOT** monitoring the API endpoint
2. SAFE **Control action:** SRE provides Configure Service
3. Rollout Manager **receives** the configuration update
4. UNSAFE Rollout Manager **does NOT start** monitoring the API endpoint

Write out your unsafe controlled process behavior scenarios below: