swisscom

# From Weeks to Seconds: Scaling Network Automation with Kubernetes Operators

Cloud Native Zurich Rejects, 03.06.2025

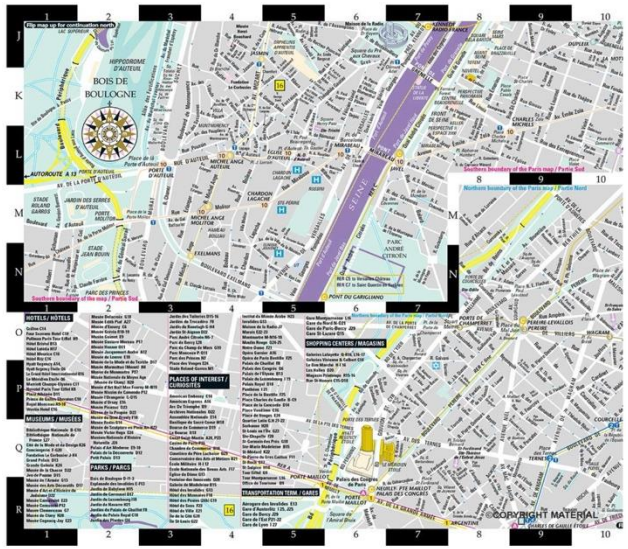
Pablo Garcia, Fabian Schulz

# An Analogy…

**Static paper map**

- Fixed
- Static
- Unchanging
- Overwhelming

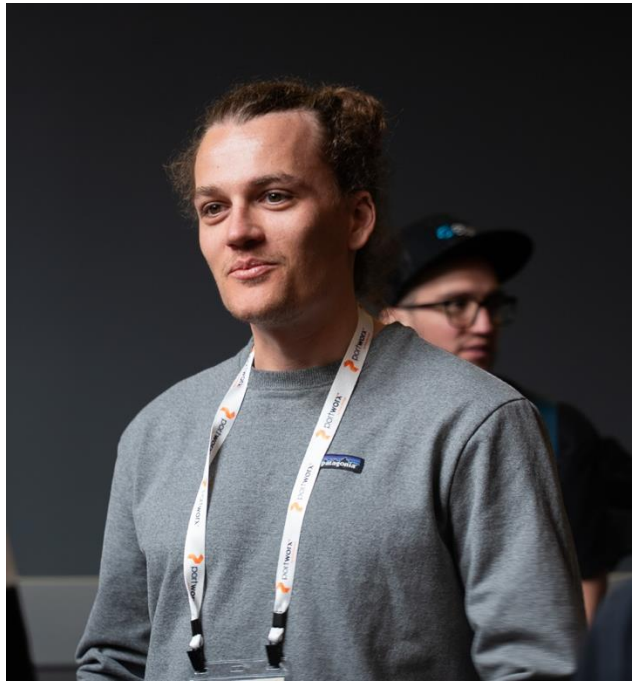
**This is GitOps today**




**Navigation App**

- Dynamic
- Changes based on external conditions
- More focused
- Simple to navigate

**This is GitOps w/ KRM**

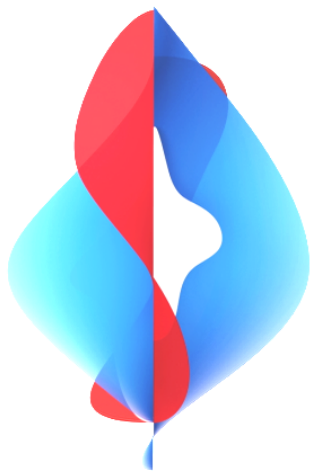


**Fabian Schulz**
DevOps Engineer

fabian.schulz1@swisscom.com

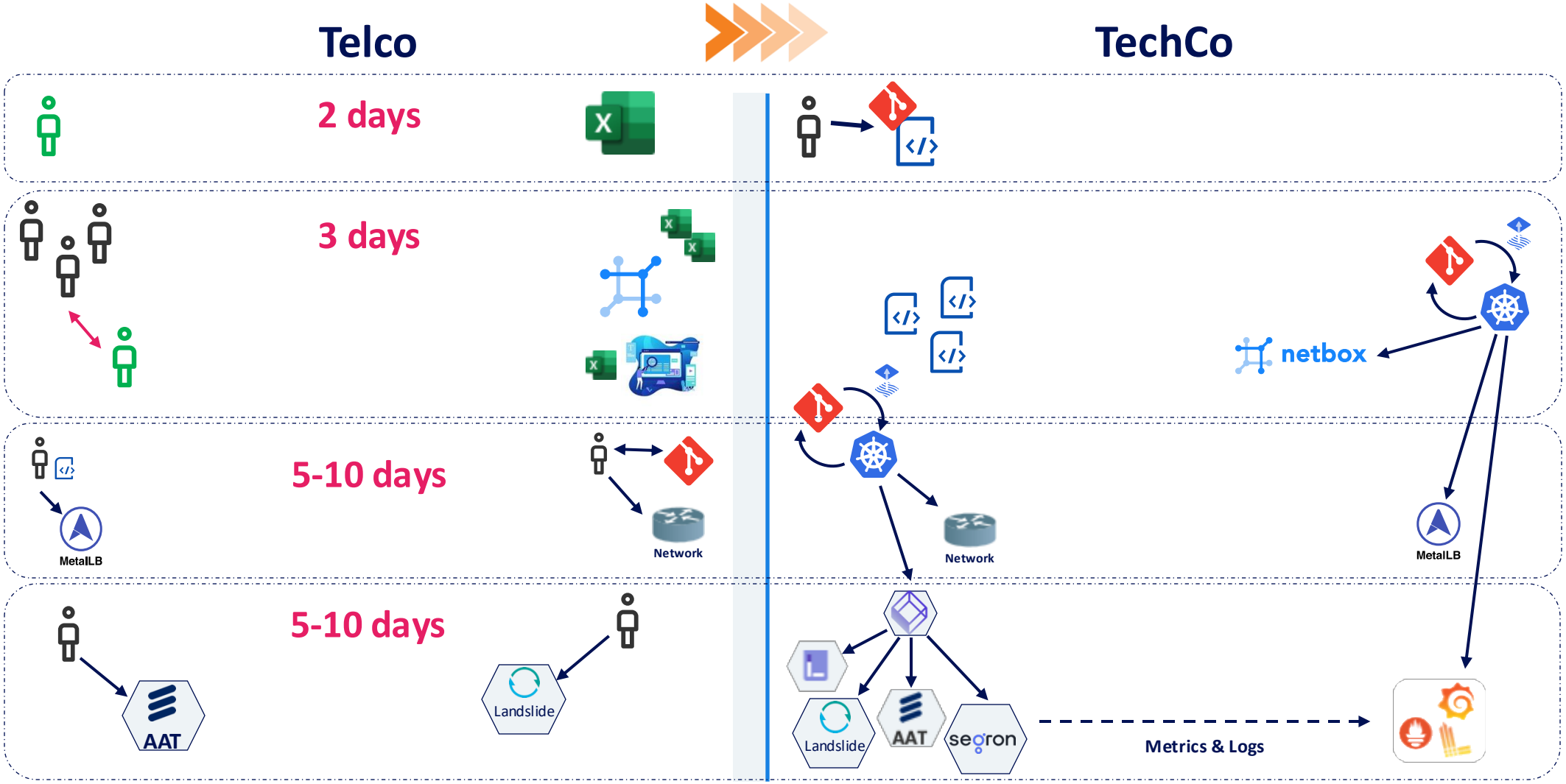
**Pablo Garcia**
DevOps Engineer

pablo.garciamiranda@swisscom.com

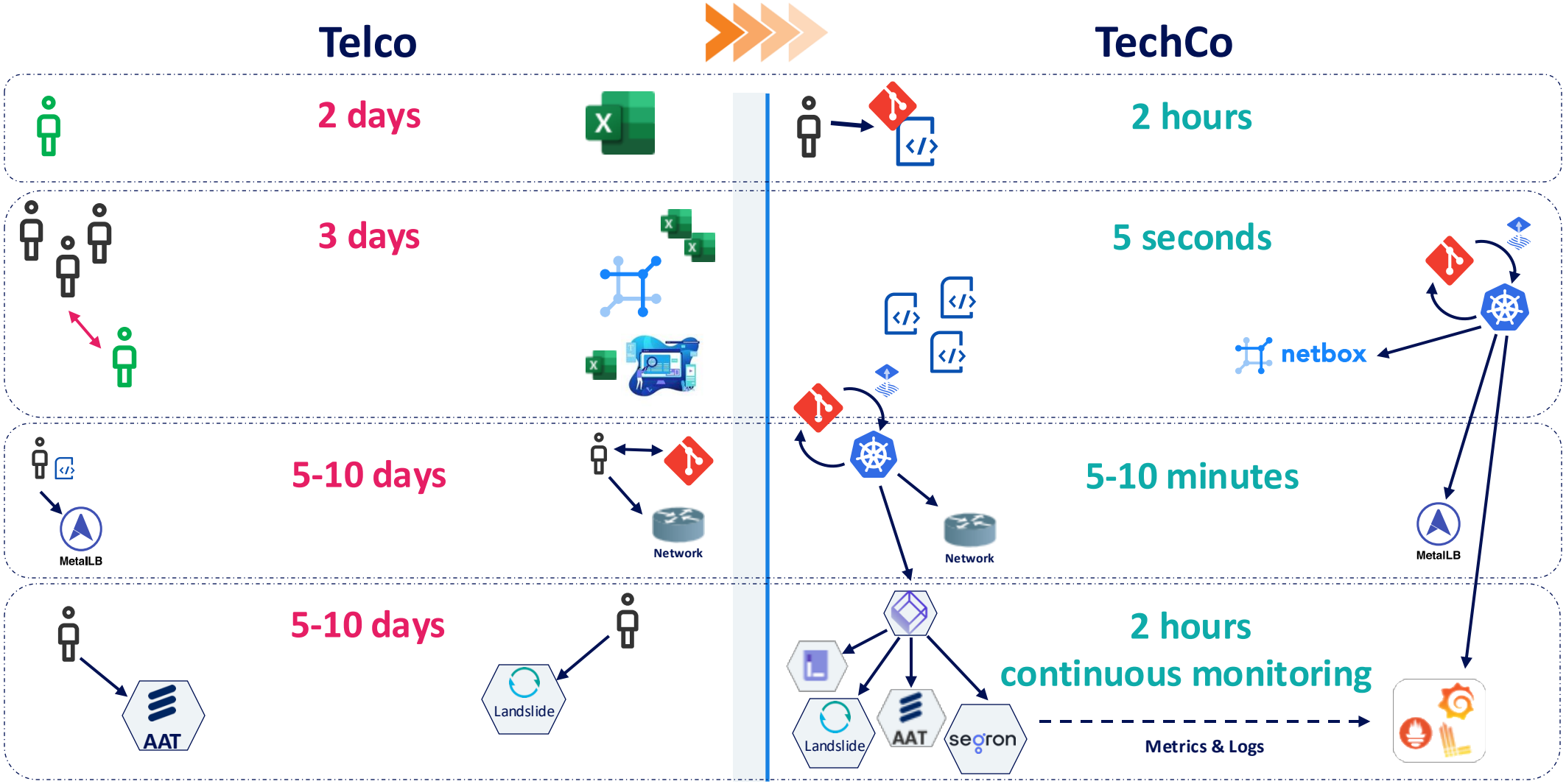


swisscom

# Productivity Gains Using Intent-Driven Automation



# Productivity Gains Using Intent-Driven Automation



# What Is a 5G Core?

**Each blue object**

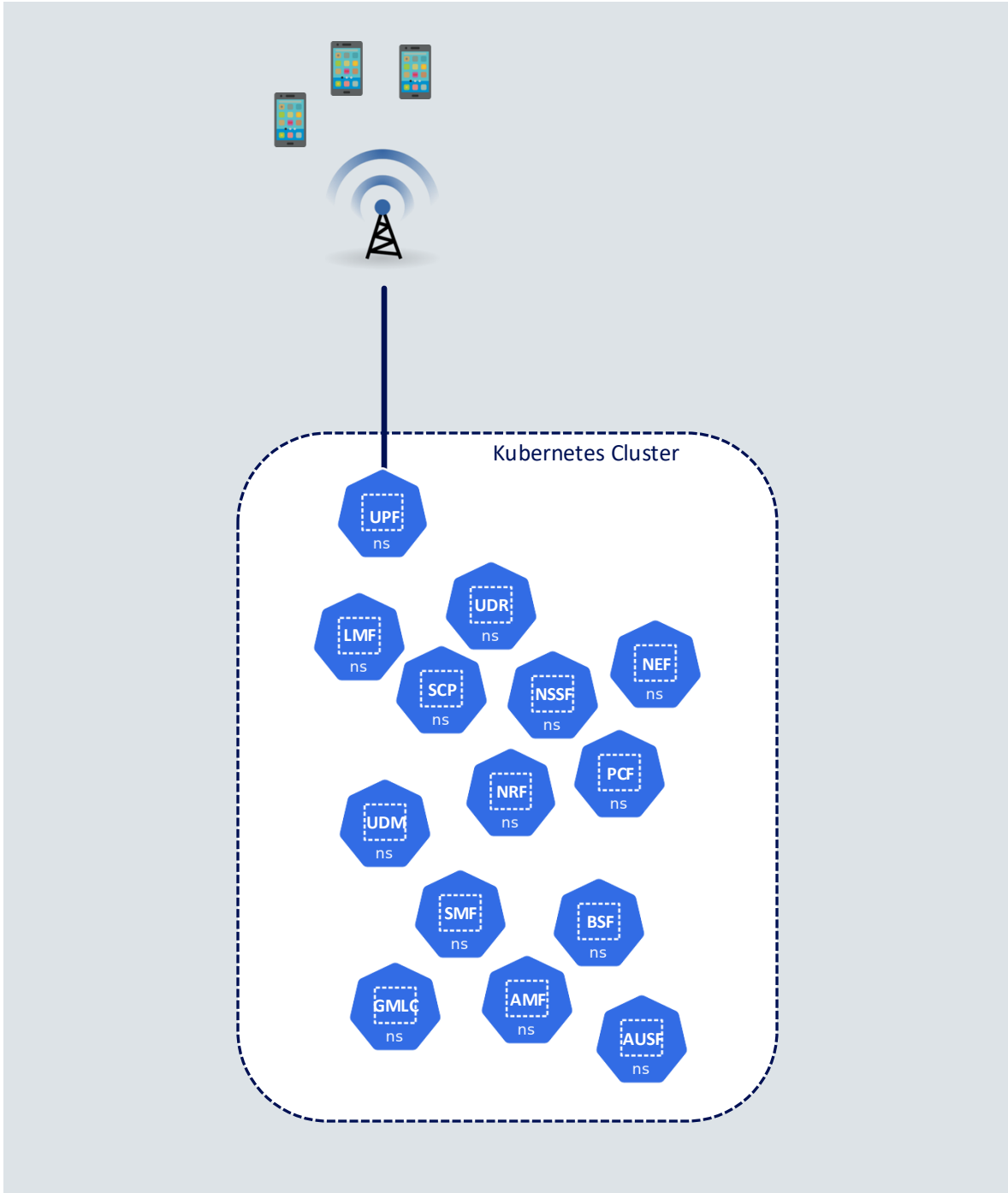
- is a «CNF» aka «Containerized Network Function»
  - e.g. Router (UPF), Authentication Service (AUSF)
- Deployed using Helm

**Configuration is done via**

- Helm Values
- Other Configuration Interfaces

**Scale**

- A development environment contains ~2000 pods
- A total of 5000 interdependent configuration parameters



# What Is a 5G Core?

IP addresses

Subnets

VLANs

DNS Records

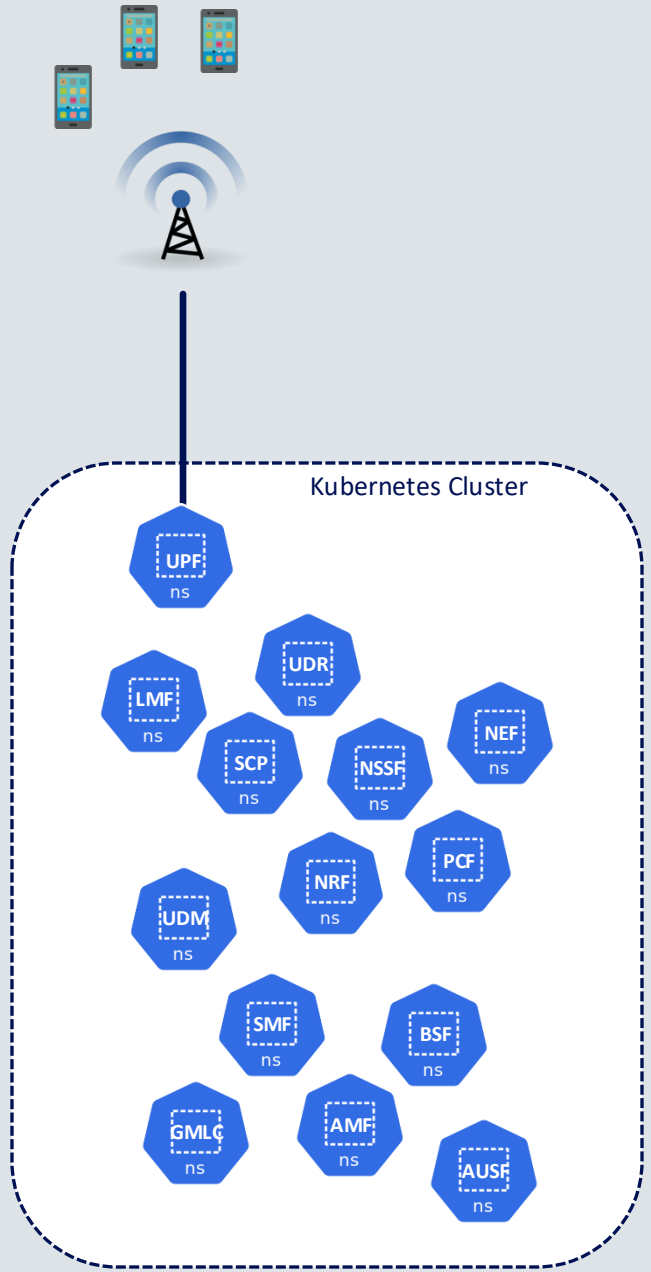
Network function variables

Infrastructure variables

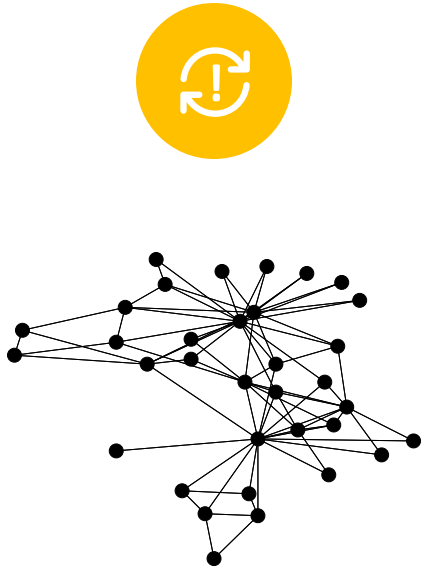
Network function-Network function mapping

Secret references

Certificate references

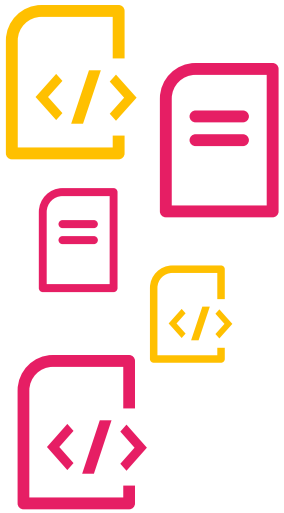



# Key Challenges



**Network Automation Complexity**

Dual Mode Core adds both 4G and 5G NFs; complexity grows



**Limited Scalability**

Complex NF configurations; many integrations; limits scaling

**System Lock-in**

Proprietary tools block multi-vendor options

# What Are Our Requirements?

**KRM Based**

Input and Output can be Kubernetes Resource Model (KRM)

**Garbage Collection**

Resources belonging together are lifecycled together

**Output Flexibility**

Generated resources stored with various backends

**Reconciliation**

Output is updated as Input is changed

**Functions**

Ability to define helper functions (e.g. string manipulation)

**Gradual Adoption**

Migration from static to dynamic taken at own pace.

# But What About Helm, Kustomize, Argo and Flux?

### Limited Dynamic Assembly

We cannot use live Kubernetes resources as source of information for e.g. a helm release

### No Custom Functions

We cannot invoke arbitrary code into Kustomize/Helm templating

### Only Partially KRM

Not all Resources involved follow KRM (e.g. Helm Values)

# What do we need to run a 5G-Core?


**IPAM**

Prefix and IP address management system

**Routing**

Routing traffic to our services and back

**Configuration of Network Core**

Generate configuration for our workloads and apply them

**NetBox**

NetBox is the network source of truth used for IPAM and DCIM

netboxlabs.com/docs/netbox

**MetalLB & Network-as-a-Service**

Load balancing and router management

metallb.io

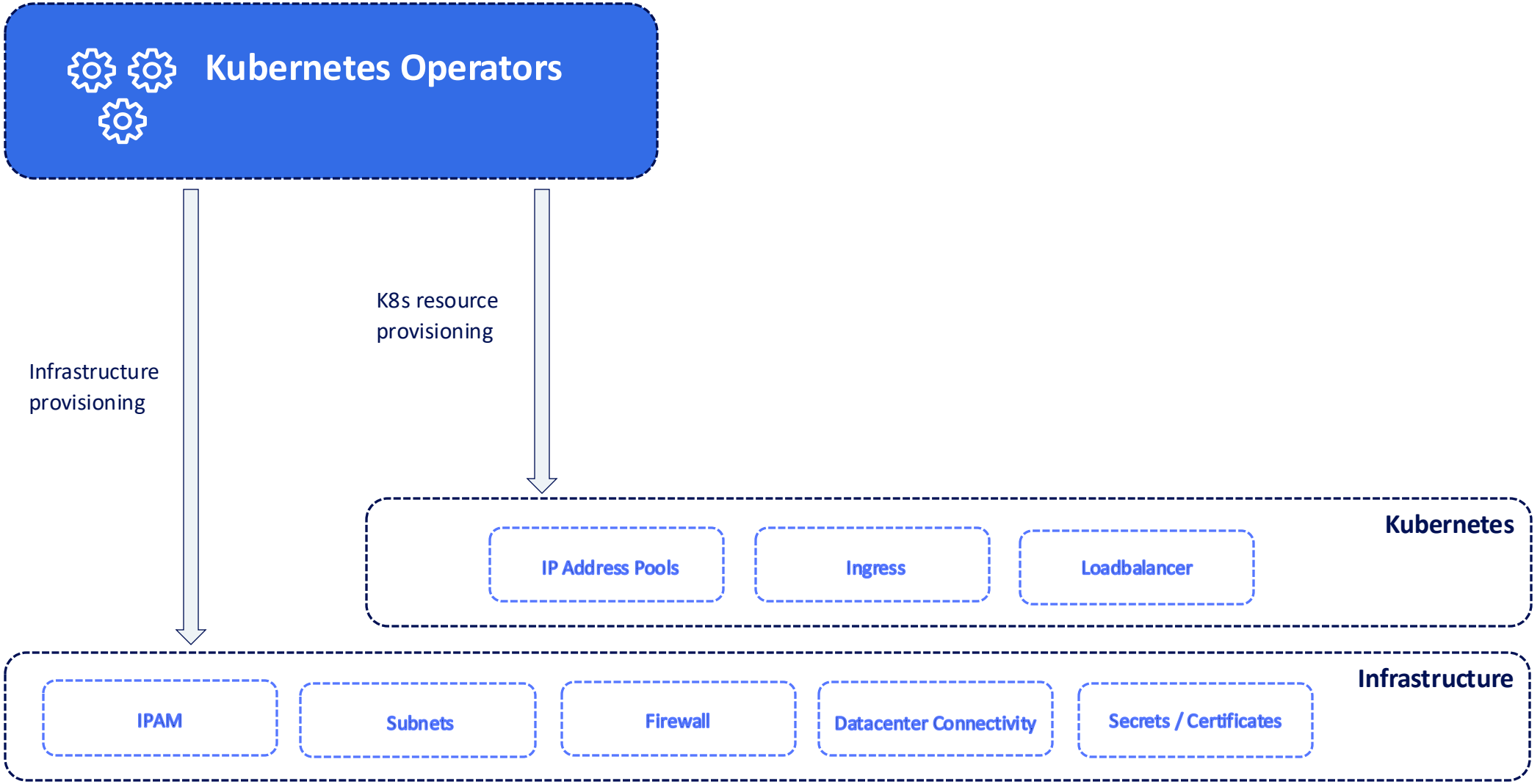
**SDCIO**

Cloud Native based Schema Driven Configuration

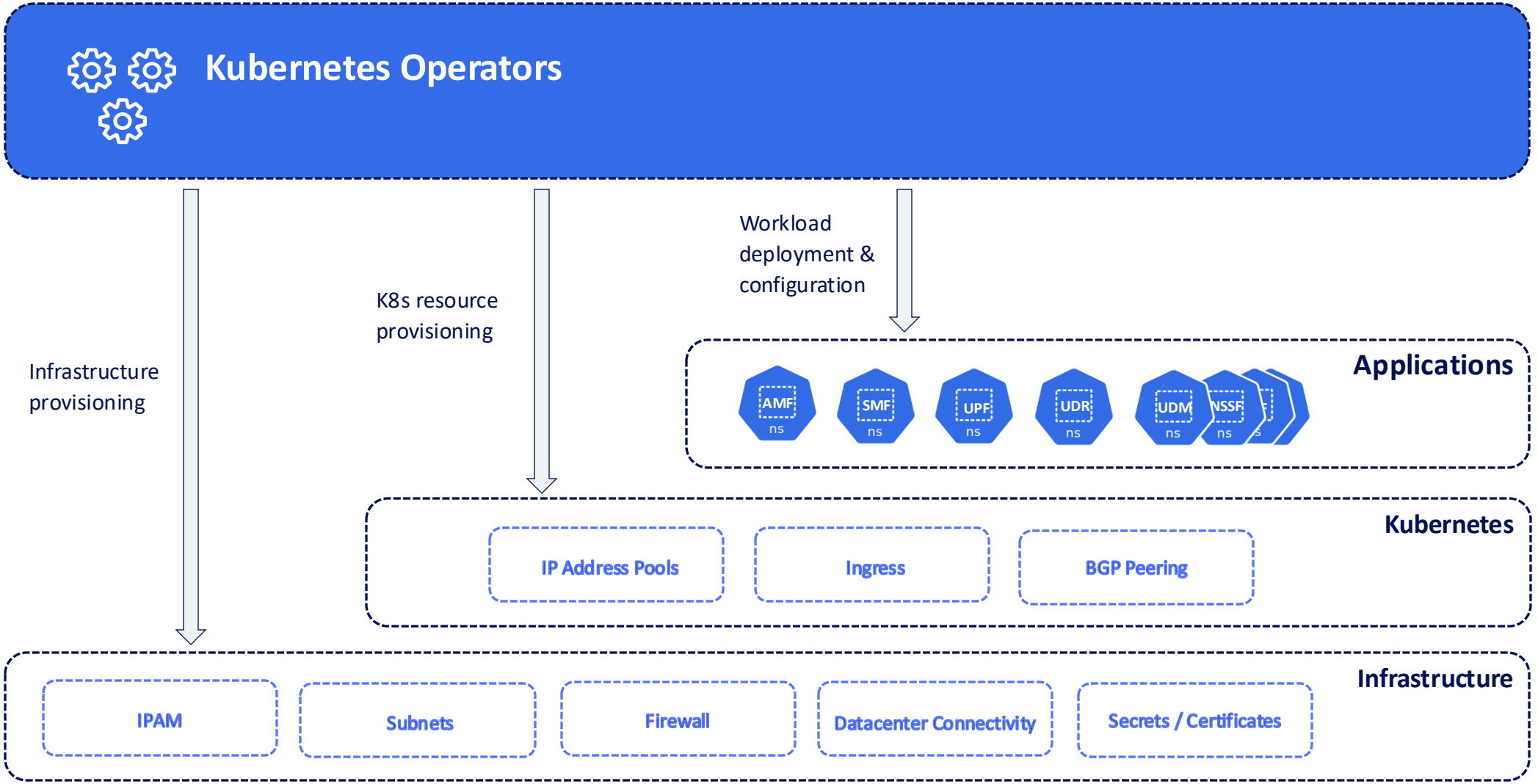
docs.sdcio.dev

# Cloud Native Resource Orchestration

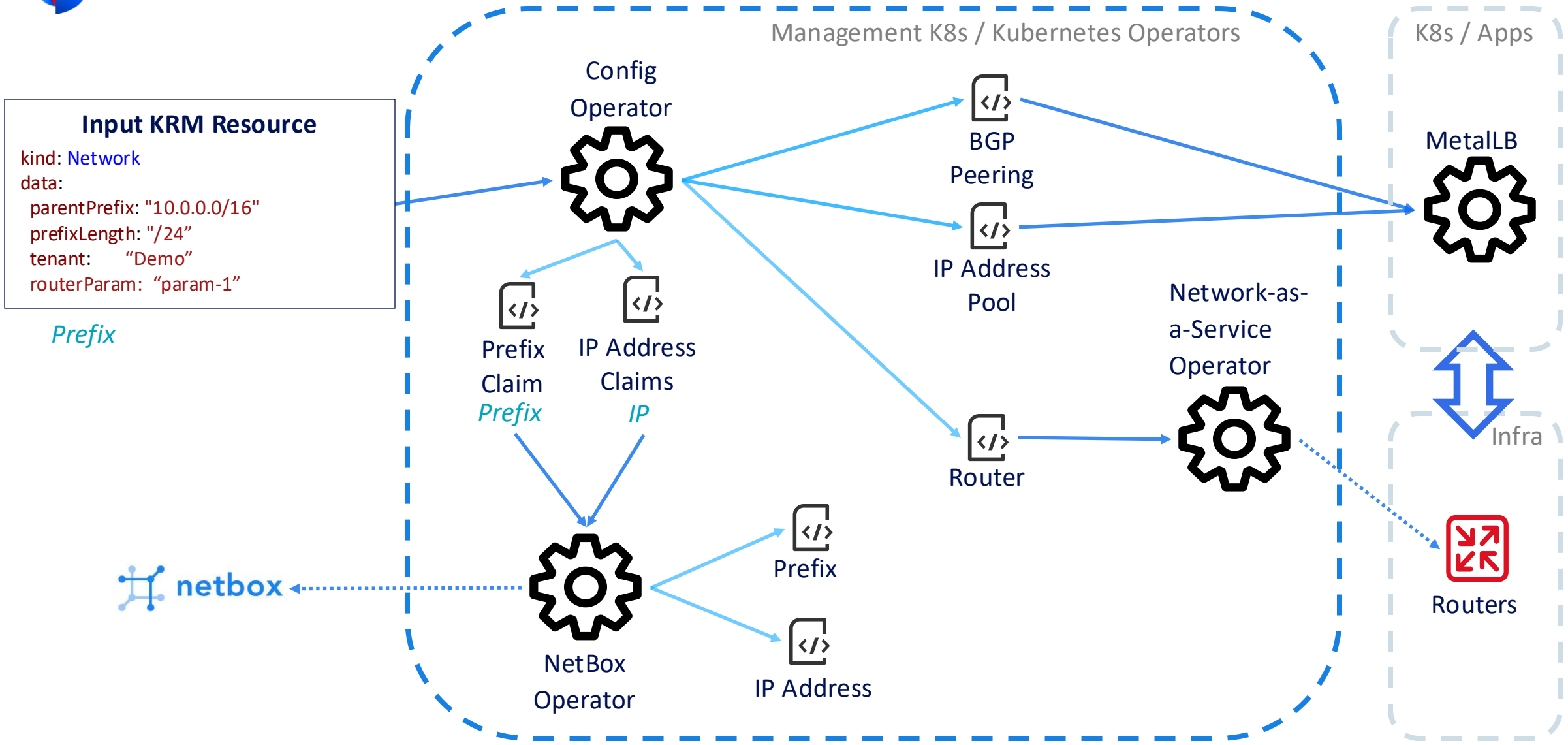
# Cloud Native Resource Orchestration



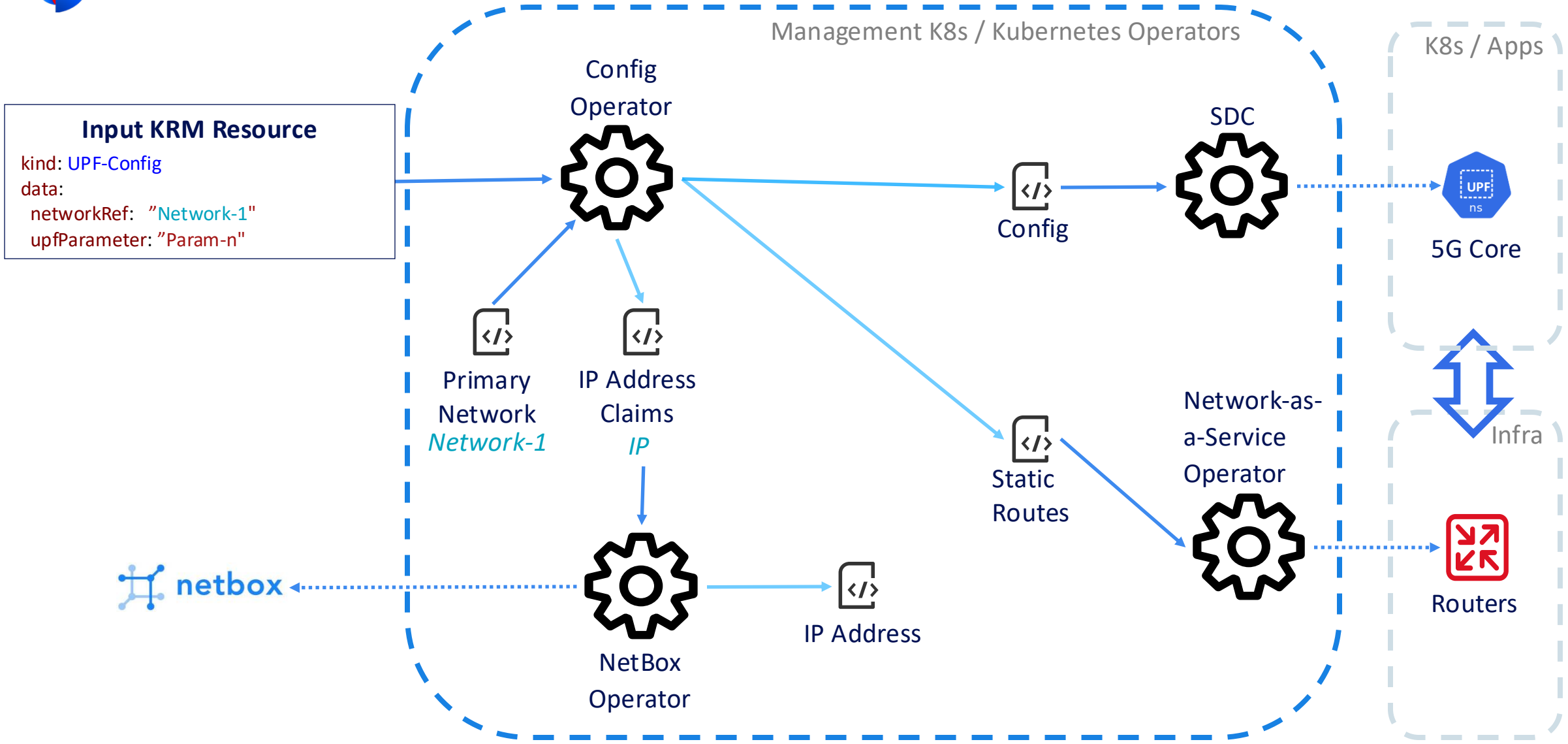
# Cloud Native Resource Orchestration



# Configuration Abstraction with Network Topology Operator



# Configuration Abstraction with Network Topology Operator



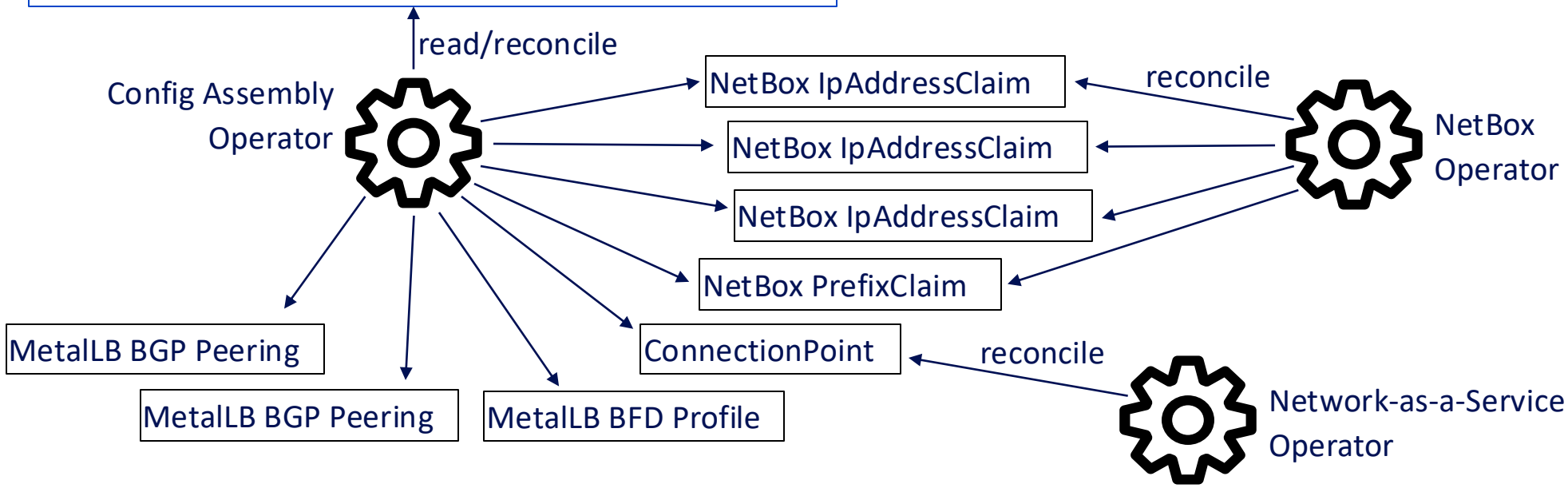

Demo

# Configuration Abstraction with Network Topology Operator

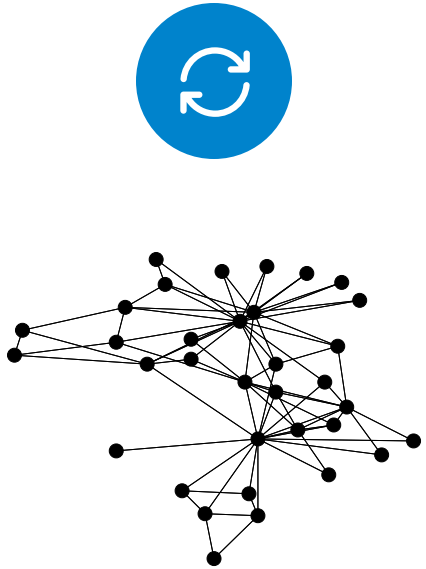
Intent

```
apiVersion: configassembly.swisscom.com/v1
kind: PrimaryNetworkTopology
spec:
  netBoxConfig:
    parentPrefixSelector:
      tenant: 5G
    prefixLength: /24
  metalLbAsn: 65000
```

Assembly



# How We've Overcome the Challenges



**Network Automation Complexity**

Automation of IPAM
and Data Center Network

**Limited Scalability**

Easy to scale since
using Kubernetes Operators

**System Lock-in**

Swisscom in full
control of the code

# Our Learnings & Suggestions

… on network automation using Operators

# Avoid

**Checking in low level configurations manually in Git**
Things like IP Addresses, VLAN IDs

**Complicated configurations**
Avoid unnecessary layers of abstraction and overengineer your Kubernetes operators

**Ignore tooling gaps**
Avoid using tools like Ansible or Jinja that aren’t designed with Kubernetes in mind

**Neglect Industry Relevance**
Don’t assume KRM challenges and solutions are unique to your sector

# Aim to

**Leverage abstraction**
Simplify complex configurations by focusing on essential controls

**Reuse cloud native tools to be in-band with K8s**
E.g. Flux, Argo, Testkube, cert-manager

**Use frameworks**
Build your operator using frameworks such a kubebuilder to concentrate on your business logic

**Add monitoring early**
integrate monitoring early so the not so k8s experienced users also have a great experience


Home › Dashboards › ROPEs Production
Add
Share
Last 6 hours
Tenants
5G DMC
EEA
EIC
vHSS
Total Connection Points
77
Total Static Routes
144
Prefix Claims
491
IP Range Claims
134
Primary Networks
32
Secondary Networks
27
IP Address Claims
205
MetalLB IP Pools
169
PCG Network Instances
6
PCC Network Instances
6
CCD Primary Networks
Primary Network Na
Status
Ready
CCD Secondary Networks
Secondary Network
Status
Ready
Static Routes
Static Route Name
Status
Ready
PCC Network Instance
PCC Network Instance
Status
Ready
PCG Network Instance
PCG Network Instance
Status
Ready
Total IP Prefixes per Tenant
Tenant ↓
Count
vhss-resources
44
eic
2
eea
7
Total Connection Points per Tenant
Tenant ↓
Count
vhss-resources
18
eic
1
eea
1

# Aim to

**Leverage abstraction**
Simplify complex configurations by focusing on essential controls

**Reuse cloud native tools to be in-band with K8s**
E.g. Flux, Argo, Testkube, cert-manager

**Use frameworks**
Build your operator using frameworks such a Kubebuilder to concentrate on your business logic

**Add monitoring early**
integrate monitoring early so the not so k8s experienced users also have a great experience

**Contribute to the ecosystem**
Share your code

https://github.com/netbox-community/netbox-operator

# Related Talks

**From Spreadsheets to "Everything as Code"**
*by Joel Studler and Jéremy Weber at ContainerDays 2023*

**How We Are Moving from GitOps to Kubernetes Resource Model in 5G Core**
*by Ashan Senevirathne and Joel Studler at KubeCon Europe 2024*

**Building and Operating a Highly Reliable Cloud Native DNS Service With Open Source Technologies**
*by Joel Studler and Fabian Schulz at ContainerDays 2024*

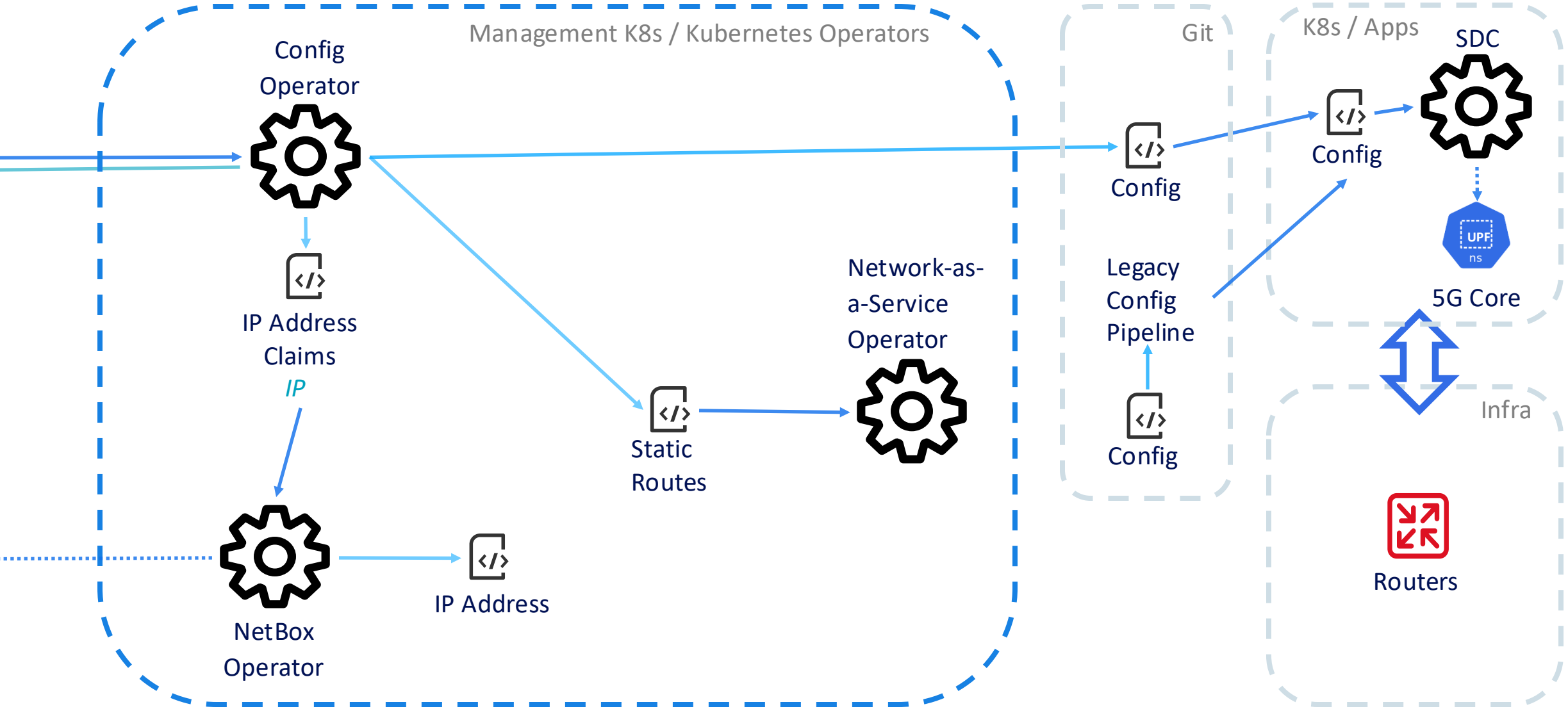
**Just Claim It: Simplifying Network Automation with NetBox Operator**
*by Joel Studler and Lea Bruhwiler at Cloud Native Telco Day 2025*

**Kubenet: Harnessing Kubernetes for Network Automation**
*by Ashan Senevirathne and Wim Hendrerickx at Cloud Native Telco Day 2025*

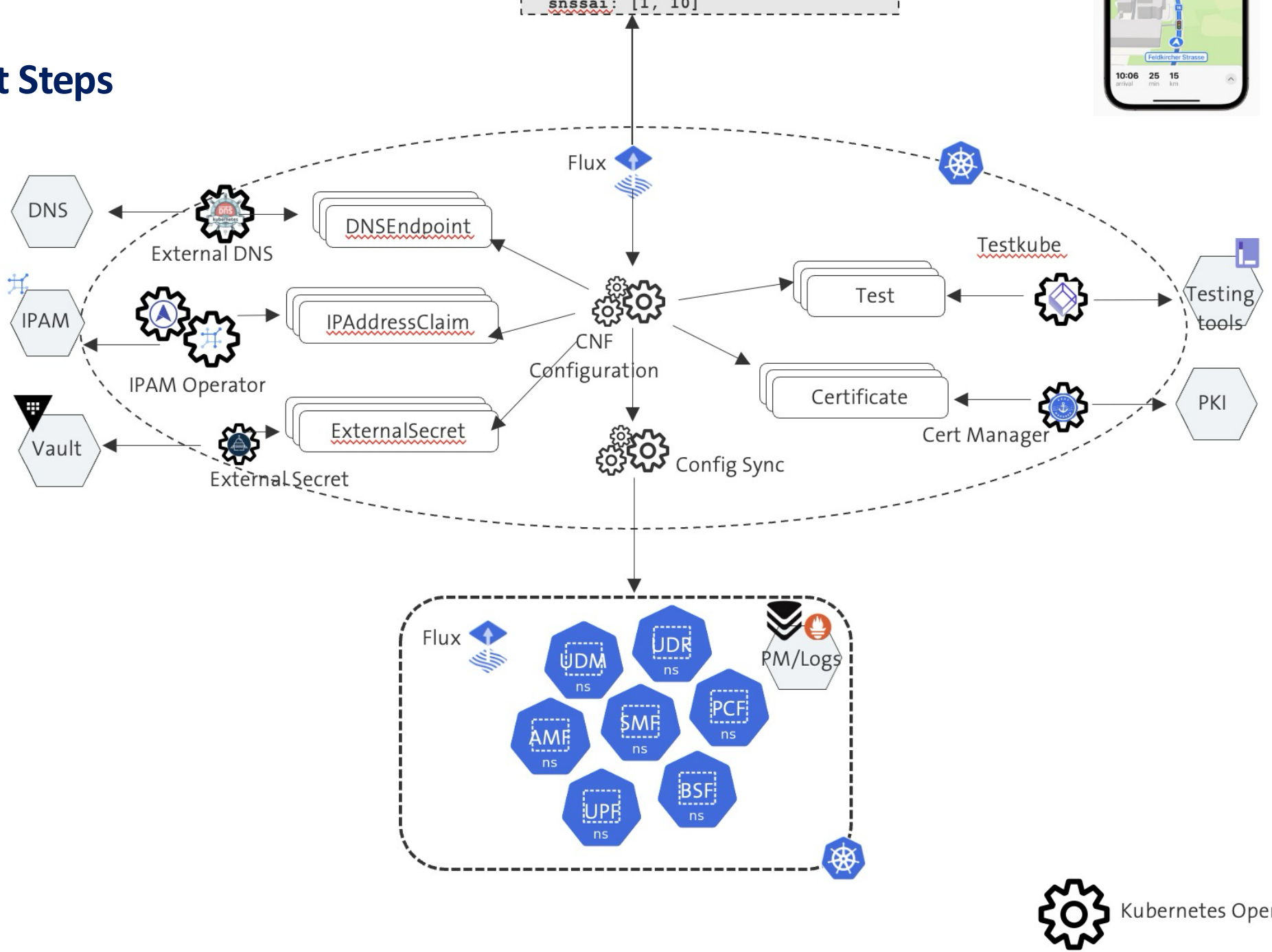
# Thanks!

# Q&A

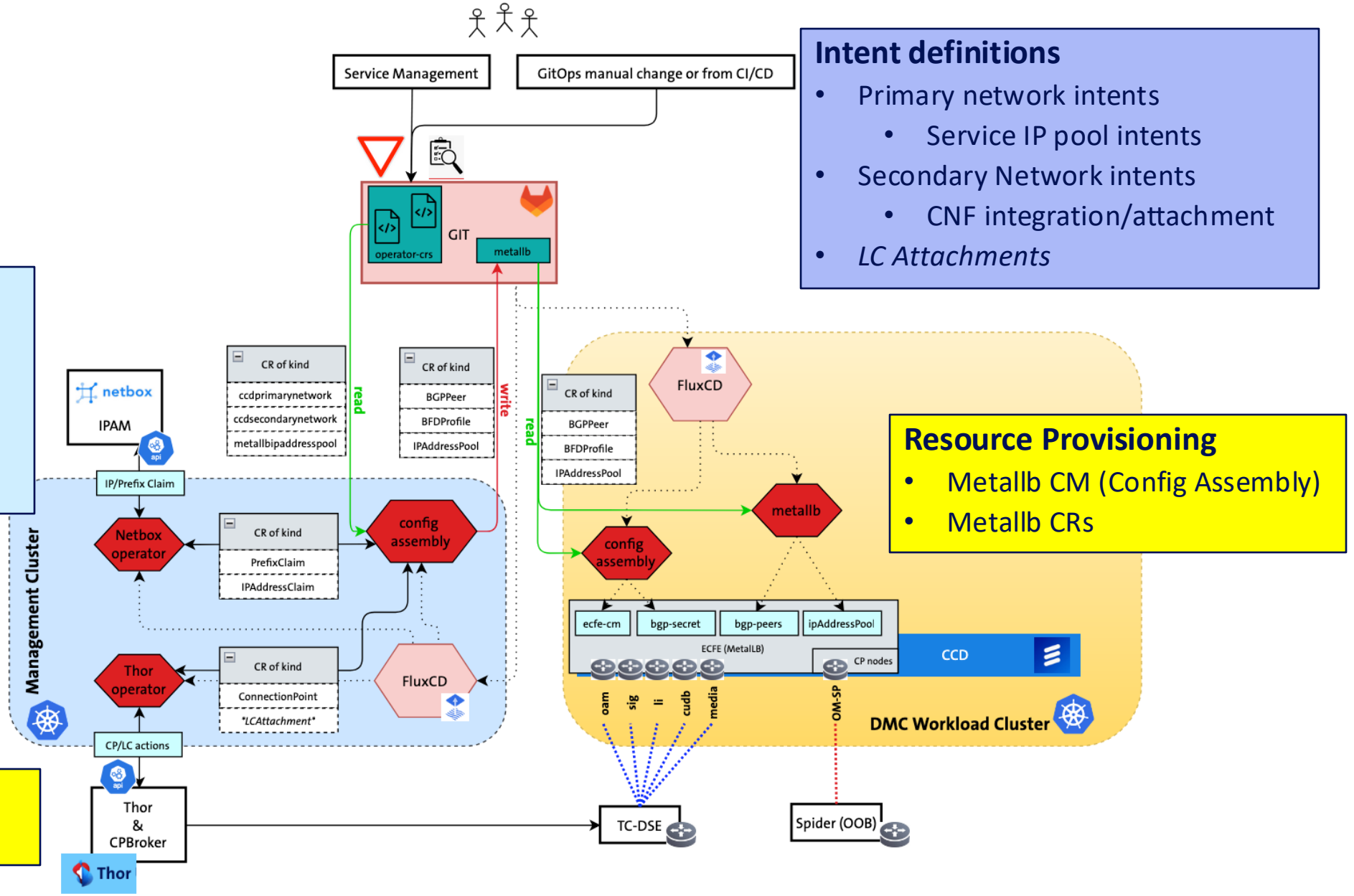
# Configuration Abstraction with Network Topology Operator



# Next Steps


snssai: [1, 10]
Feldkircher Strasse
10:06 arrival
25 min
15 km
Flux
DNS
External DNS
DNSEndpoint
IPAM
IPAM Operator
IPAddressClaim
CNF Configuration
Testkube
Test
Testing tools
Certificate
Cert Manager
PKI
Vault
External Secret
ExternalSecret
Config Sync
Flux
UDM ns
UDR ns
PM/Logs
AMF ns
SMF ns
PCF ns
UPF ns
BSF ns
Kubernetes Operator

# Demo: Primary Network Provisioning, including TC-DSE and Metallb config




## Intent definitions

- Primary network intents
  - Service IP pool intents
- Secondary Network intents
  - CNF integration/attachment
- *LC Attachments*

## Resource Orchestration

- Netbox (IPAM) operator
- Thor (TC-GW) operator
- Config Assembly (Network Topology) operator

## Resource Provisioning

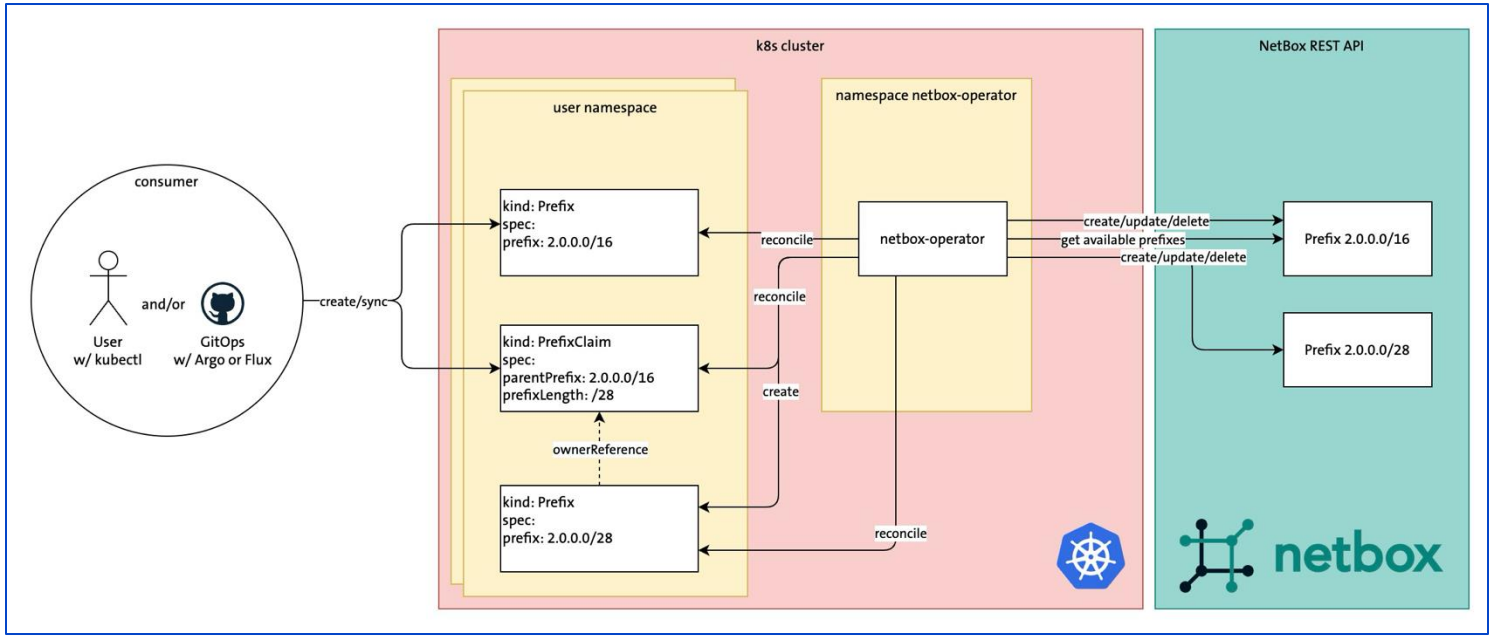
- Metallb CM (Config Assembly)
- Metallb CRs

## Thor Provisioning

- TC-DSE configuration

# NetBox Operator

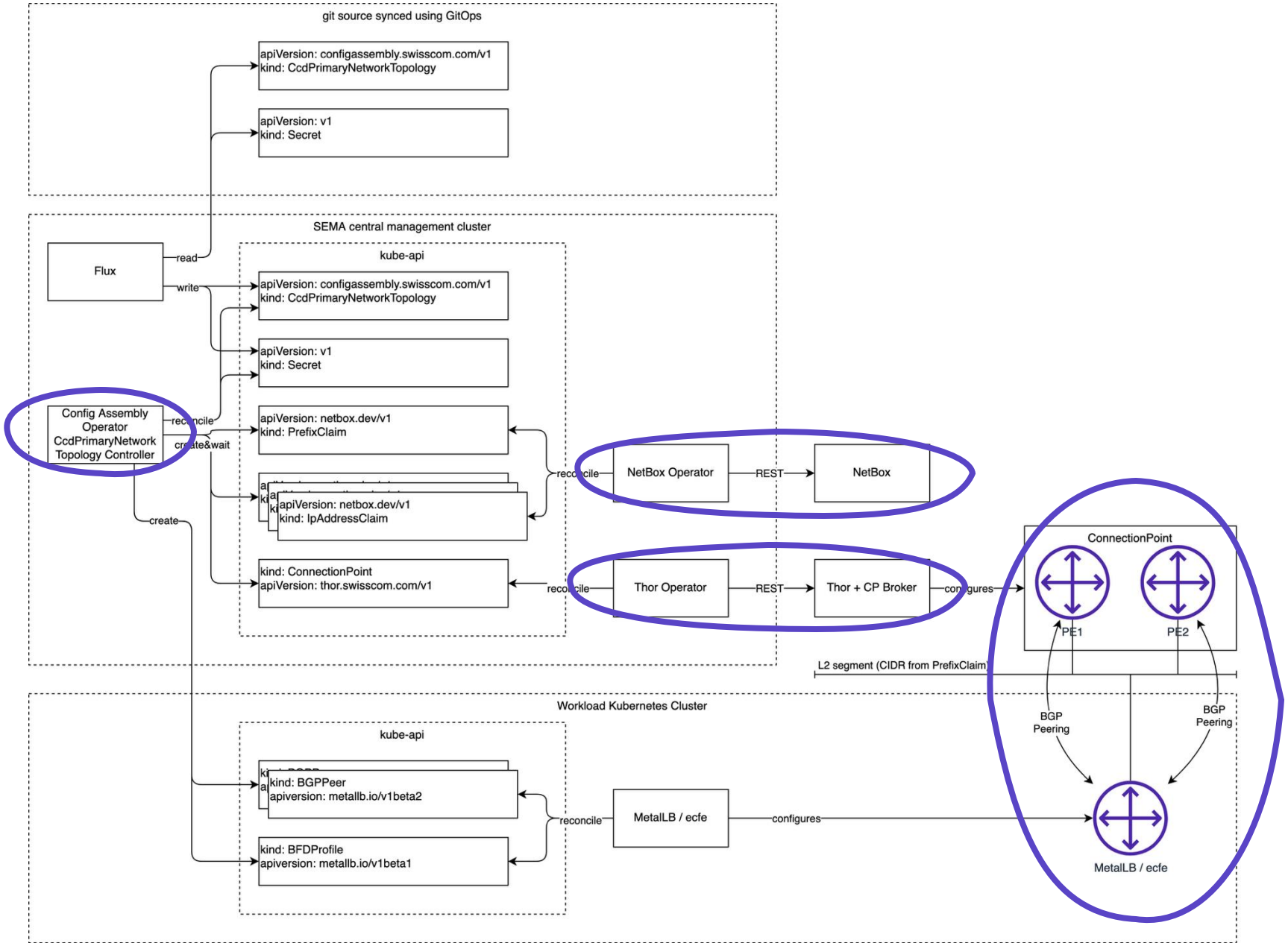
NetBox Operator, a tool designed to integrate NetBox resource management – for IPAM, DCIM and more – directly into your Kubernetes environment.

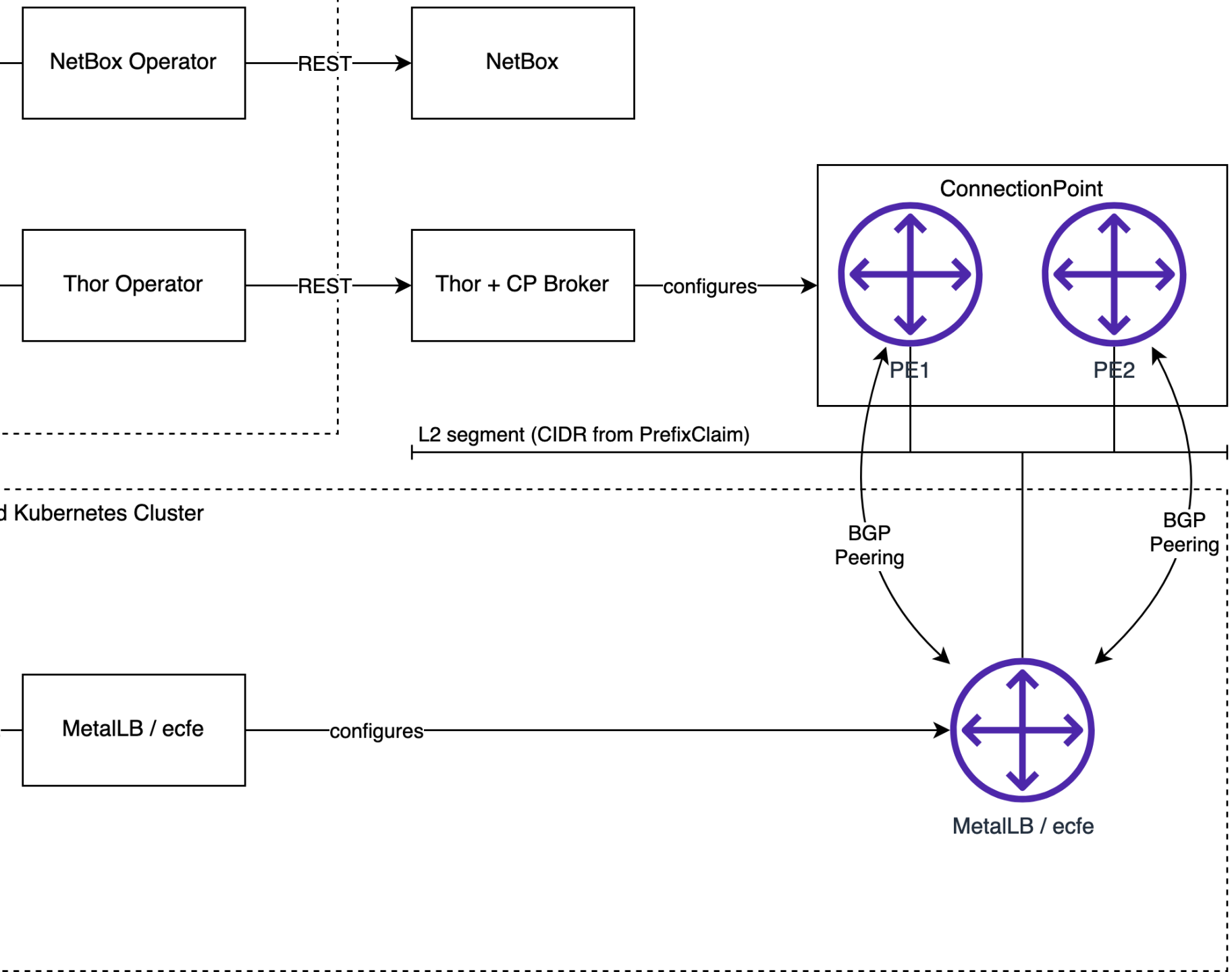




https://github.com/netbox-community/netbox-operator
CNCF Blog Post

# Config Assembly Operator CcdPrimaryNetworkTopology Controller Context

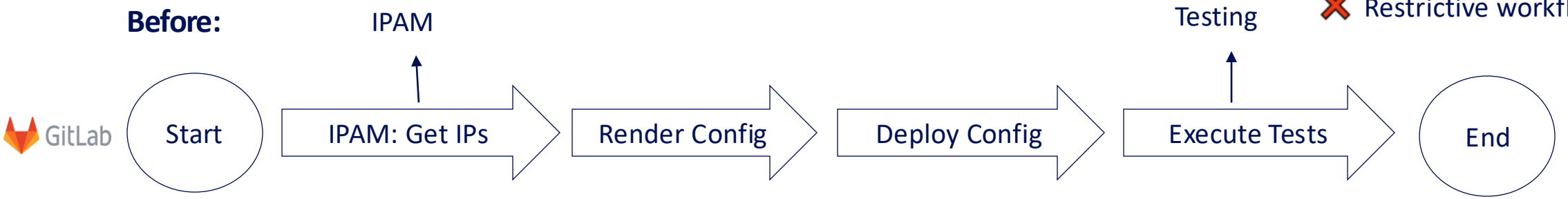



NetBox Operator
REST
NetBox
Thor Operator
REST
Thor + CP Broker
configures
ConnectionPoint
PE1
PE2
L2 segment (CIDR from PrefixClaim)
d Kubernetes Cluster
BGP
Peering
BGP
Peering
MetalLB / ecfe
configures
MetalLB / ecfe

# From the production pipeline to the conditional dance

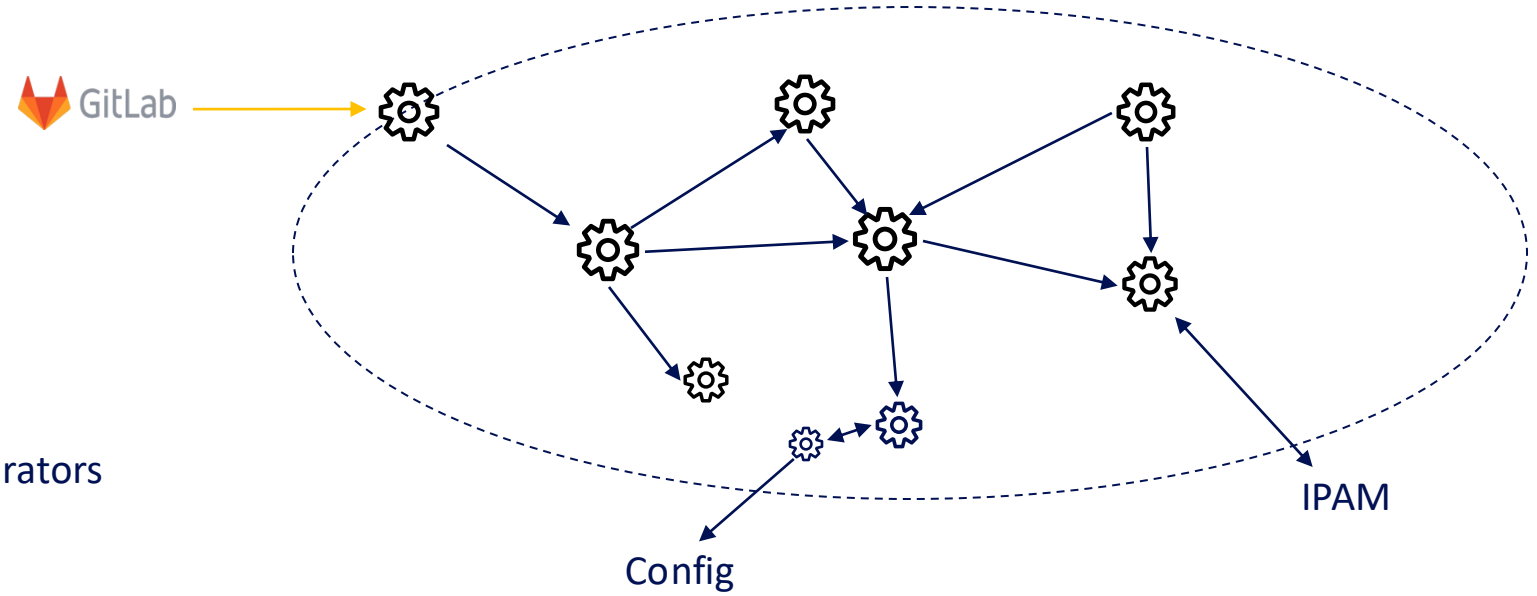
- ✗ No Reconciliation
- ✗ Fire and forget
- ✗ No standard interfaces
- ✗ Restrictive workflow

**Before:**




**Now:**

- ✓ Constant Reconciliation
- ✓ Standard interfaces
- ✓ Complex workflows possible




Operators

# Kubernetes Operators

# Kubernetes Operators: Why?

**K8s is well Established**

Kubernetes is broadly adopted and Know-How is growing globally.

**Reconcile Loop**

Self-healing by design.

**Community**

Kubebuilder has a vivid community.

# Kubernetes Resource Model (KRM)

**API extensions**

Custom Resource Definitions extend the Kubernetes API.

e.g. API definition for NetBox PrefixClaim

**CRs as Instances**

Custom Resources instantiate a CRD.

e.g. NetBox PrefixClaim resource

**Business Logic**

Use of Operators or templates to run custom logic

e.g. Assemble a config, Self healing