

PoC 16 on “Automation across multi-site and multi-stakeholder environments”



PoC Presenters: Georgios P. Katsikas,

Kostis Trantzas,

Lluís Gifre Renom,

Dimitrios Triantafyllou



ETSI ISG ZSM PoC 16 demonstration



Online webinar



November 14, 2025

10:00 – 12:00 CET

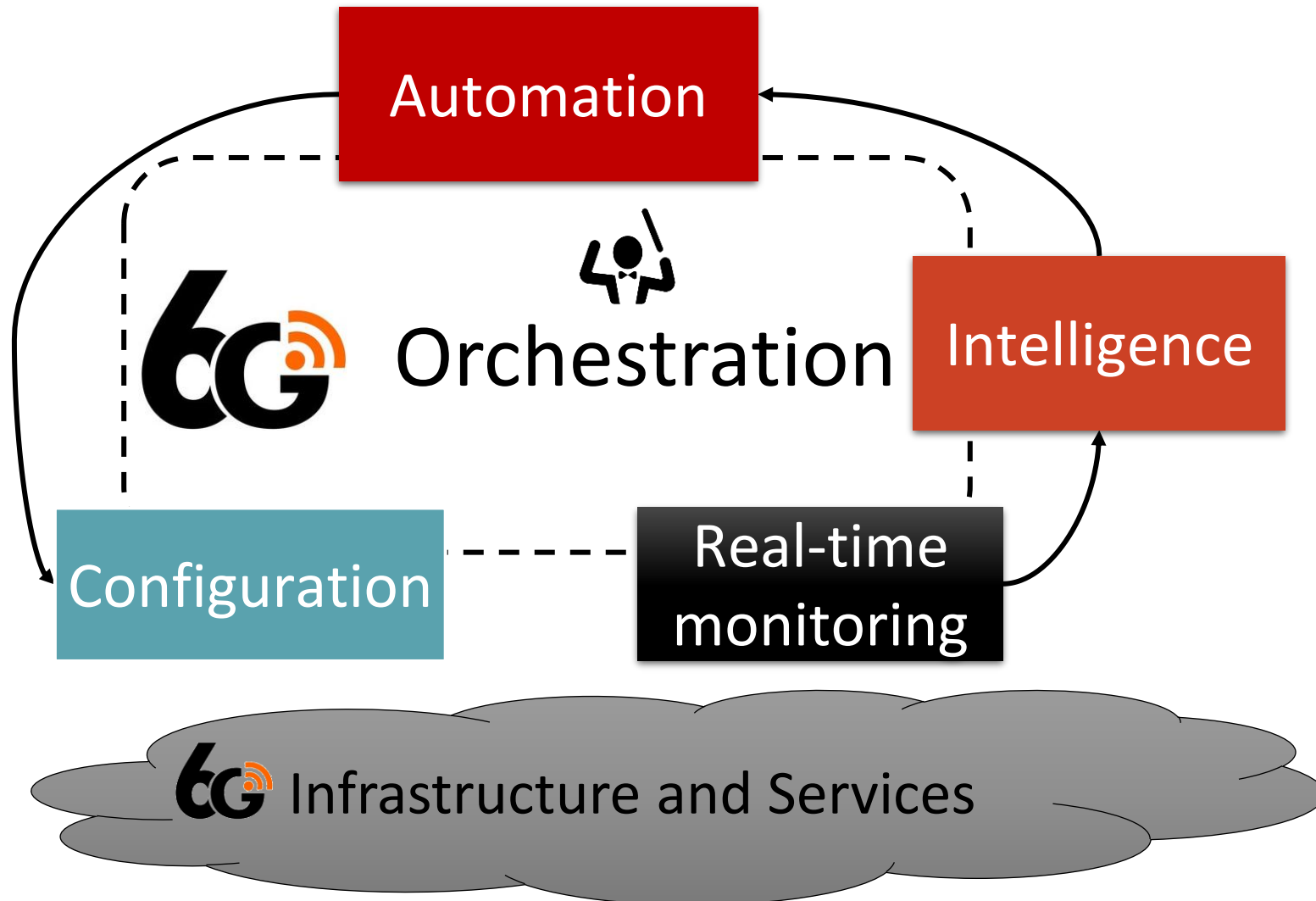


PoC Contributors:

UBI, UOP, PNET, NOVA, K3Y, CTTC, WINGS, LMI, TID, UPM

Introduction

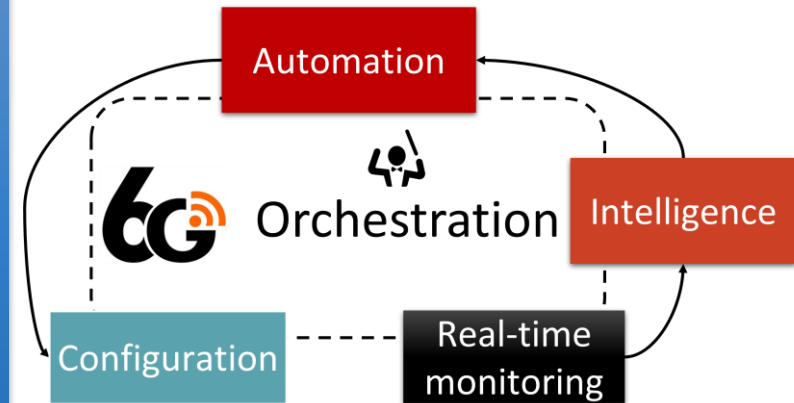
Introduction



PoC Objective

PoC Objective

Demonstrate a 6G-ready orchestration use case across multiple administrative domains with minimal manual configuration, emphasizing on:



Platform
Lifecycle



Expansion of the infrastructure to a new **private** domain



Service
Lifecycle

Dynamic service provisioning over **on-demand** compute and network resources

End-to-end (multi-domain) **SLA-driven service management**

PoC Infrastructure



Domain A
Athens, GR

PoC Domains' Locations

Domain B
Patra, GR



UNIVERSITY OF
PATRAS
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

Domain C
Madrid, ES



End-to-end service management

+

Zero-trust connectivity fabric

Domain A
Athens, GR

PoC Domains'
Roles

Domain B
Patra, GR

Domain C
Madrid, ES



End-to-end service management

+

Zero-trust connectivity fabric

Domain A
Athens, GR

PoC Domains'
Roles

Domain C
Madrid, ES

Domain B
Patra, GR

Network planning

End-to-end service management

+

Zero-trust connectivity fabric

Domain A
Athens, GR

PoC Domains' Roles

Domain C
Madrid, ES

Domain B
Patra, GR

**Private edge infrastructure
and end users**

Network planning

PoC Setup

PoC Setup – Initial testbeds' state



Outline the state of the platform before the PoC

Domain A serves as the central domain for the platform

Domain C is used by the platform for offline network planning



Let's see what components are deployed in advance, where, and why?

**Cloud
infrastructure**



Compute

Domain A
Athens, GR

**PoC Domains'
Capabilities**

Domain B
Patra, GR



Users

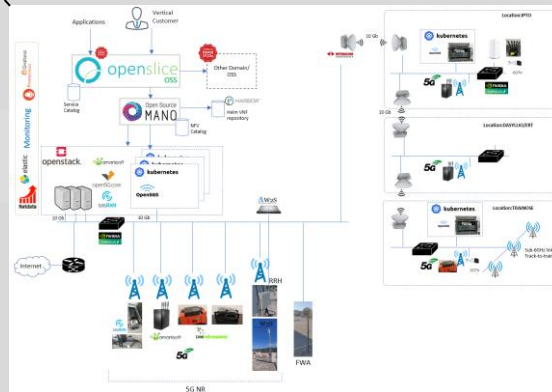


Network



Compute

**Patras 5G
Testbed**



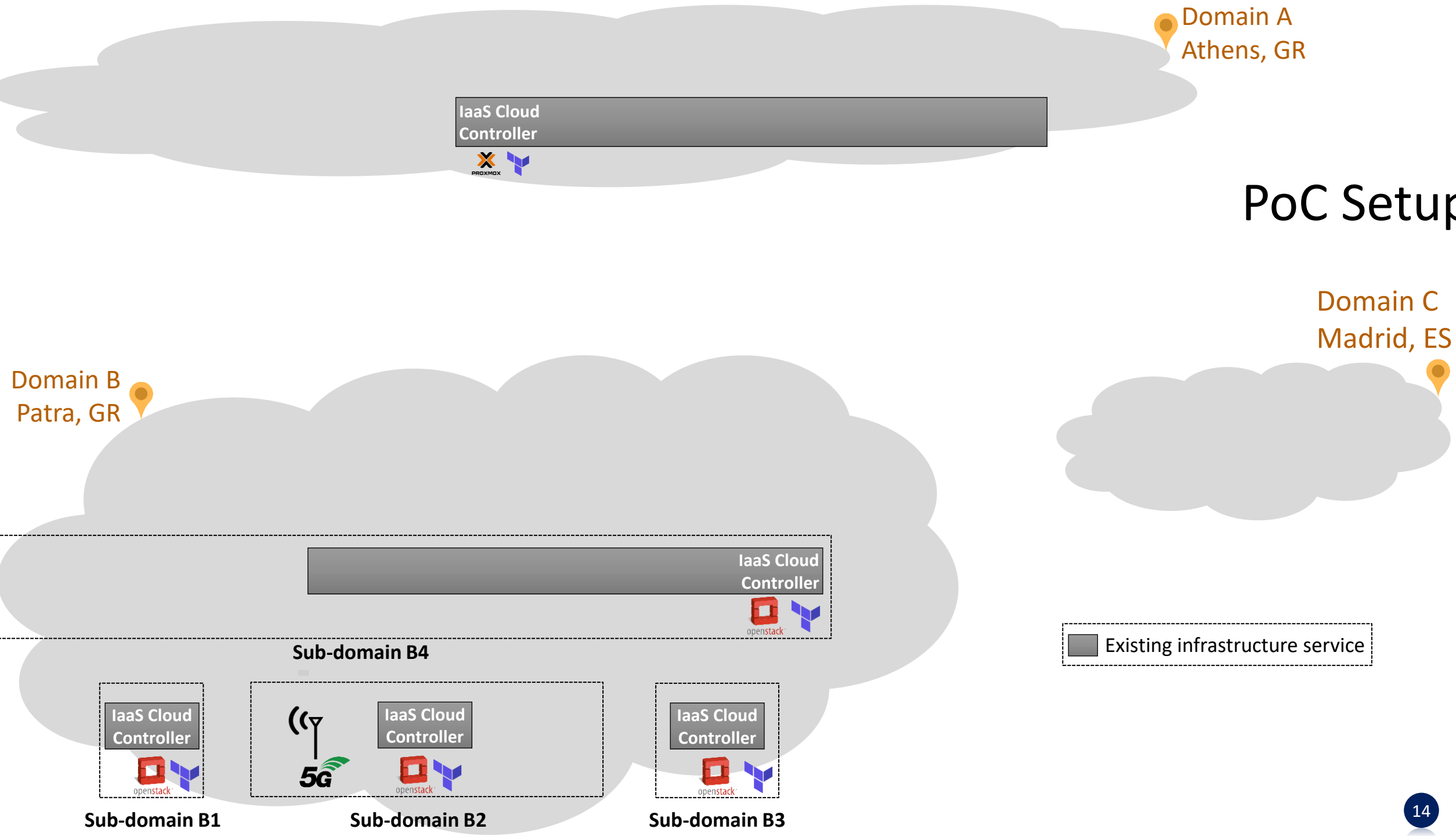
Domain C
Madrid, ES



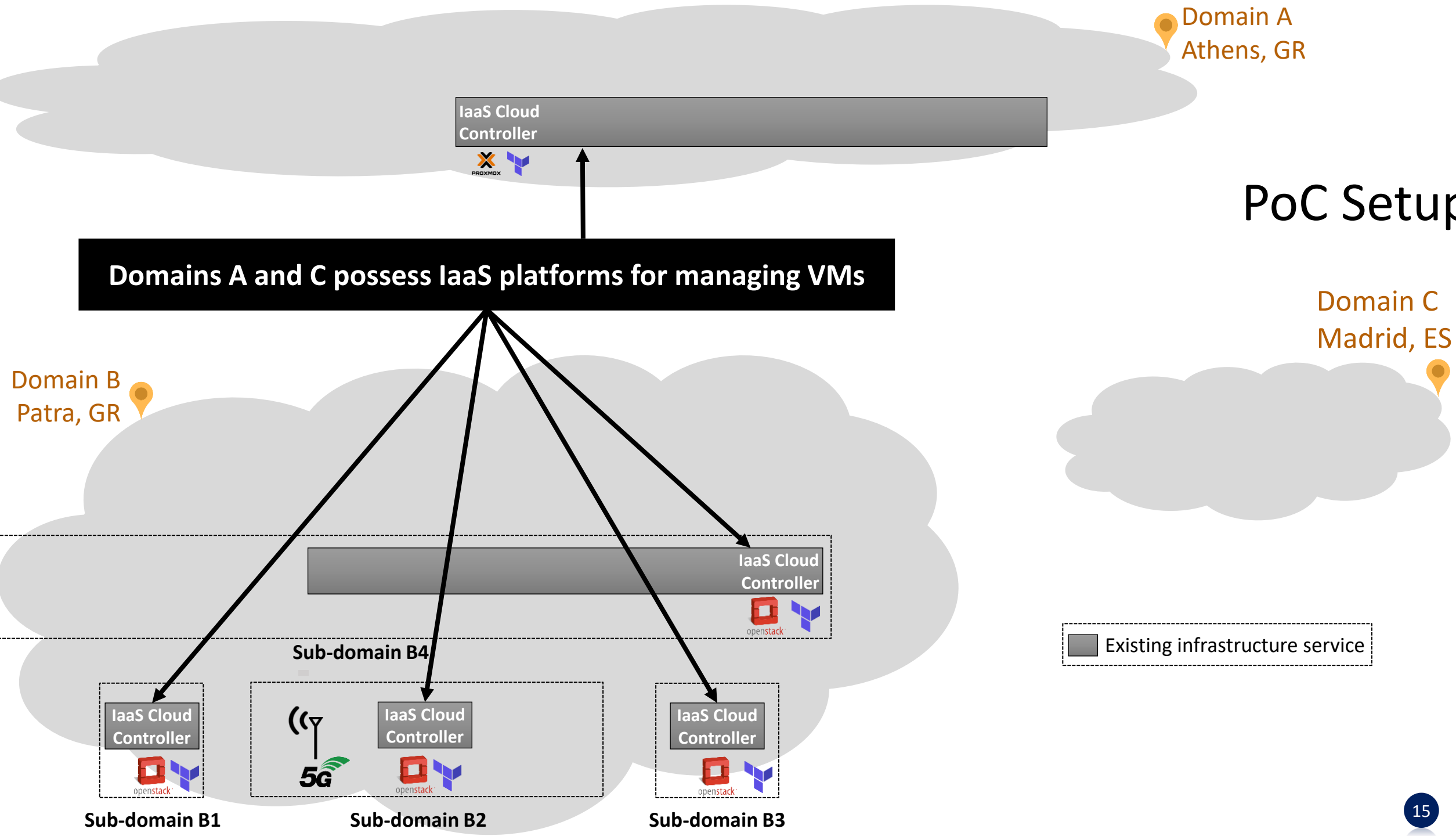
Compute

**Cloud
infrastructure**

PoC Setup



PoC Setup



Domain A
Athens, GR

IaaS Cloud
Controller

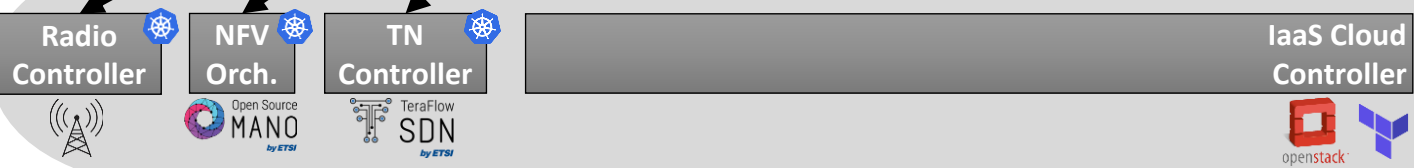


PoC Setup

Radio, transport, and NFV controllers are in place in Domain C

Domain B
Patra, GR

Domain C
Madrid, ES



Sub-domain B4

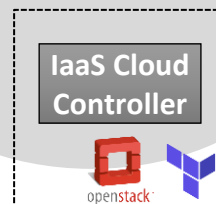
Existing infrastructure service



Sub-domain B1



Sub-domain B2



Sub-domain B3

Domain Orchestrator #1



IaaS Cloud Controller



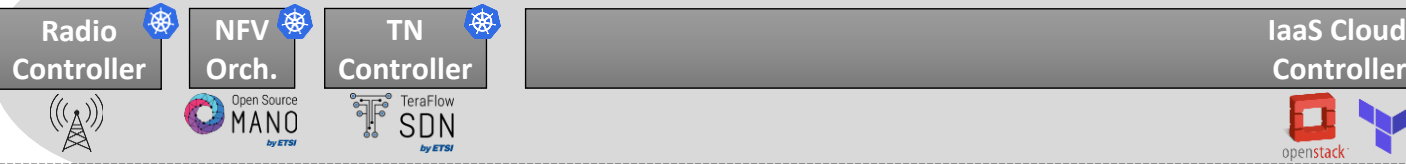
Manages compute and network resources within Domain A
Offers resource-as-a-service via standardized APIs

Domain A
Athens, GR

PoC Setup

Domain B
Patra, GR

Domain C
Madrid, ES



Sub-domain B4

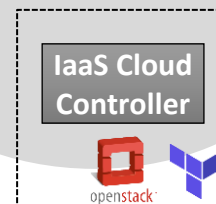
ACROSS service
Existing infrastructure service



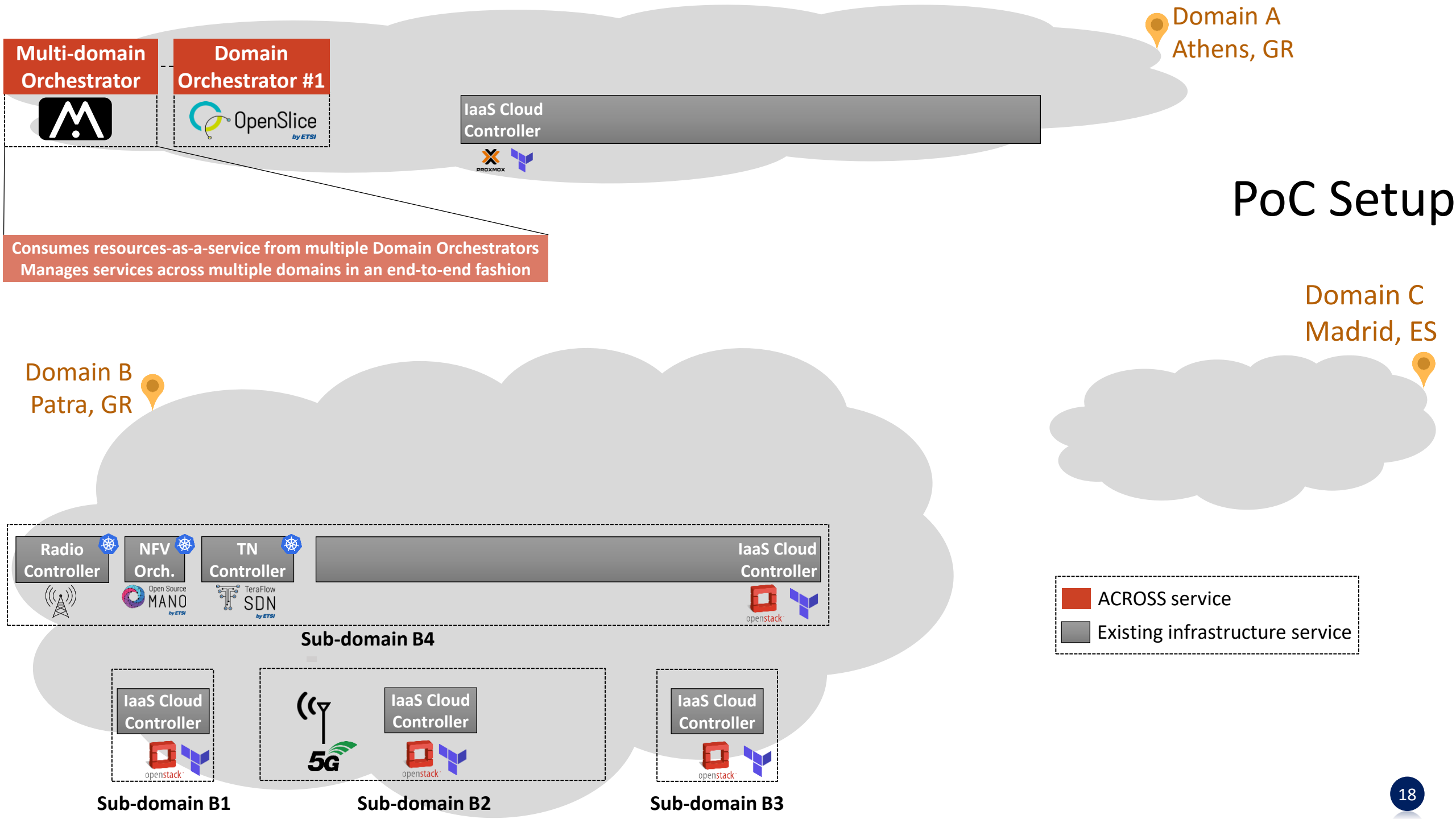
Sub-domain B1

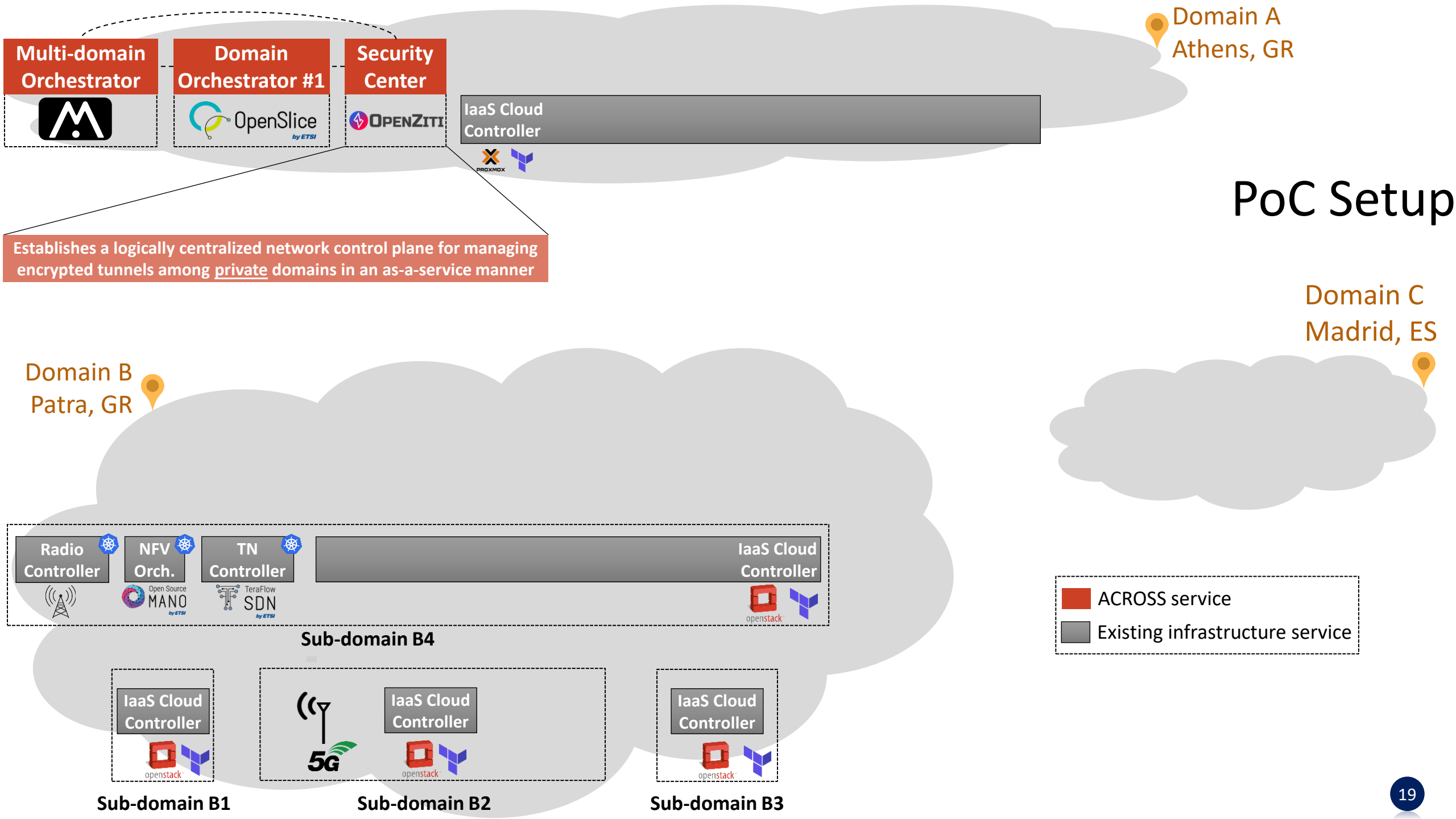


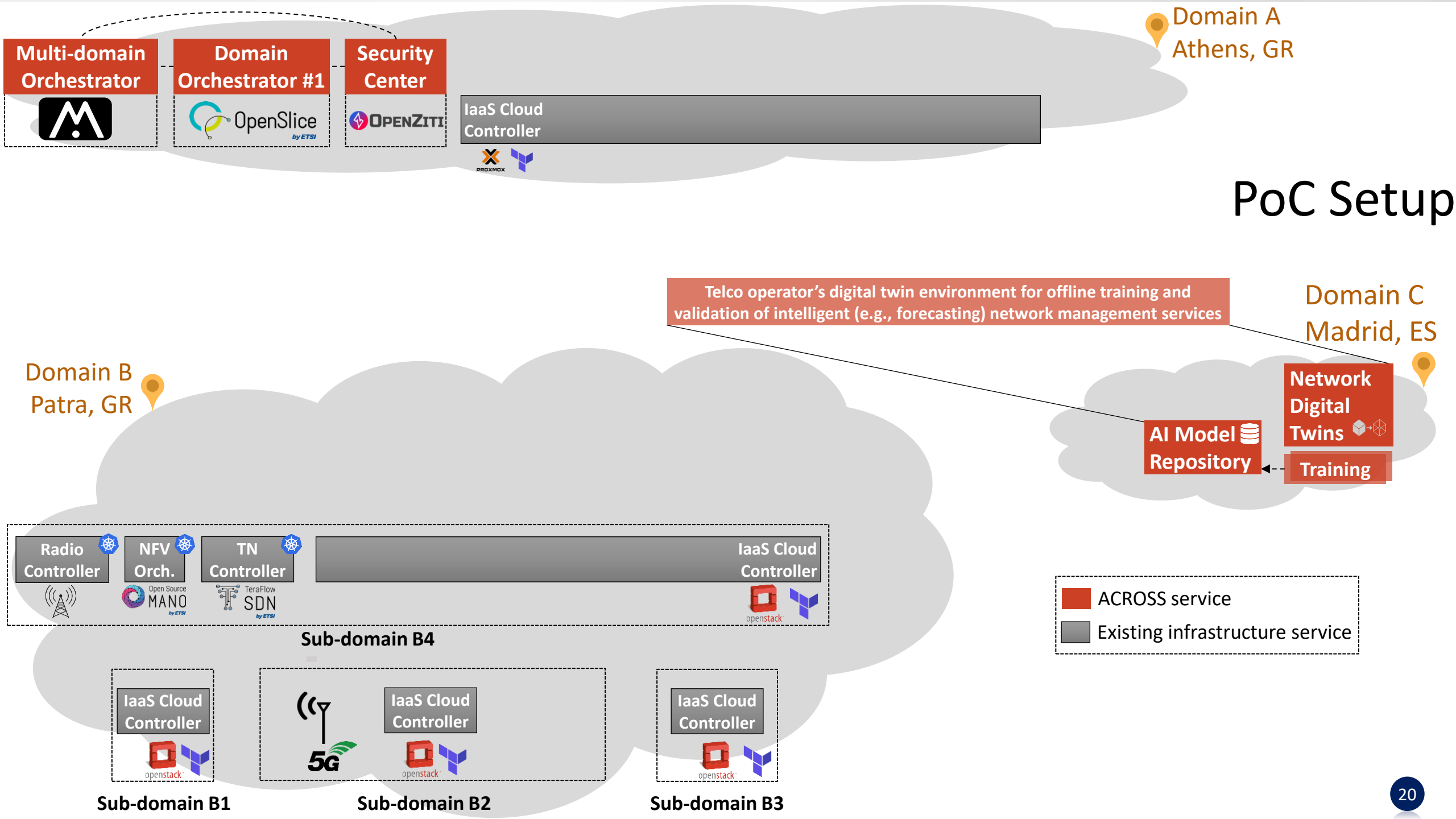
Sub-domain B2



Sub-domain B3







PoC Setup – Remarks

Explain the basic environment before starting the PoC

- Domain A is equipped with orchestrators and the network fabric to connect to other domains
- Domain C has the necessary NDT services for network planning purposes
- Domain B is not yet associated with the platform (non-orchestrated), but contains the necessary infrastructure services to do so

PoC Stories – Scenario #1



Scenario #1 Presenter

UBIT²CH
ubiquitous solutions



Georgios P. Katsikas

ACROSS + COP-PILOT

Technical Coordinator

ETSI OSL/TFS TSC Member

PoC Scenario #1 – Platform expansion to private domain



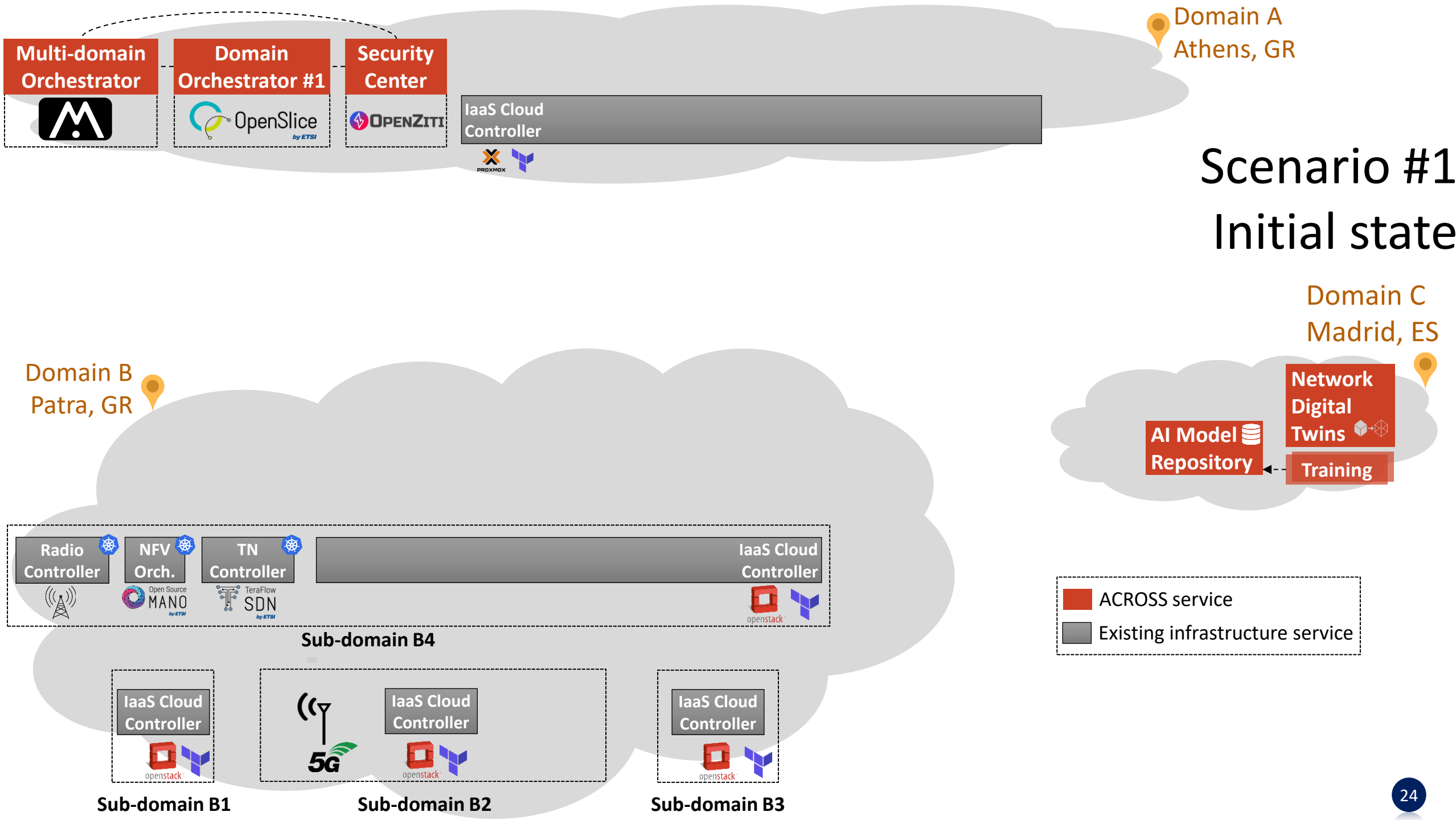
The owner of a new private edge domain (domain B) wants to add this domain under the platform's realm

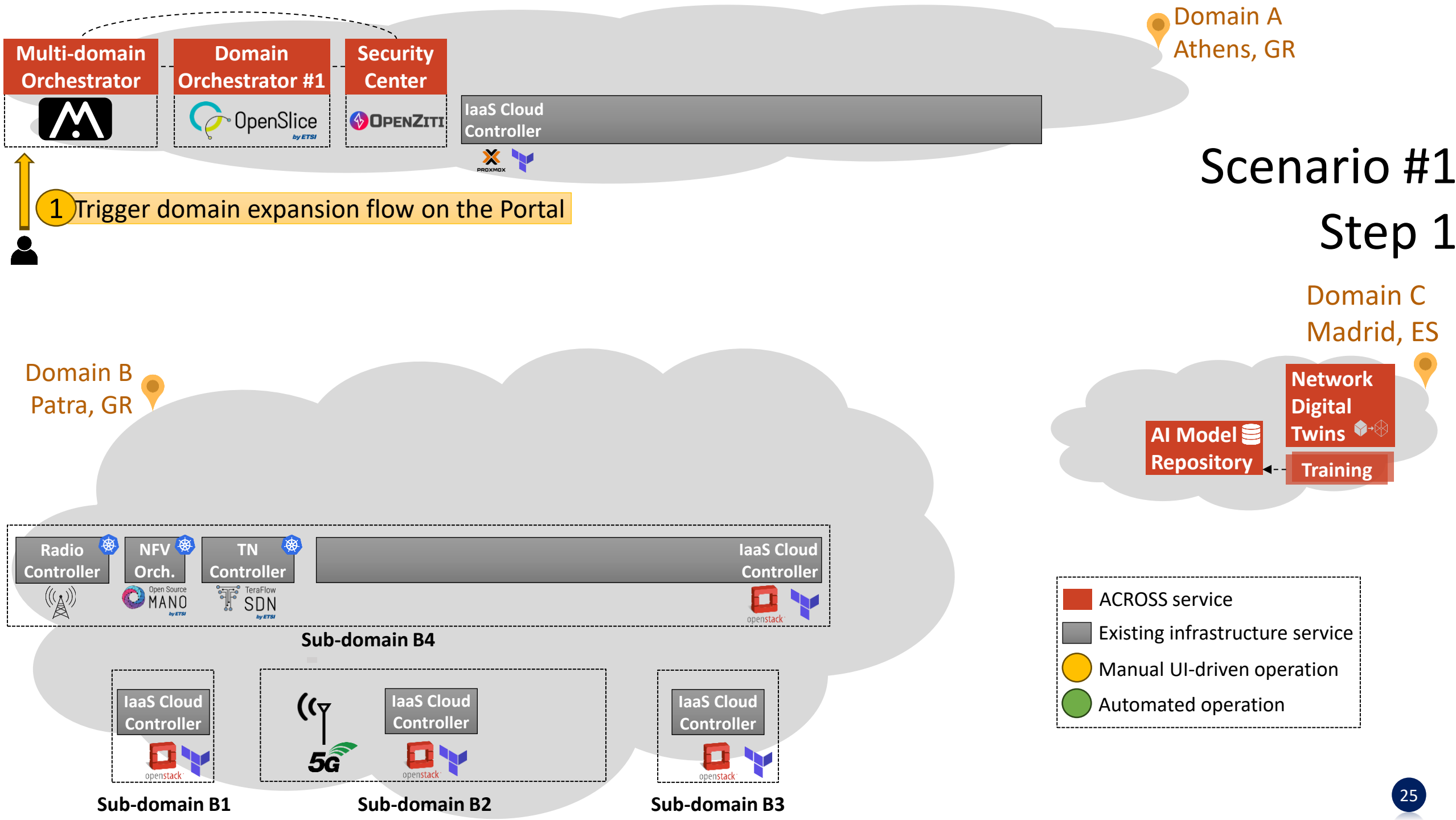


The platform should greatly-facilitate this process without compromising security and trust



The scenario unfolds a UI-driven flow which automates most of the required operations for secure expansion of the platform in Domain B





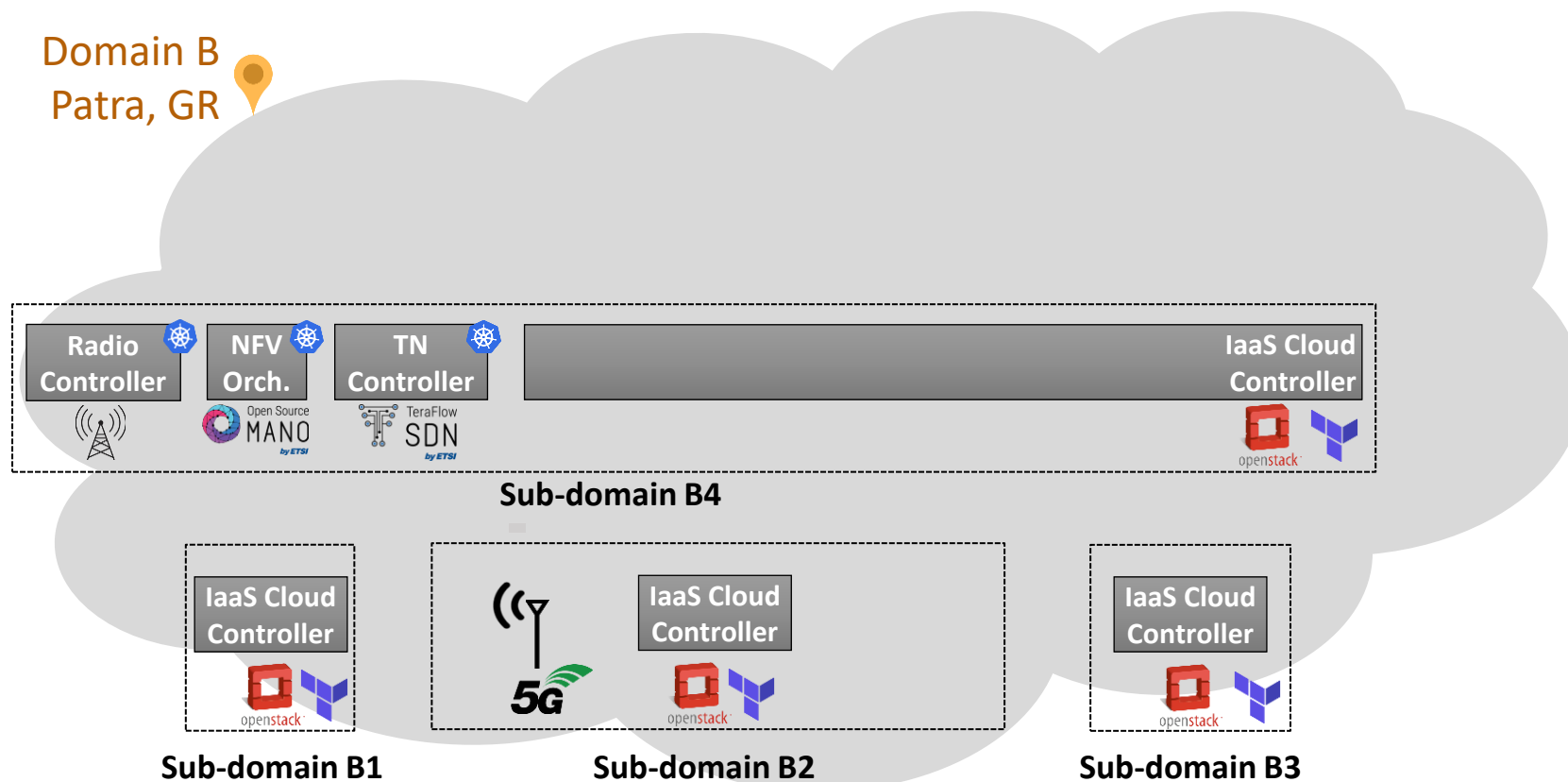


Scenario #1

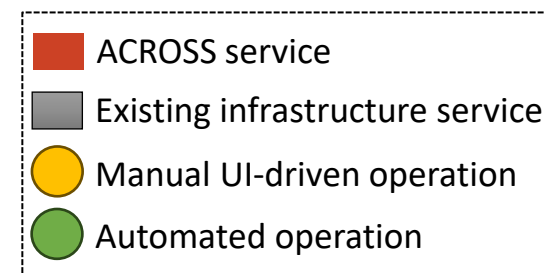
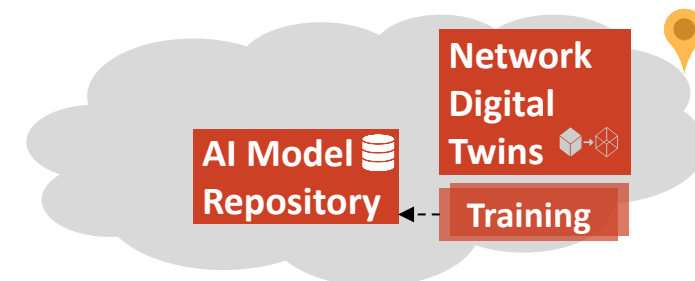
Step 2

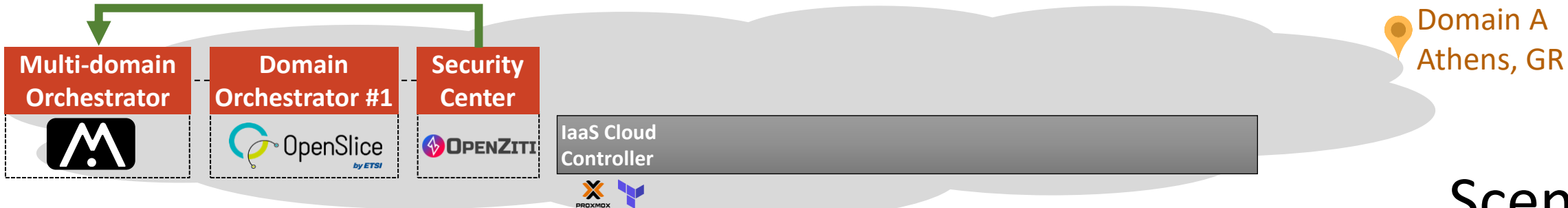
2 Request new domain identity (ZWT token) for domain owner

Domain B
Patra, GR



Domain C
Madrid, ES



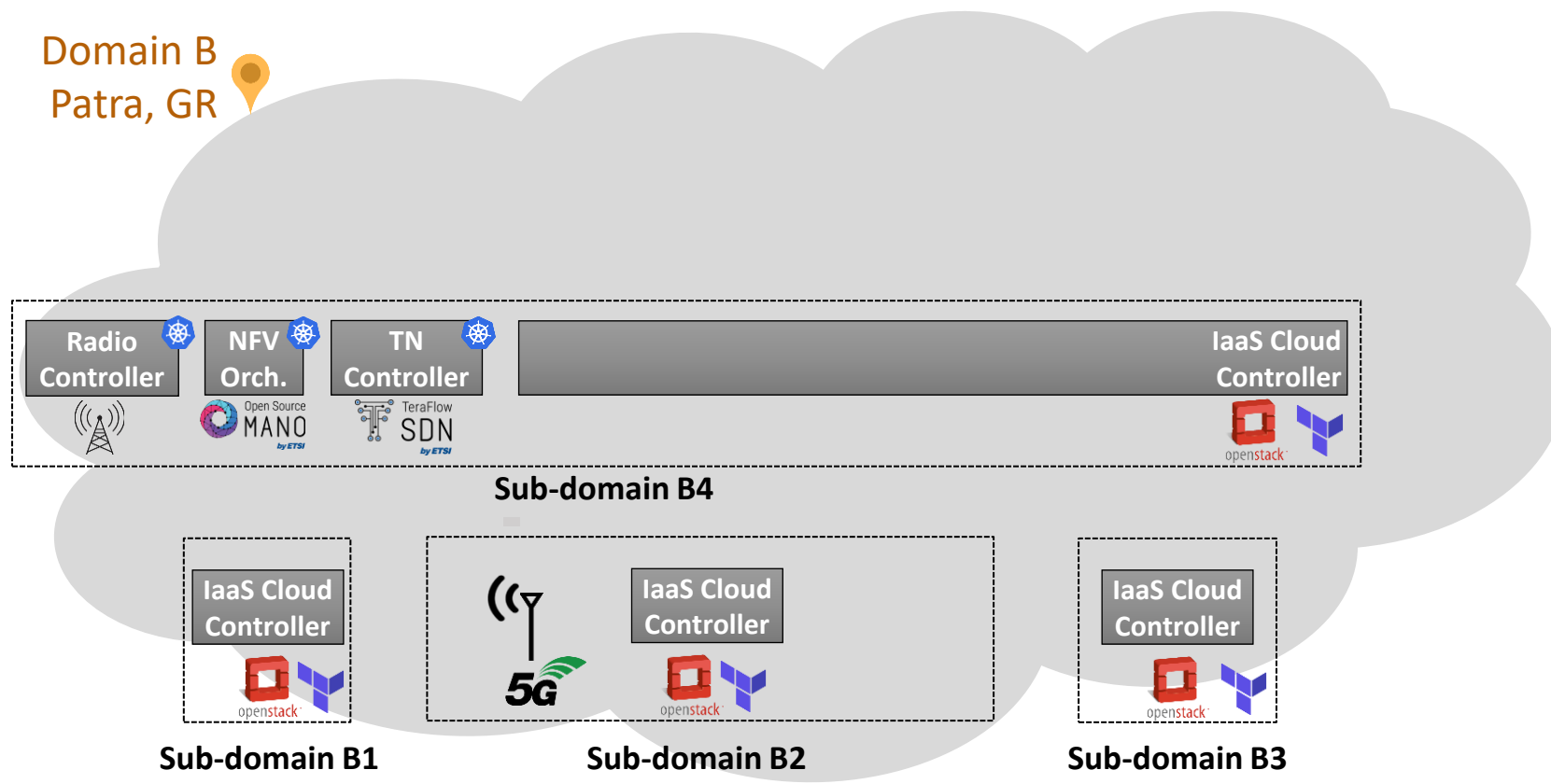


Scenario #1

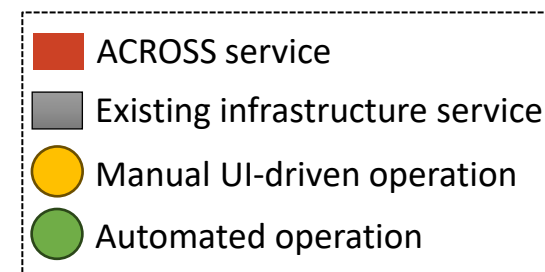
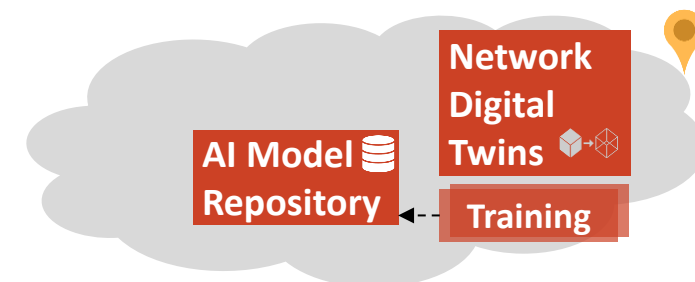
Step 3

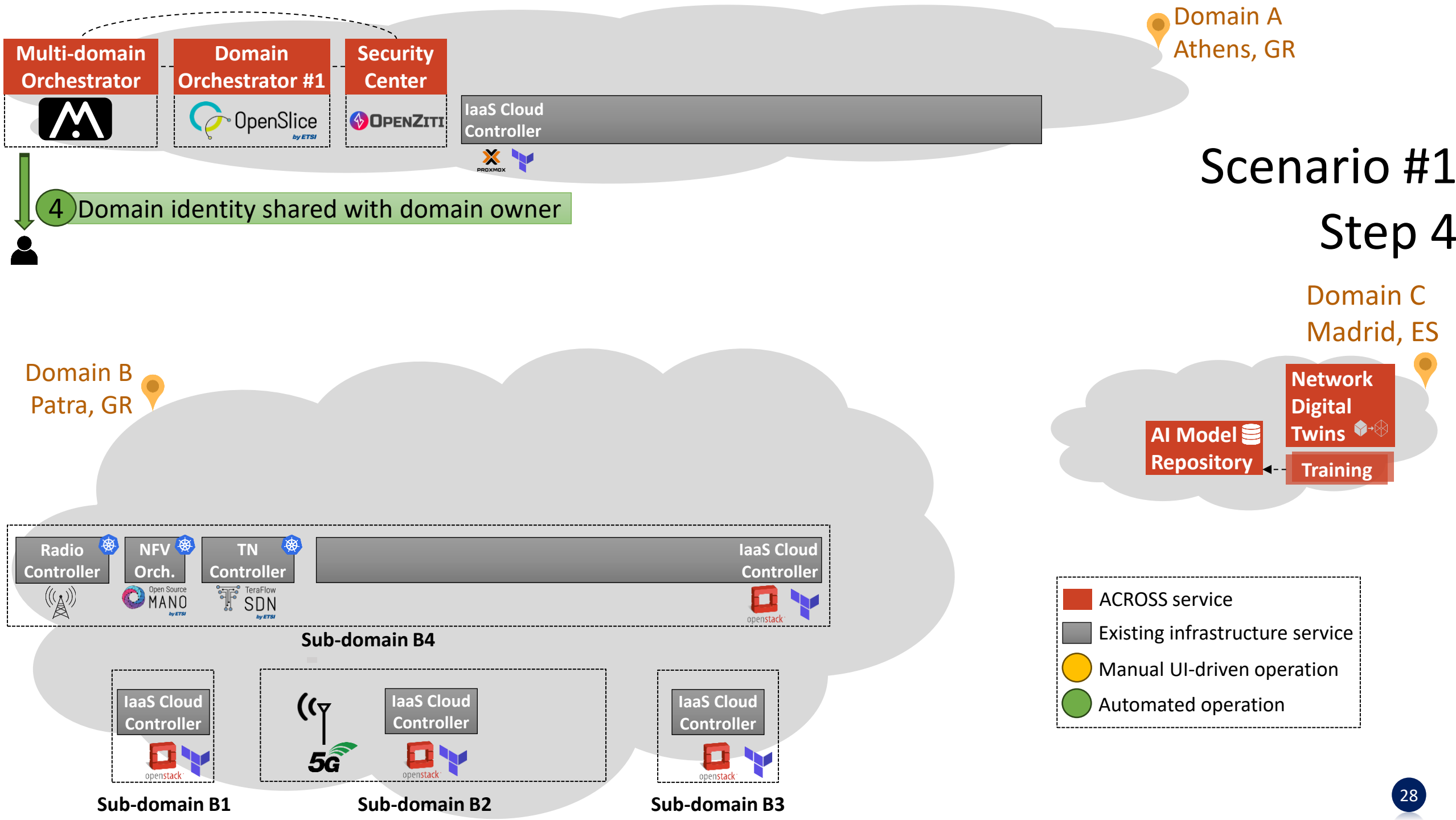
3 Domain identity (ZWT token) created and returned

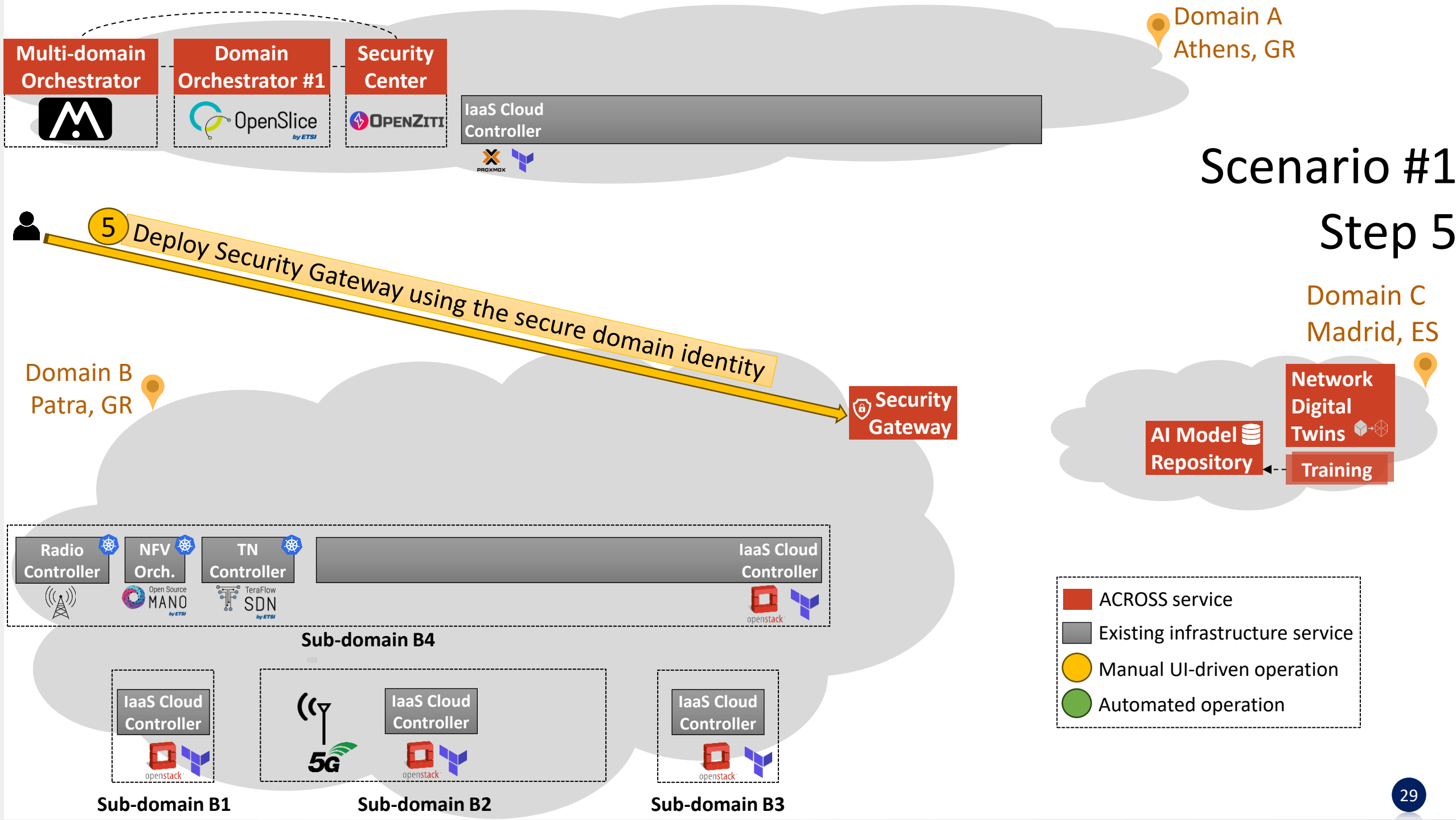
Domain B
Patra, GR

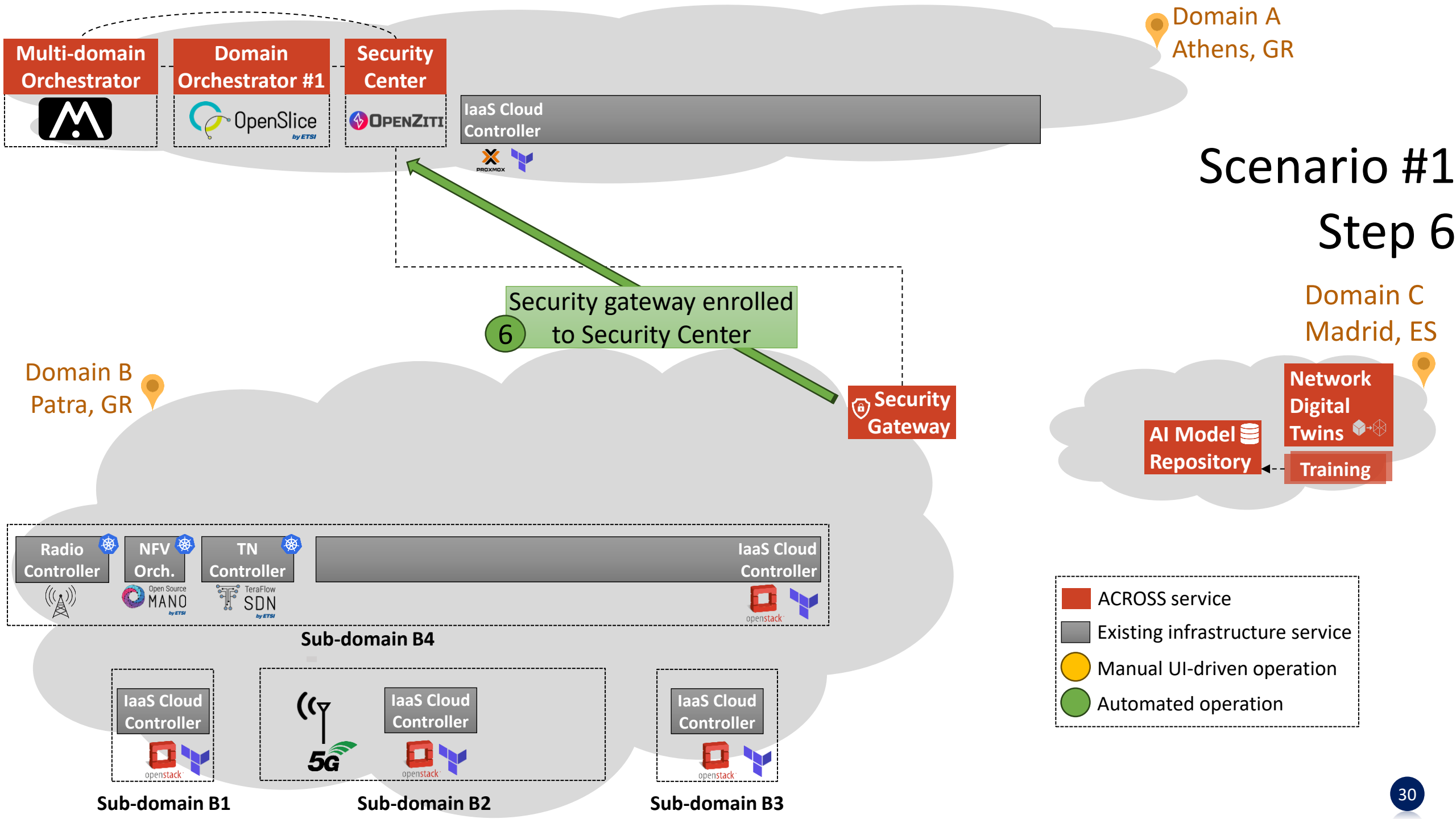


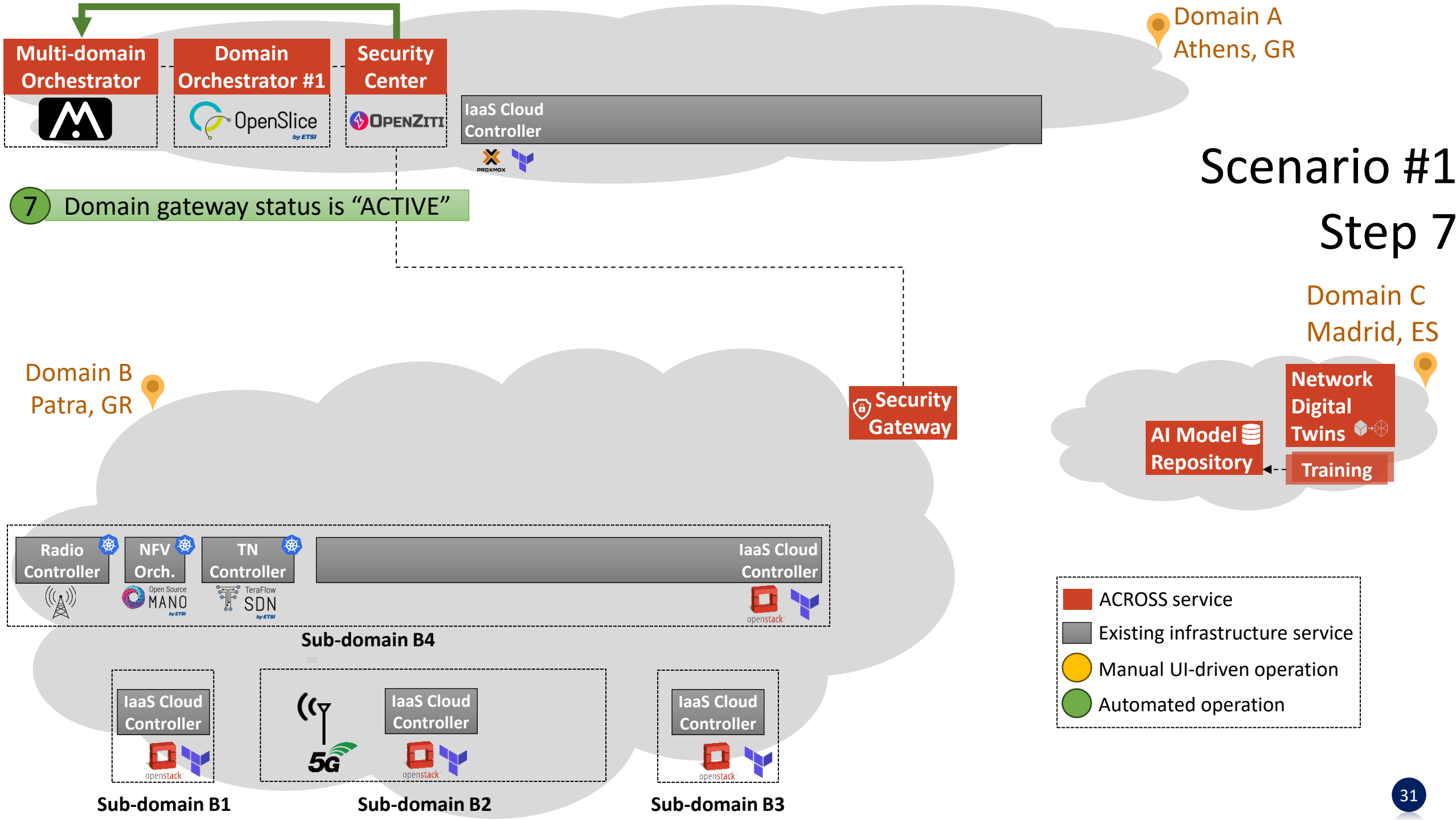
Domain C
Madrid, ES

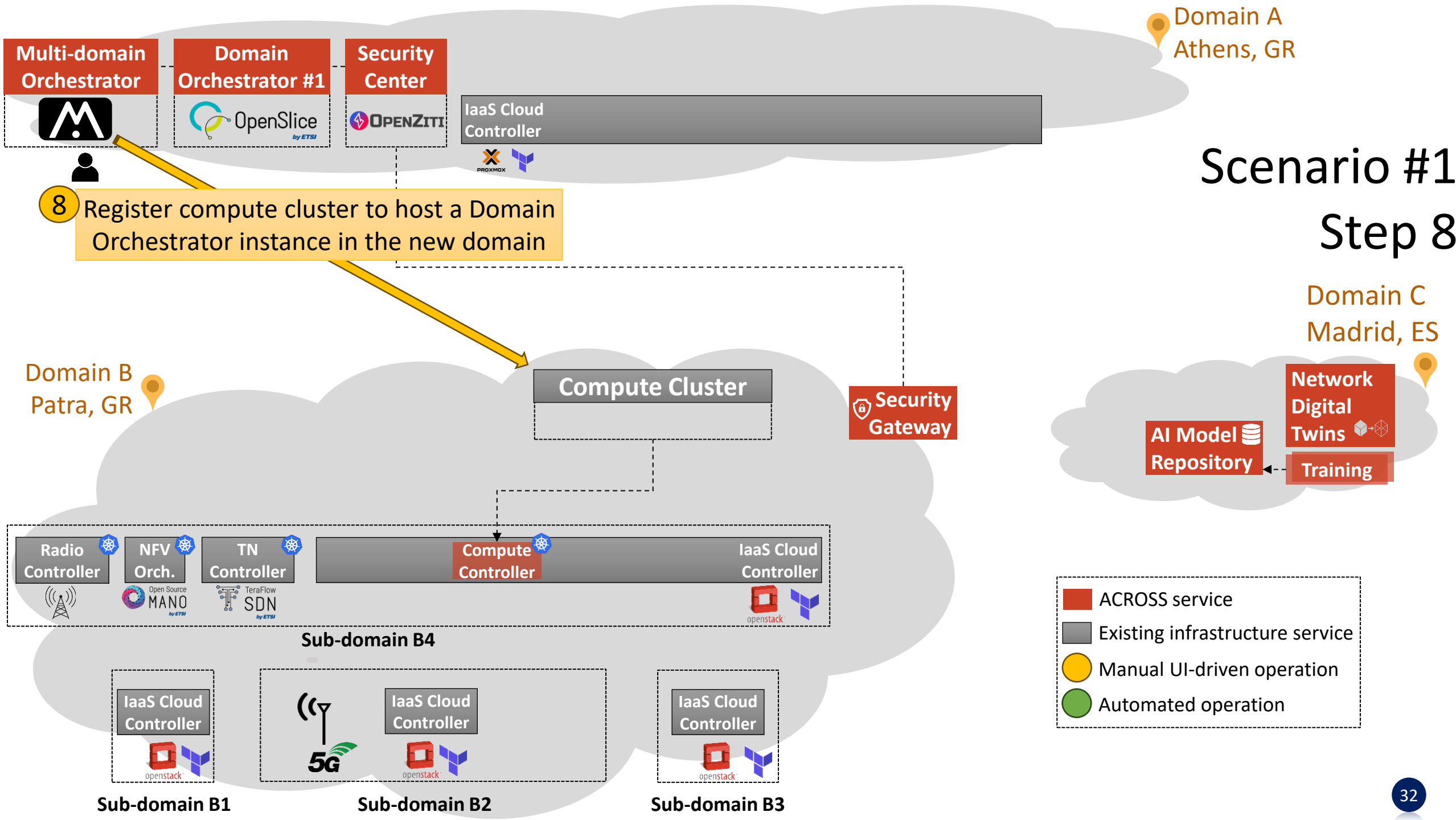


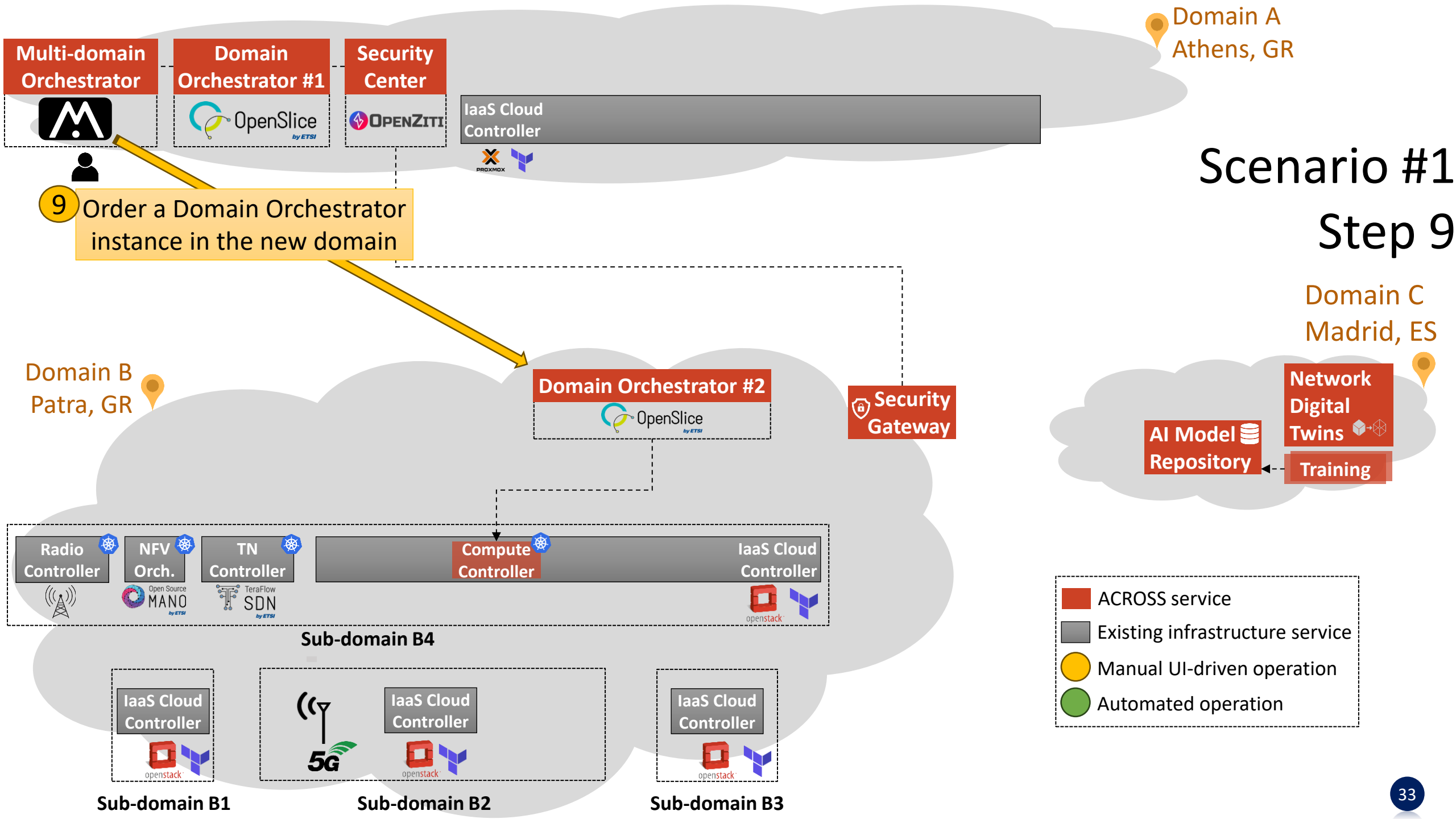


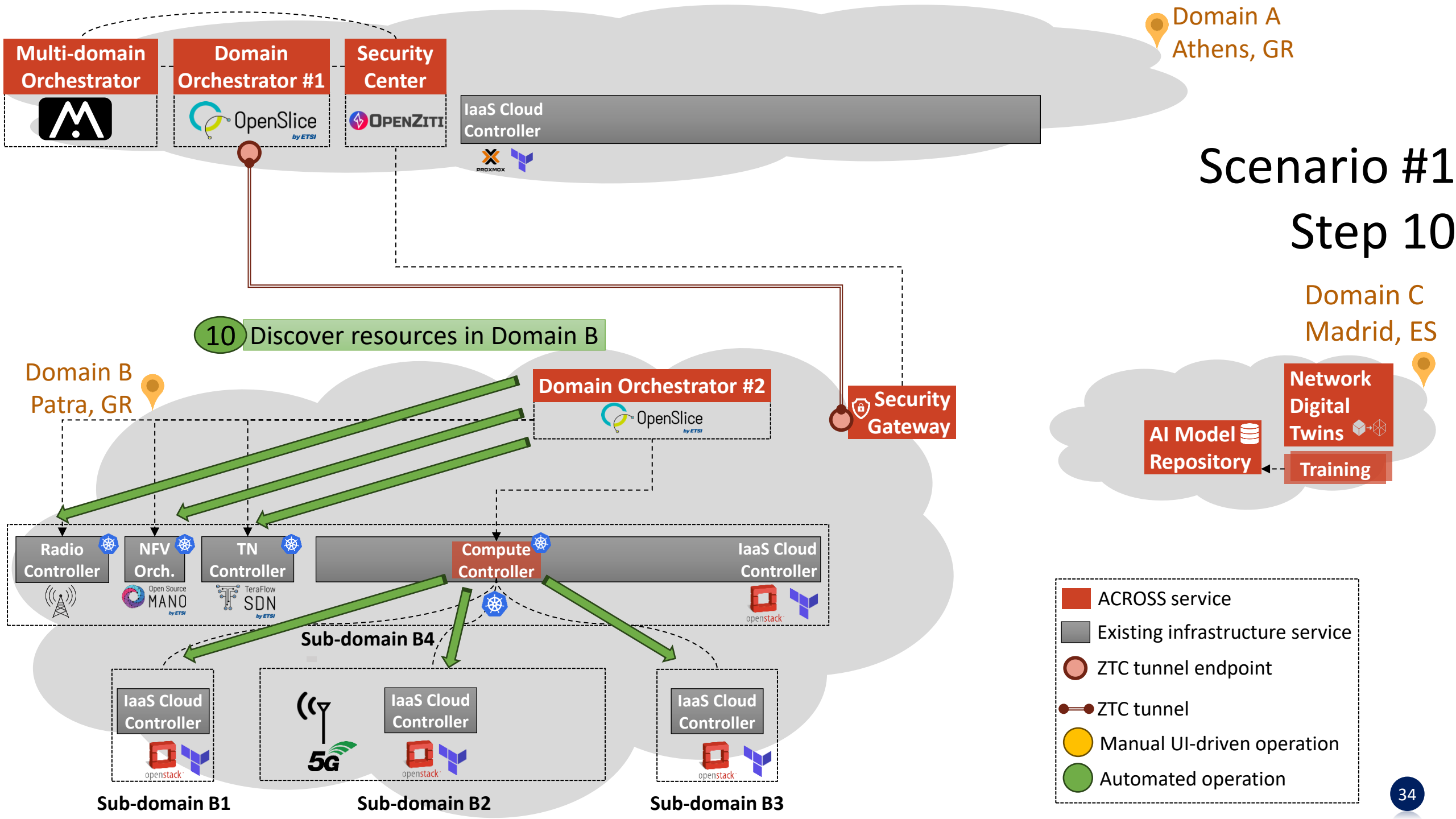


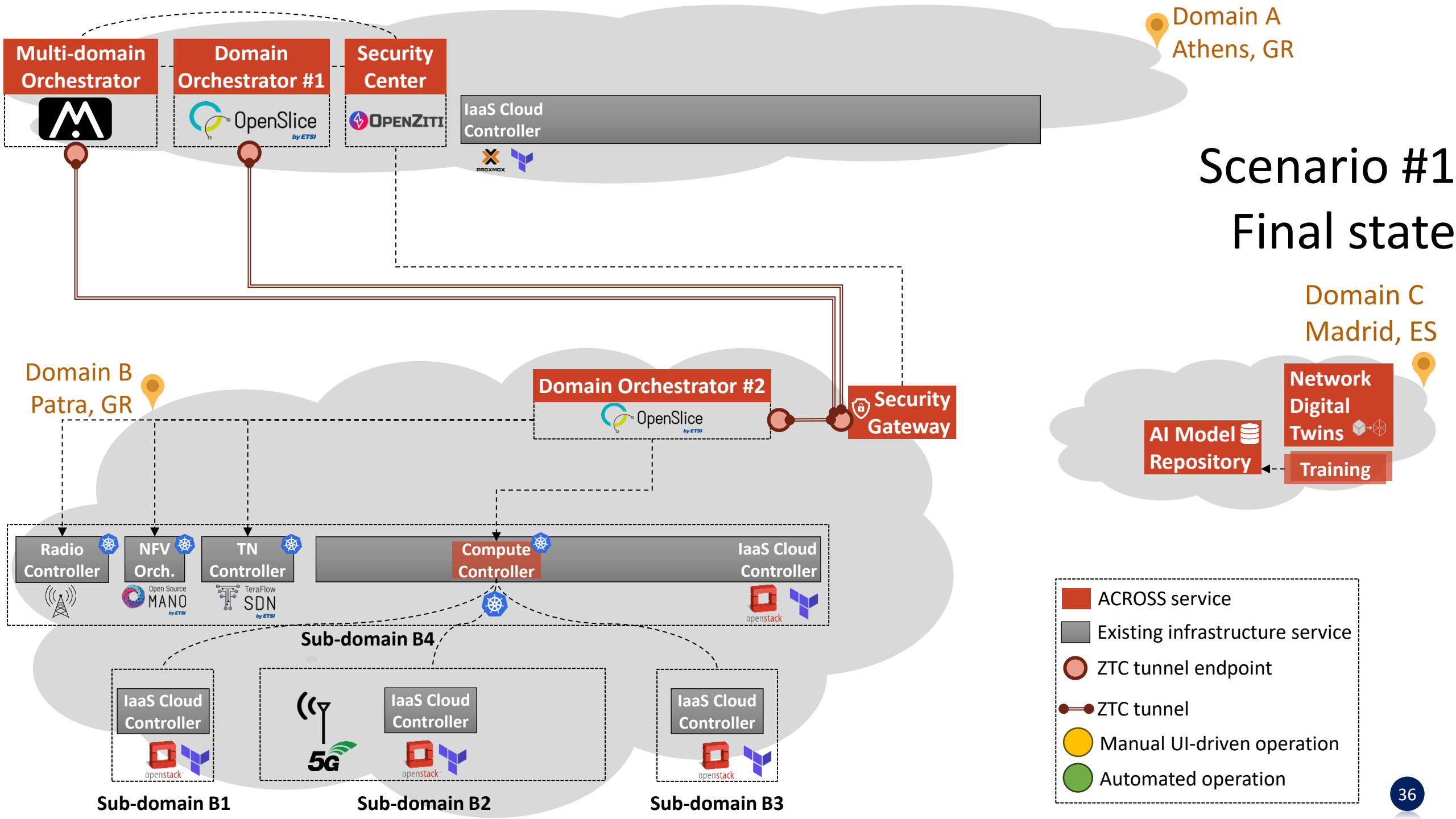




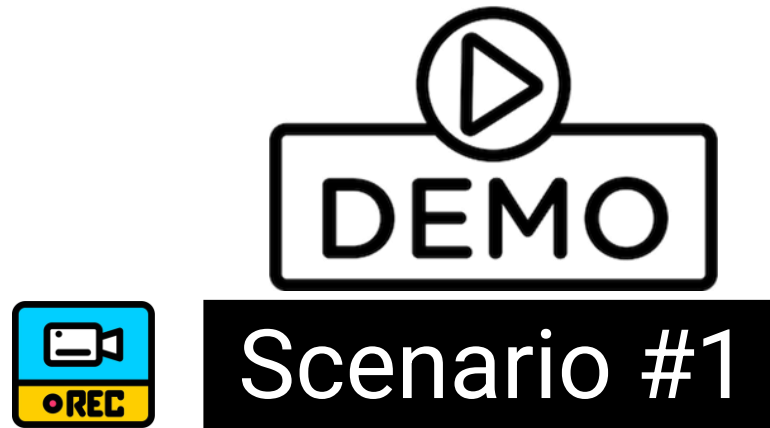








PoC Scenario #1 – Demo time

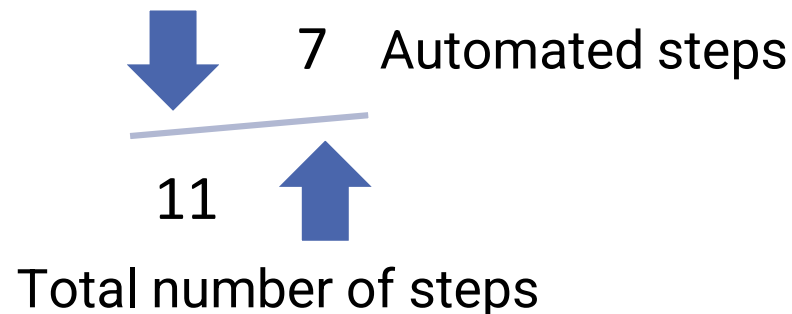


PoC Scenario #1 – Remarks (1/2)

East-West expansion of the platform to a new private domain (Domain B)

- Domain B is now orchestrated by a new DO#2 instance (East-West expansion of the DO)
- Domain B's local orchestrator (DO#2) has automatically discovered the underlying resources
- Domain B's local orchestrator (DO#2) is accessible by the MDO

Amount of Automation ≈ 64%



PoC Scenario #1 – Remarks (2/2)

Even the non-automated steps (yellow highlighted) are greatly facilitated by the portal

➡ Only minimum user intervention is required

Amount of Automation > 90% is possible if we sacrifice security (not recommended)

➡ Allow MDO to auto-deploy the Security Gateway on a pre-defined IP:port in Domain B

➡ This is nearly impossible in the real world as no domain administrator would allow this

PoC Stories – Scenario #2



Scenario #2 Presenter



Kostis Trantzas

ETSI OSL TSC Chair



UNIVERSITY OF
PATRAS
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

PoC Scenario #2 – Automated Service Provisioning



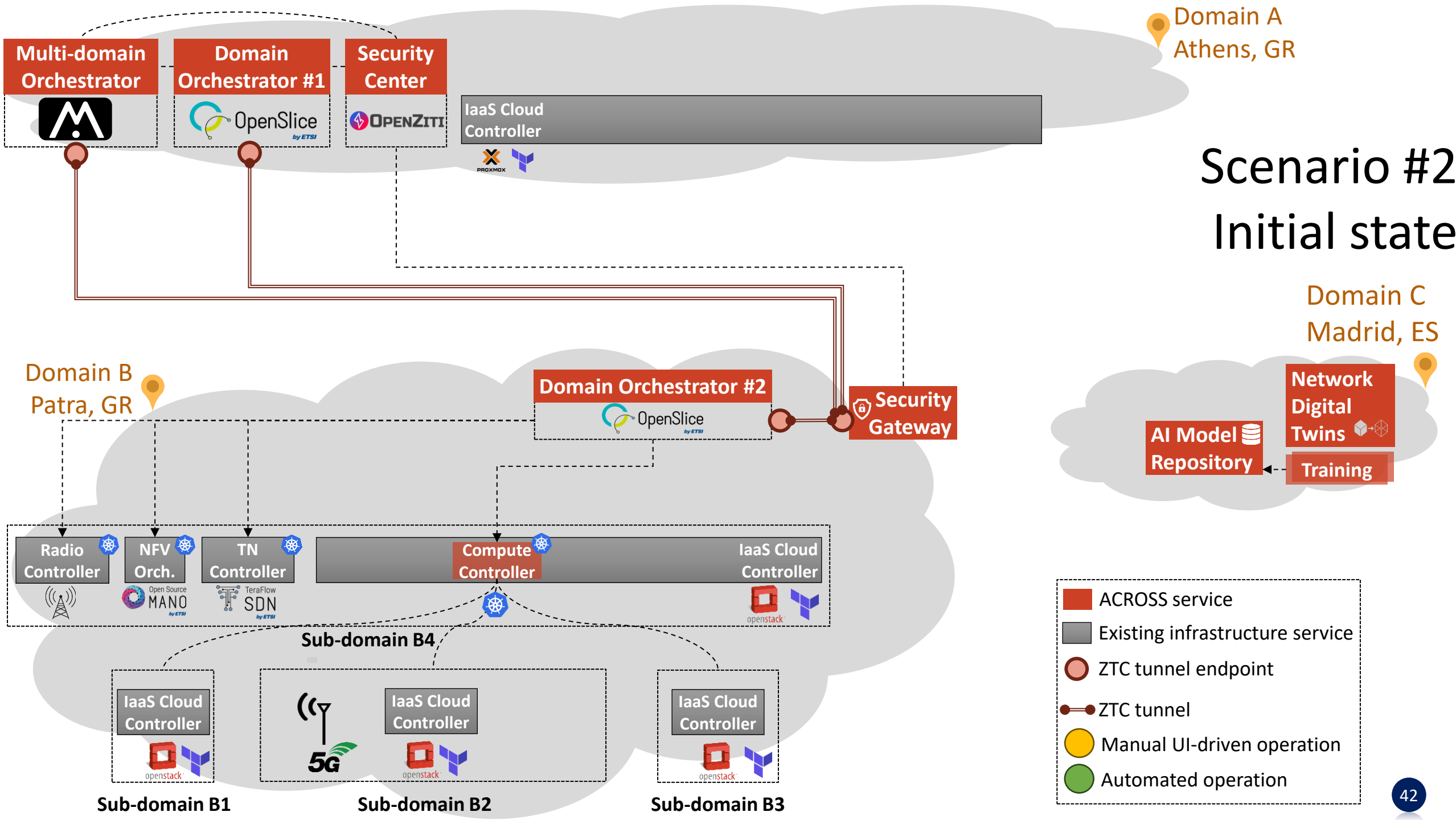
- A 5G video streaming service should be provisioned in Domain B
- Streaming clients should connect to a streaming server via 5G
- End-to-end telemetry data must be collected for this service

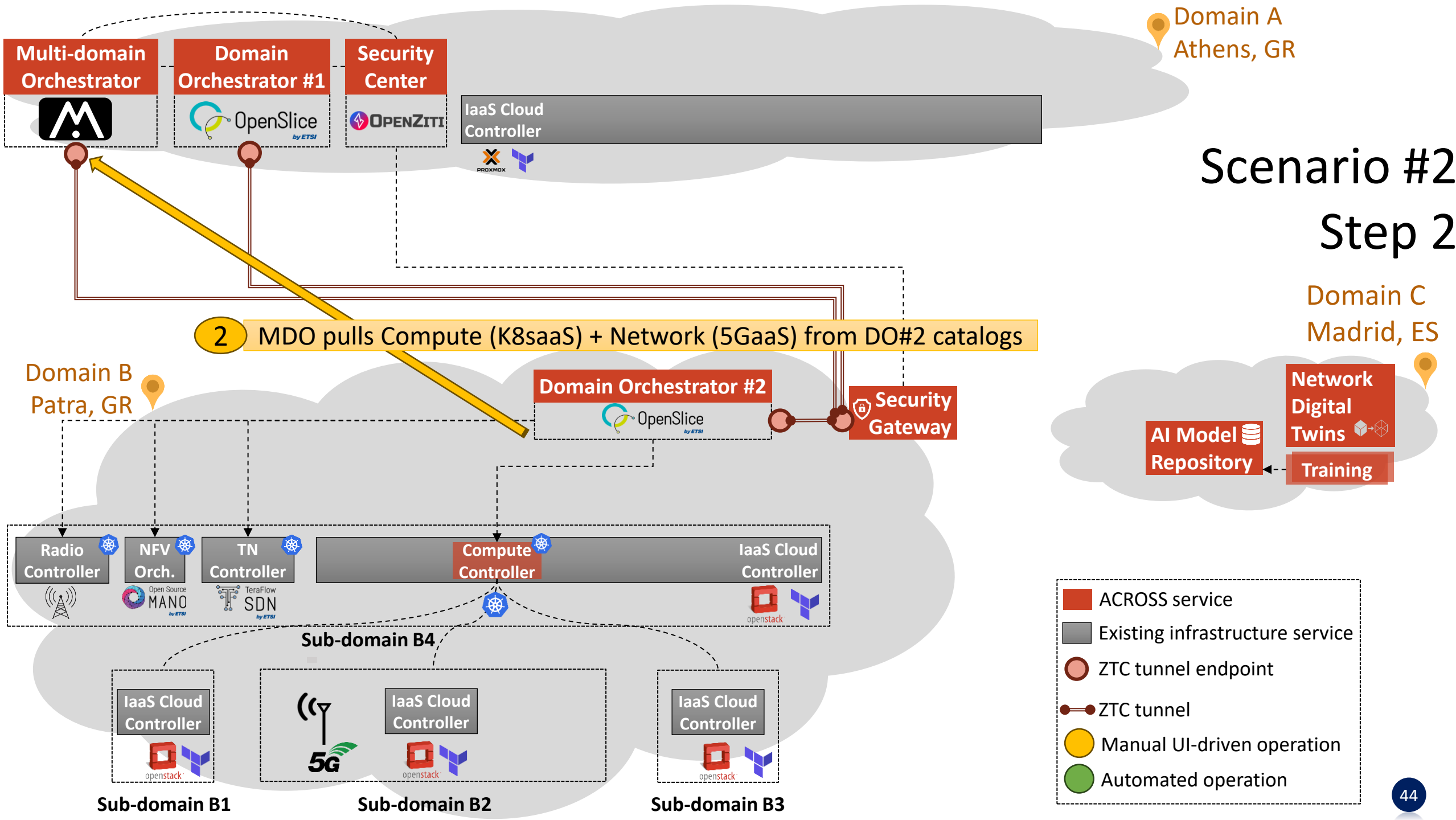


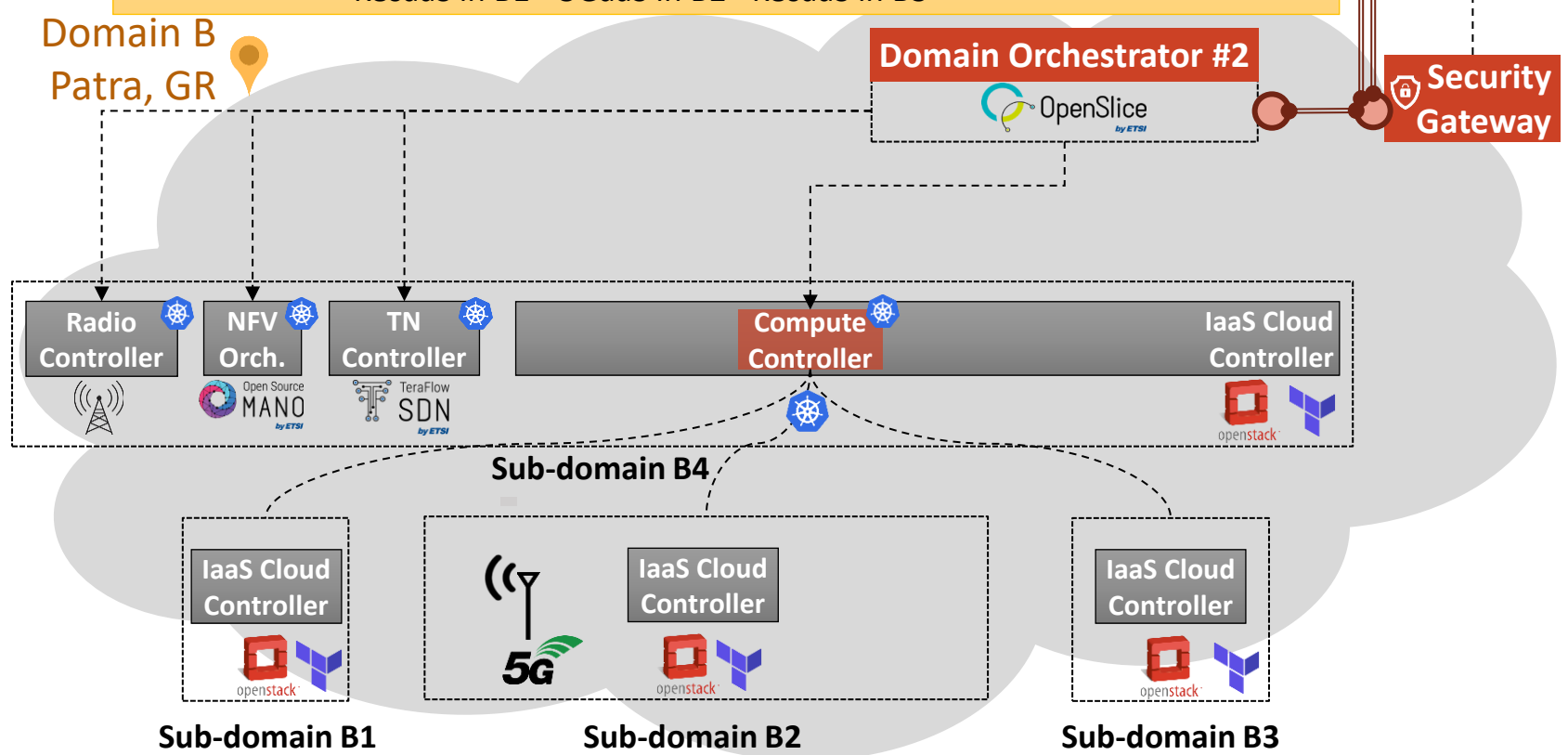
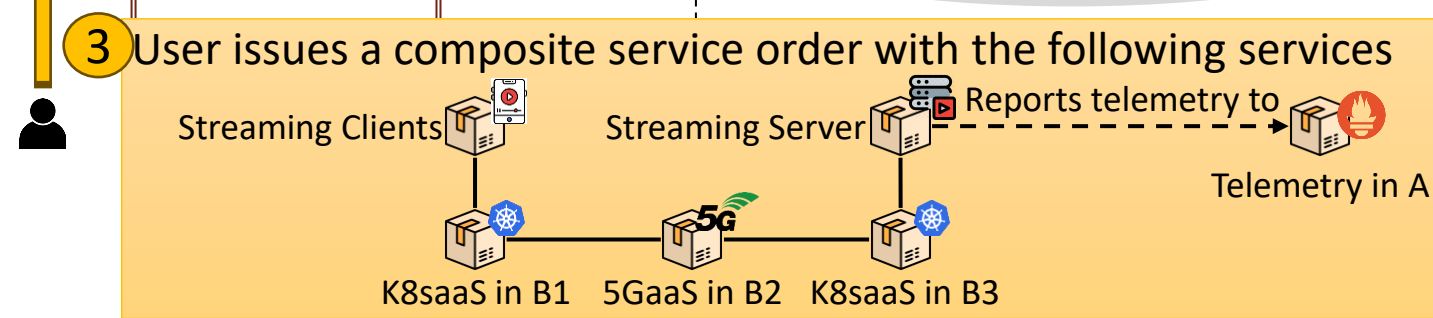
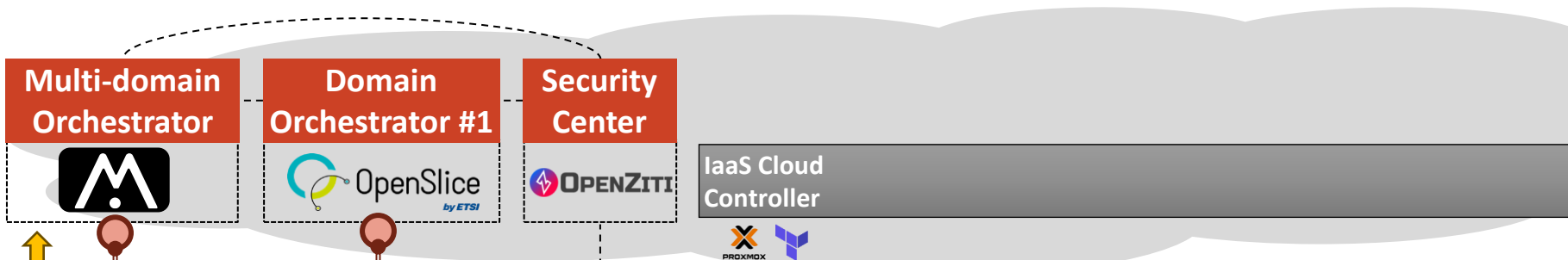
The platform should greatly-facilitate the end-to-end service provisioning, ideally via a single service order



The Multi-domain orchestrator (MDO) co-operates with the Domain Orchestrator (DO#2) to offer a composite service bundle that greatly automates service provisioning

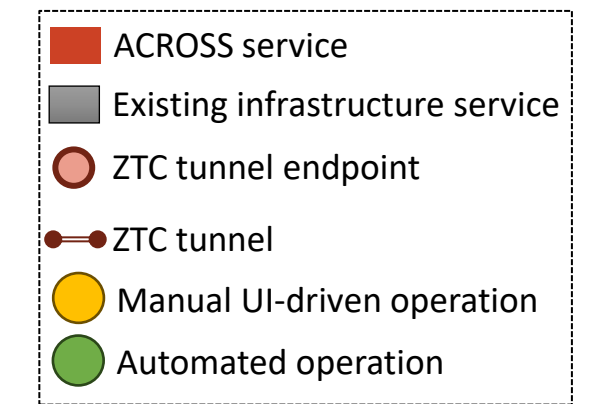
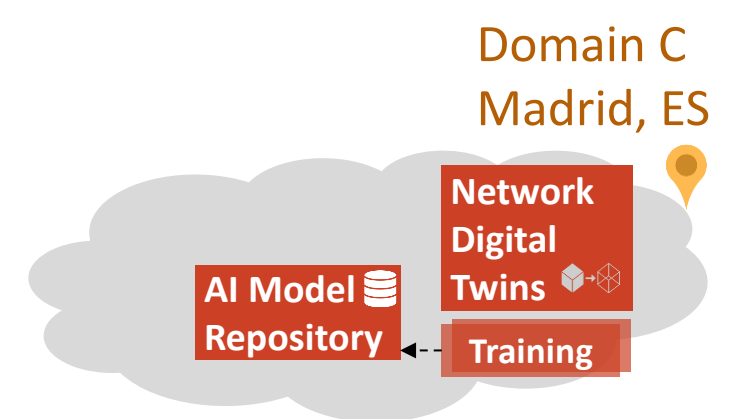


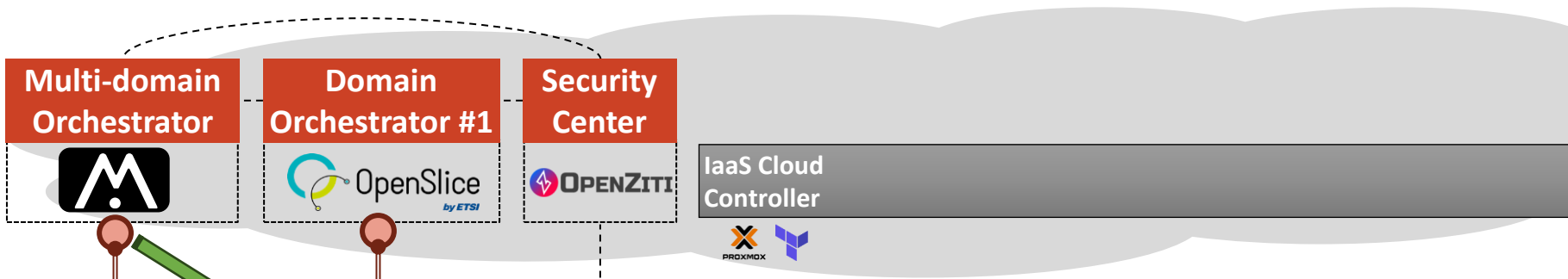




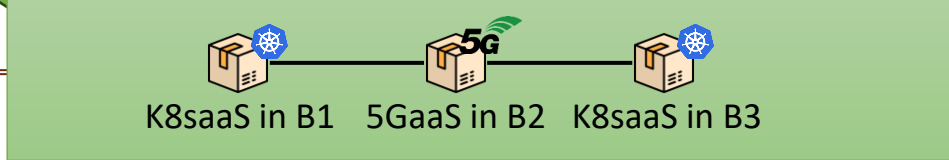
Scenario #2

Step 3

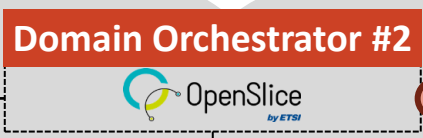
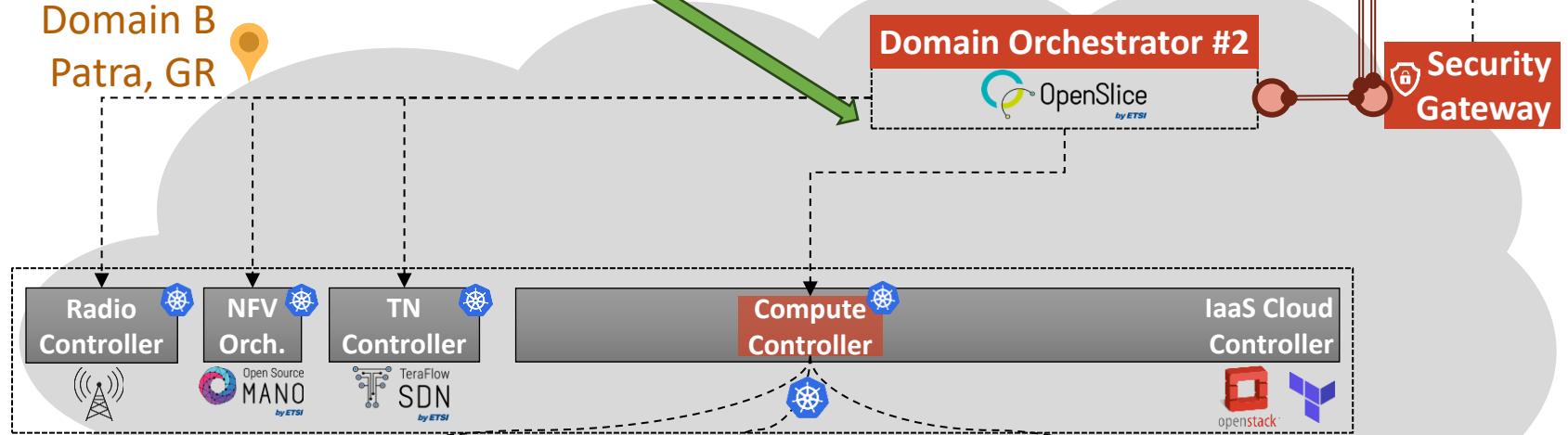




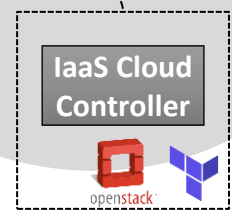
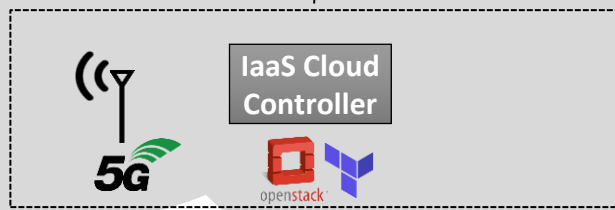
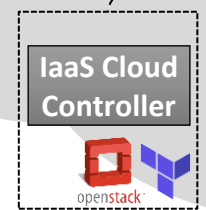
4 MDO orders basic platform services from DO#2



Domain B
Patra, GR



Sub-domain B4



Sub-domain B1

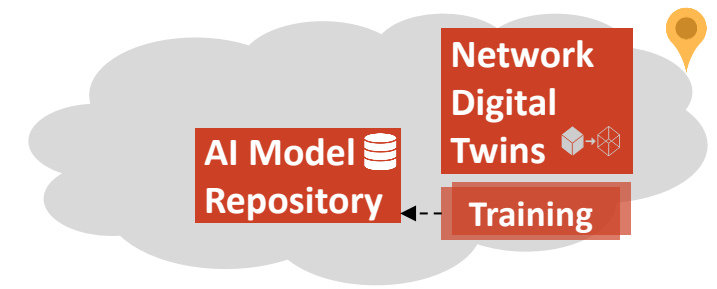
Sub-domain B2

Sub-domain B3

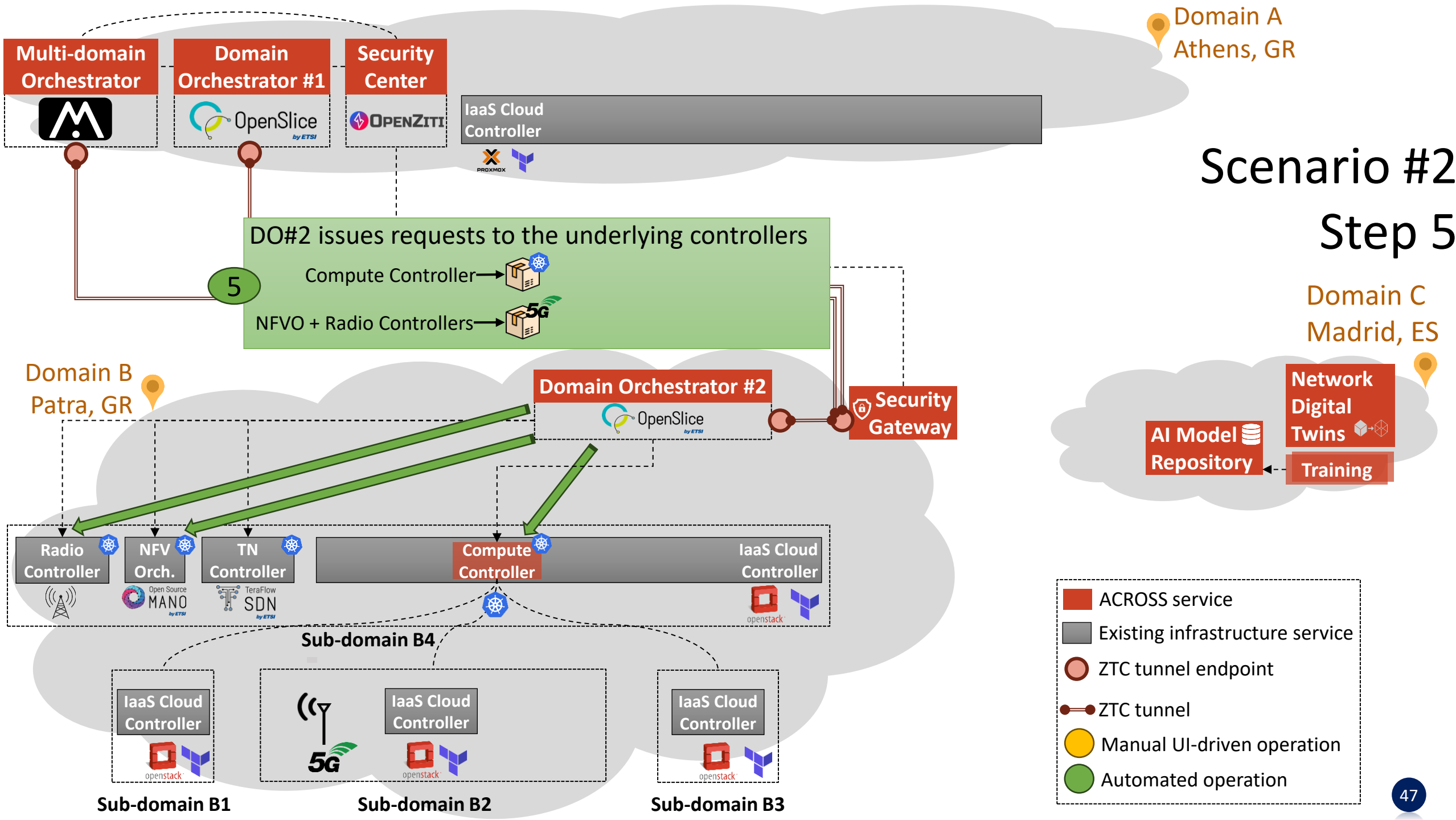
Scenario #2

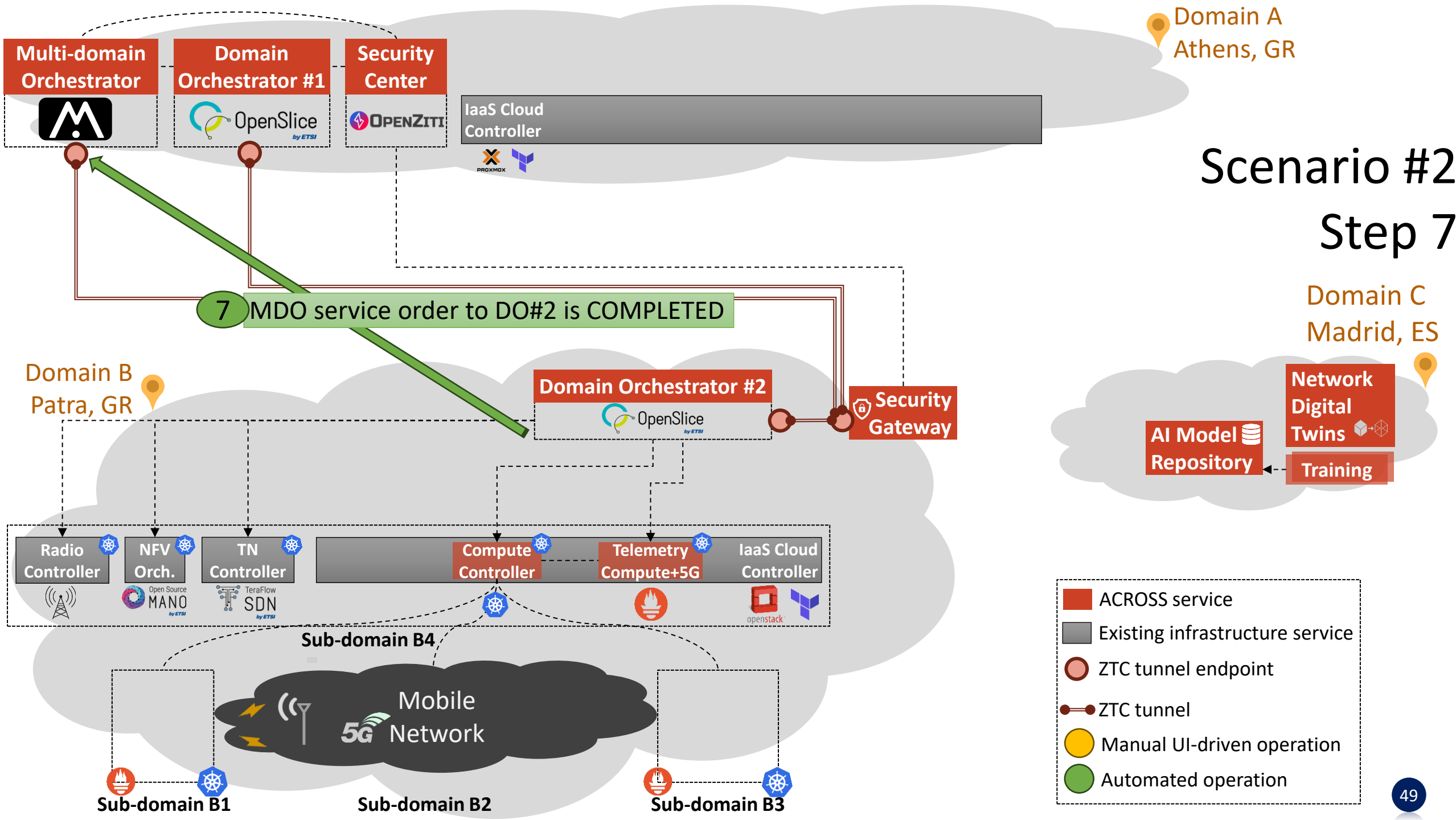
Step 4

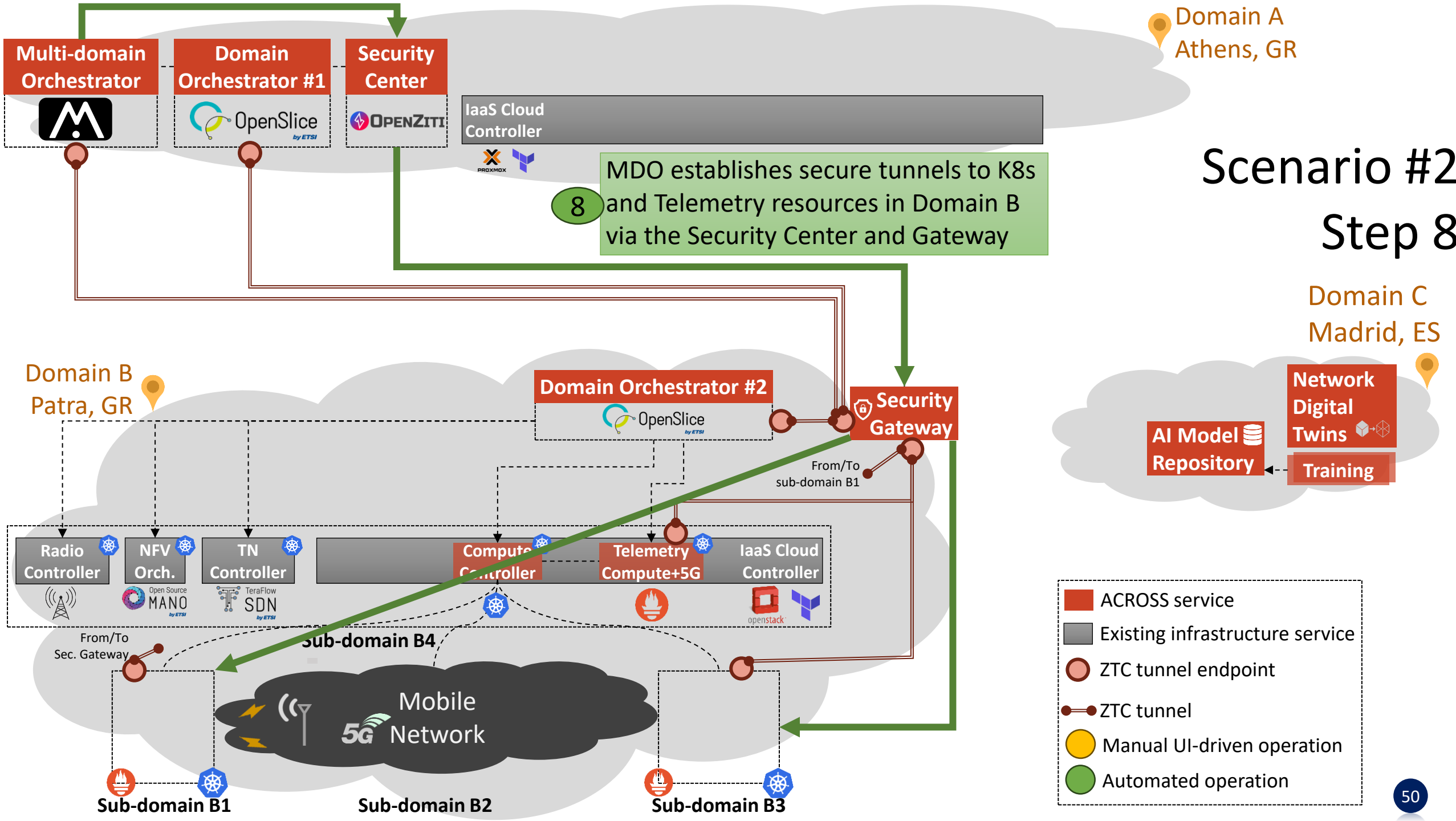
Domain C
Madrid, ES

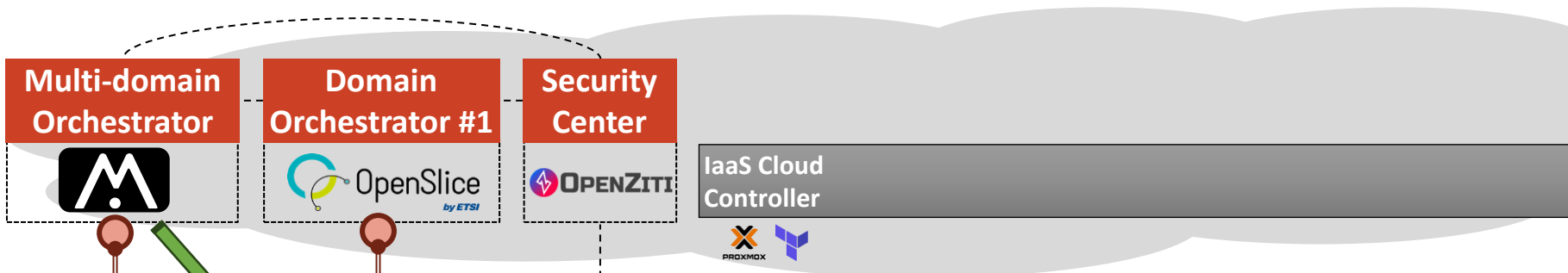


- ACROSS service
- Existing infrastructure service
- ZTC tunnel endpoint
- ZTC tunnel
- Manual UI-driven operation
- Automated operation









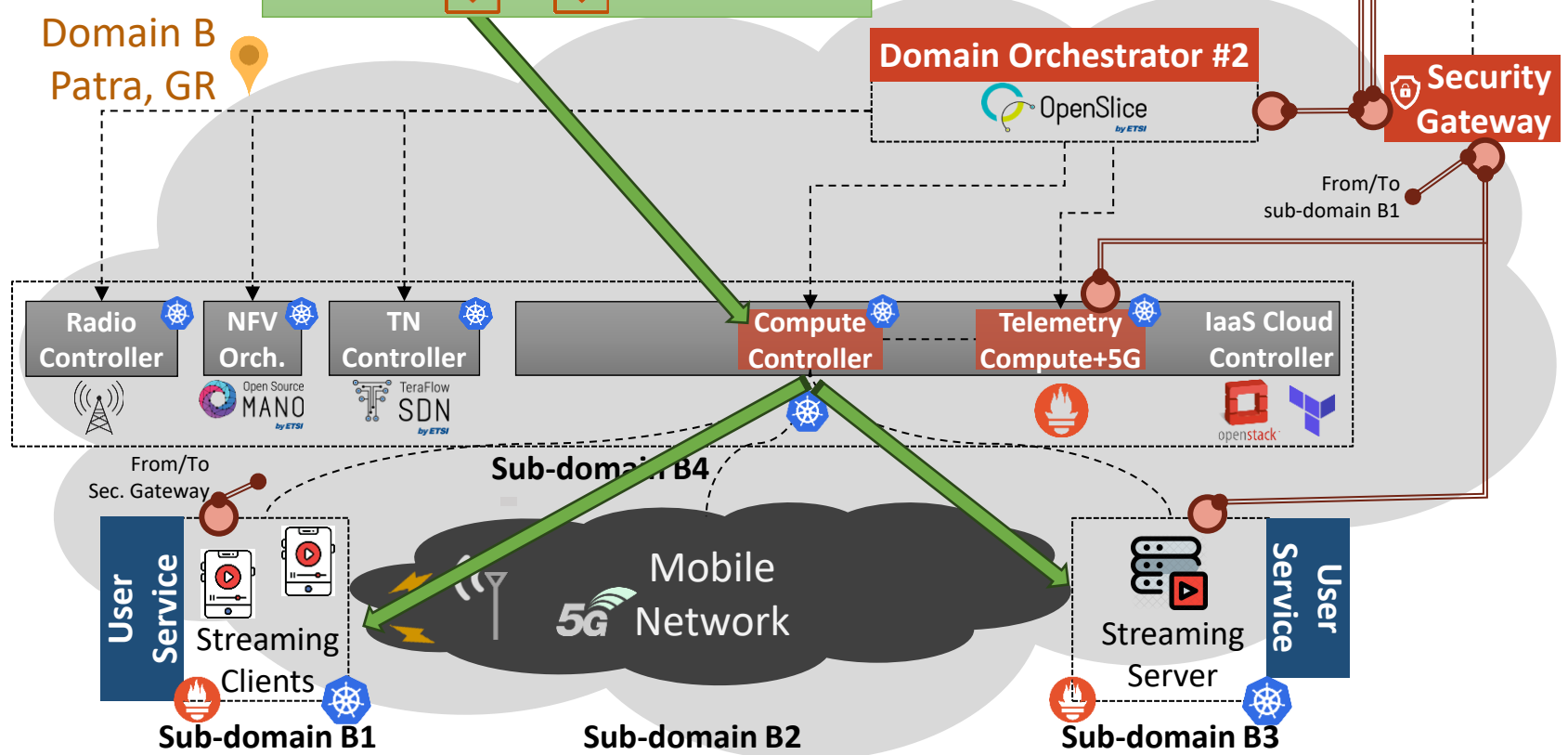
Domain A
Athens, GR

Scenario #2

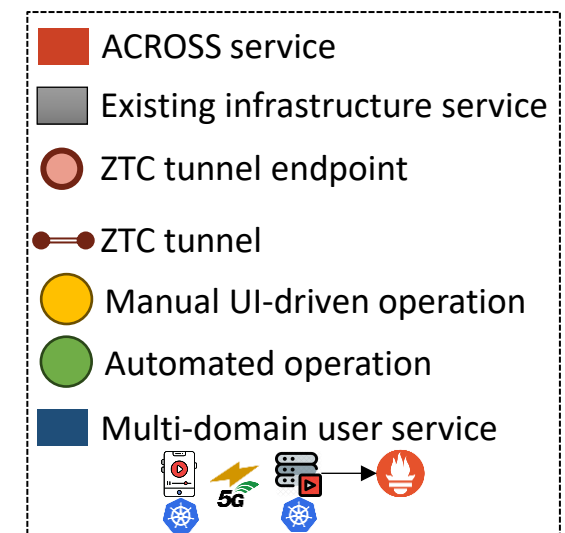
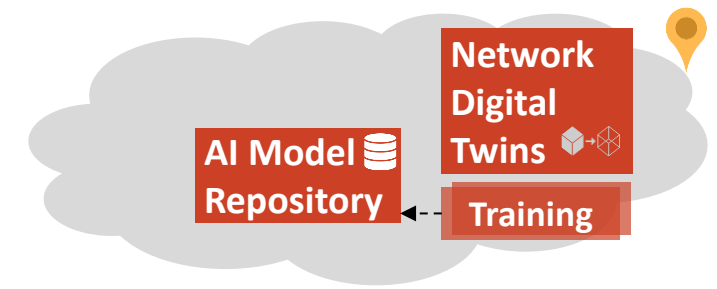
Step 9

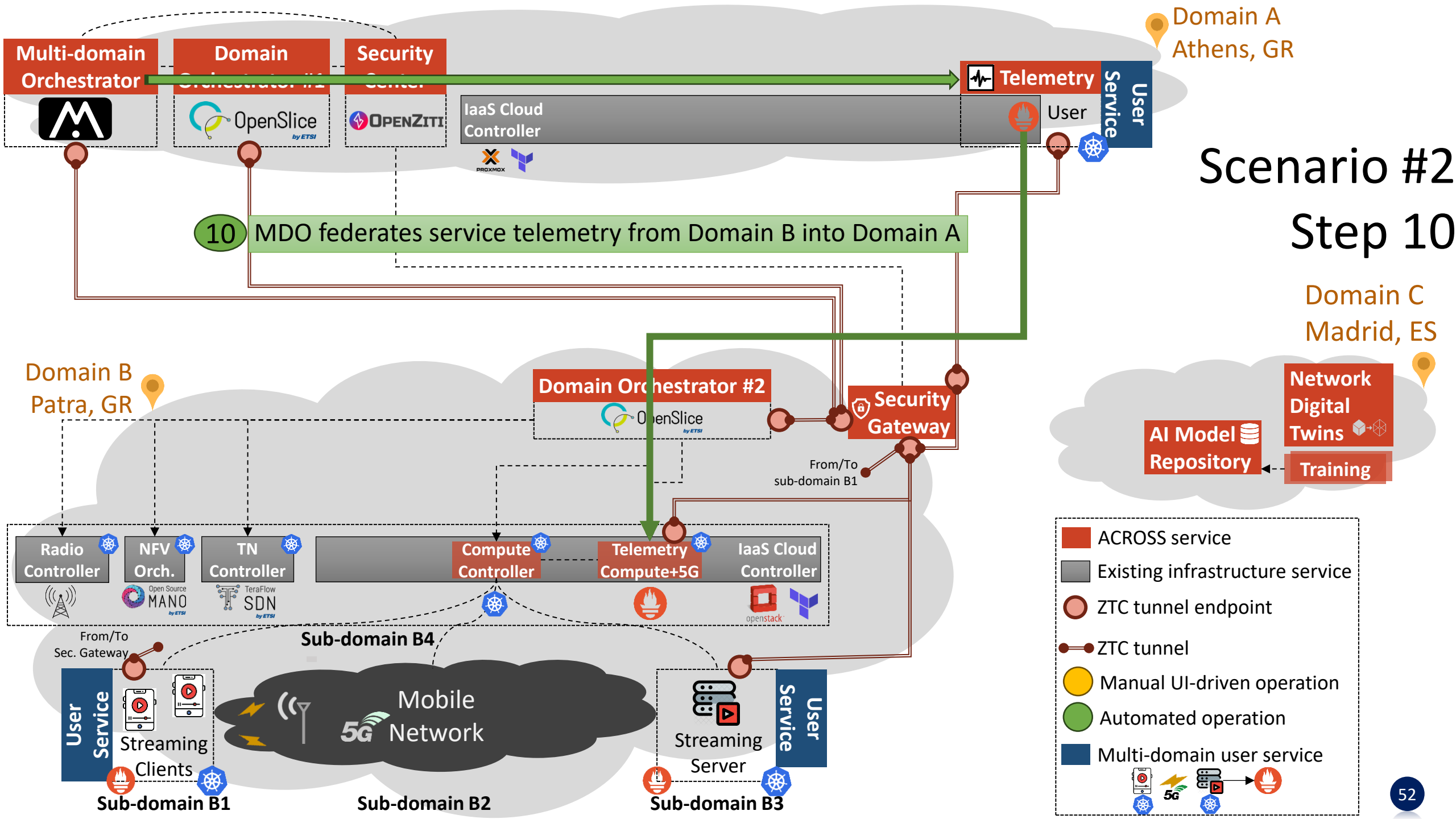
9 MDO deploys streaming services in Domain B's compute clusters

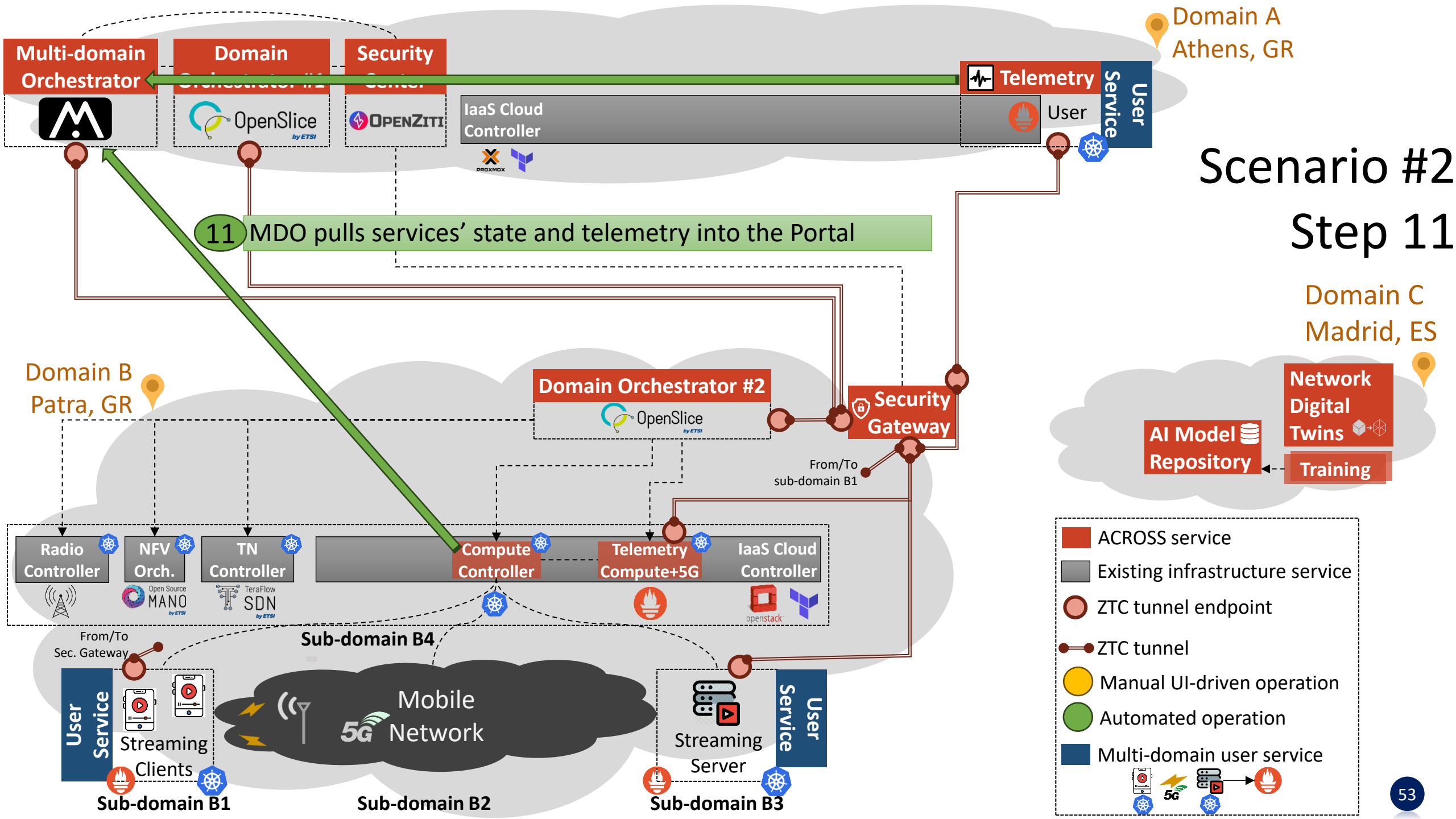
Domain B
Patra, GR

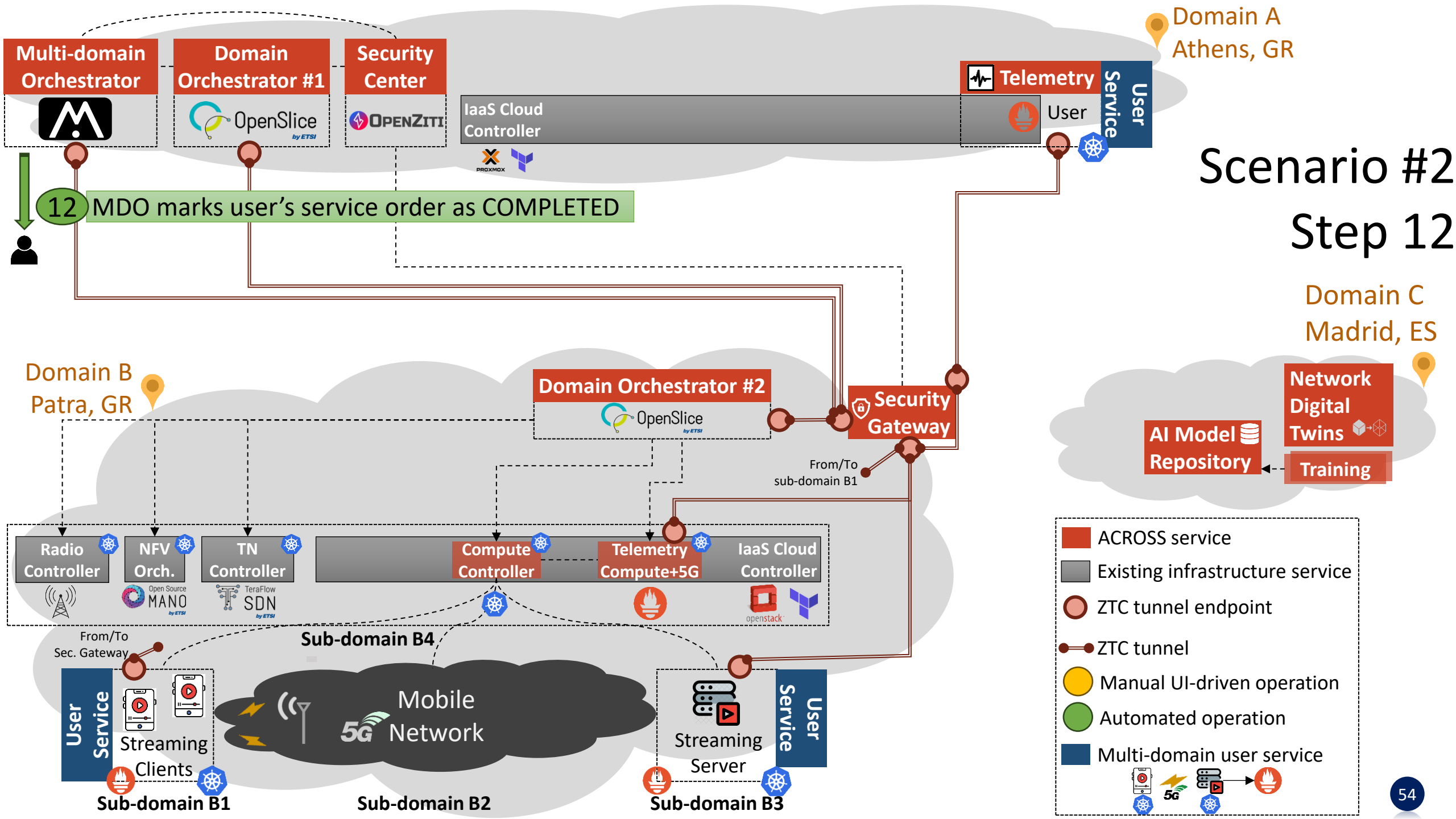


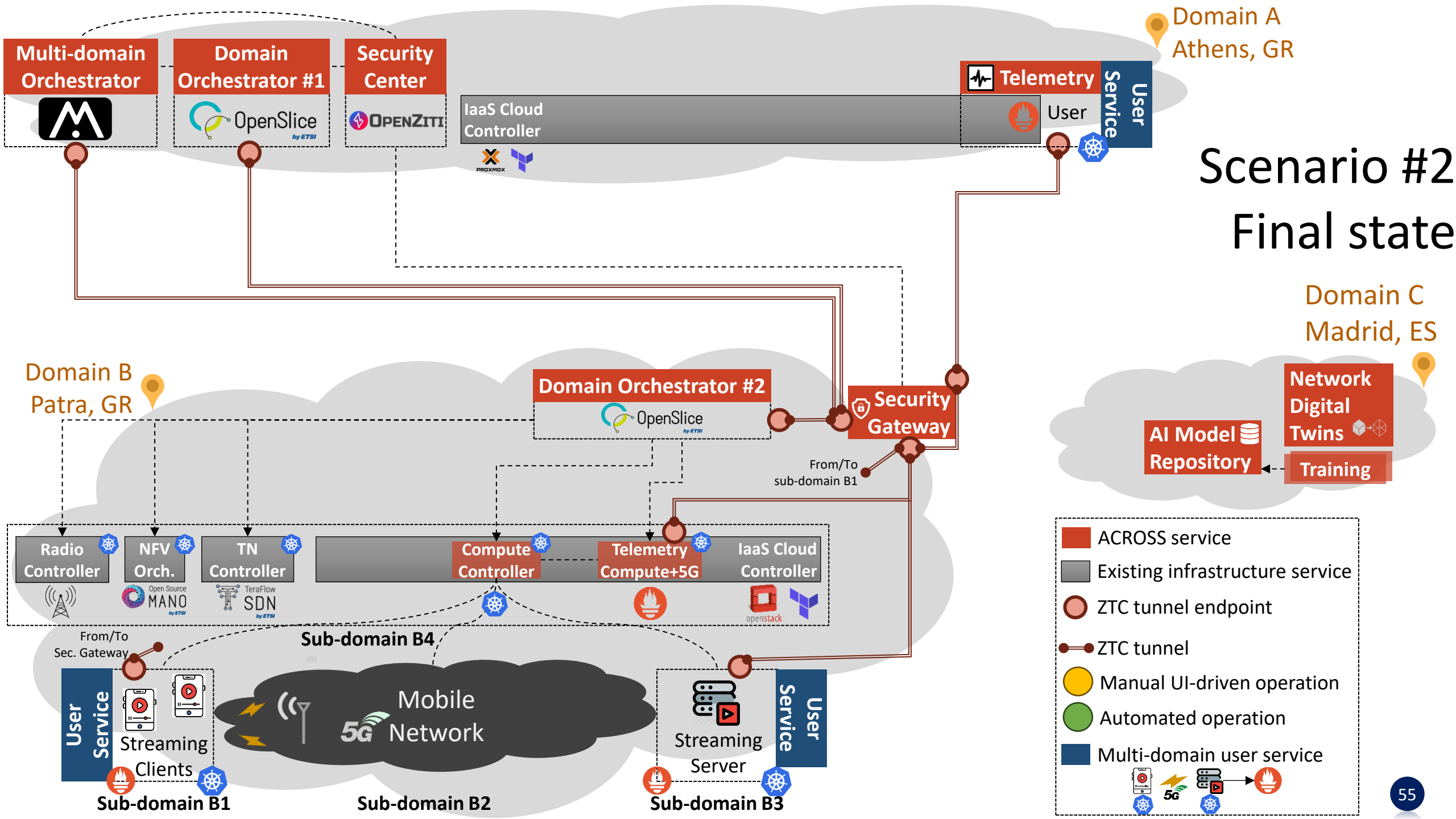
Domain C
Madrid, ES



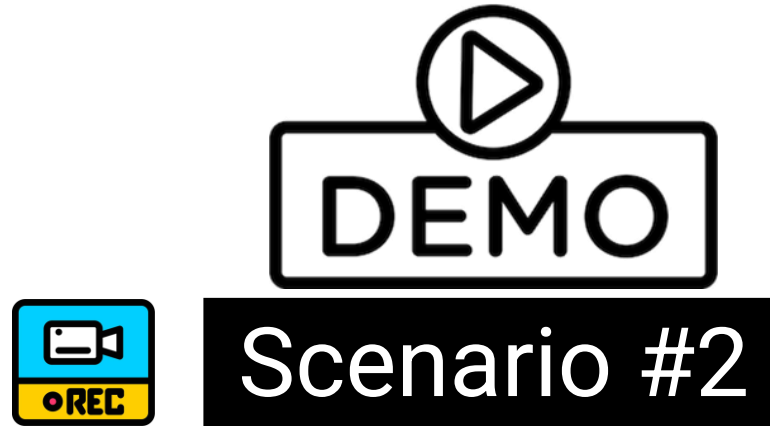








PoC Scenario #2 – Demo time

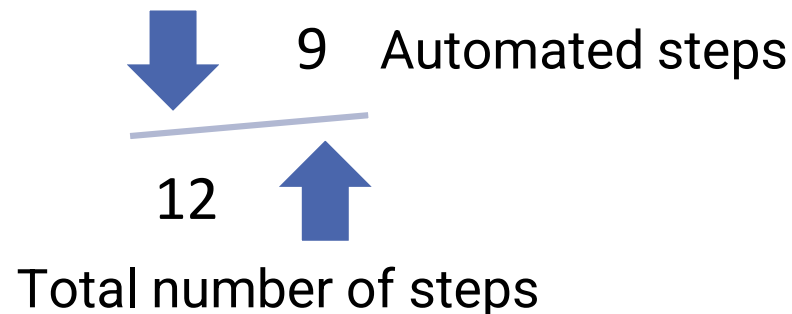


PoC Scenario #2 – Remarks (1/2)

Multi-domain and telemetry-assisted **service provisioning** over on-demand compute (K8s) and network (5G) resources

- DO#2 manages compute and network (platform) services within domain B
- MDO deploys end-user services atop platform services
- MDO federates telemetry across Domains A & B to acquire the state of the deployed services

Amount of Automation = 75%



PoC Scenario #2 – Remarks (2/2)

Amount of Automation = 100% is possible if we sacrifice dynamicity and user-experience

➔ Static synchronization of catalogs (peering) between MDO and DO#2

MDO portal prioritizes UX via dynamic, user-driven peering



➔ Automated service order upon release of a new service version

MDO allows tight integration with the service provider

PoC Stories – Scenario #3



Scenario #3 Presenters



Lluís Gifre
ETSI TFS TSC Chair



Dimitrios Triantafyllou **wings.**

PoC Scenario #3 – On-demand Service Security & Predictive SLA Preservation



Service provider requests:

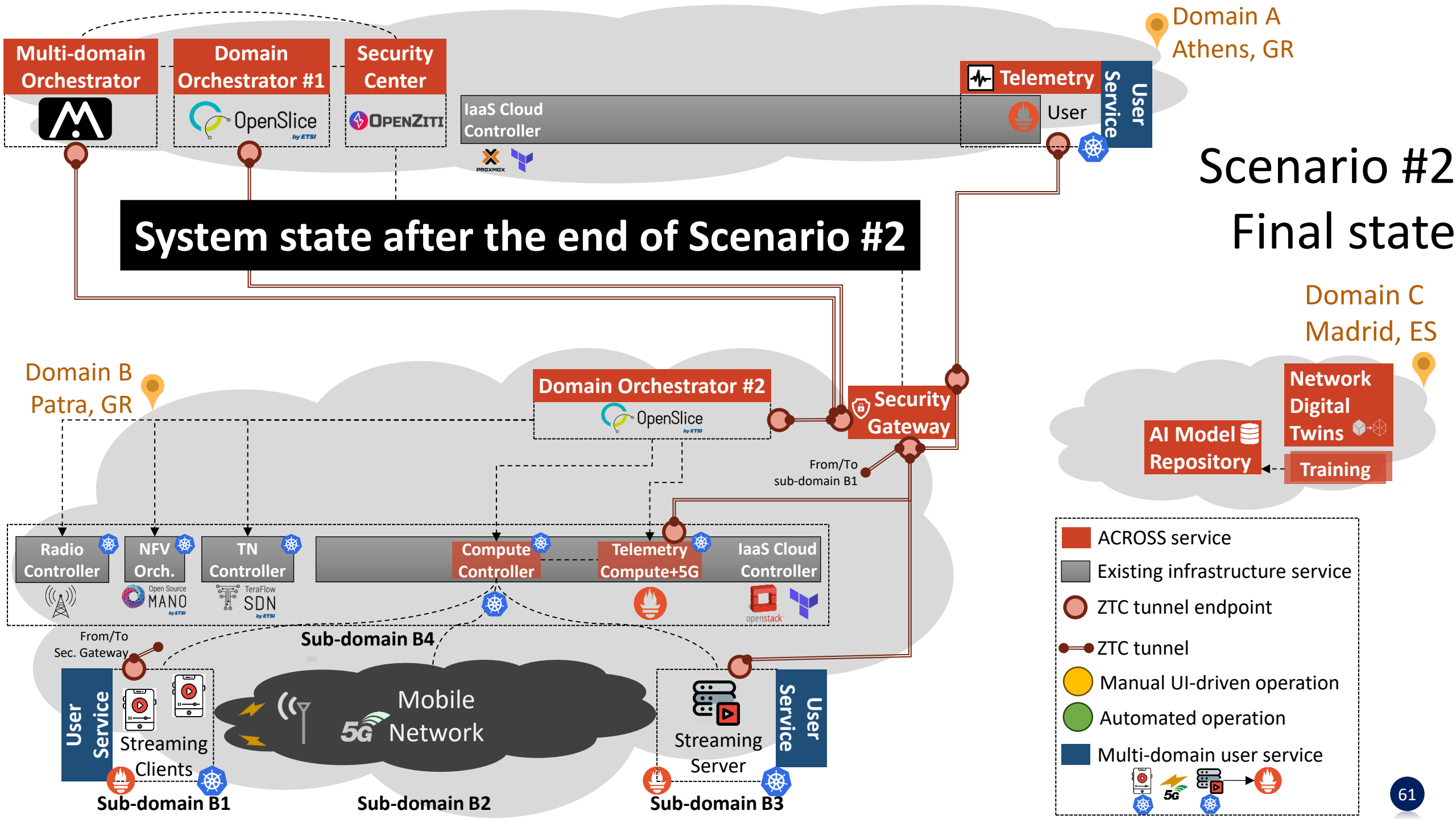
- a security SLA for protecting some service components (on demand)
- a performance SLA which should be preserved in a proactive fashion

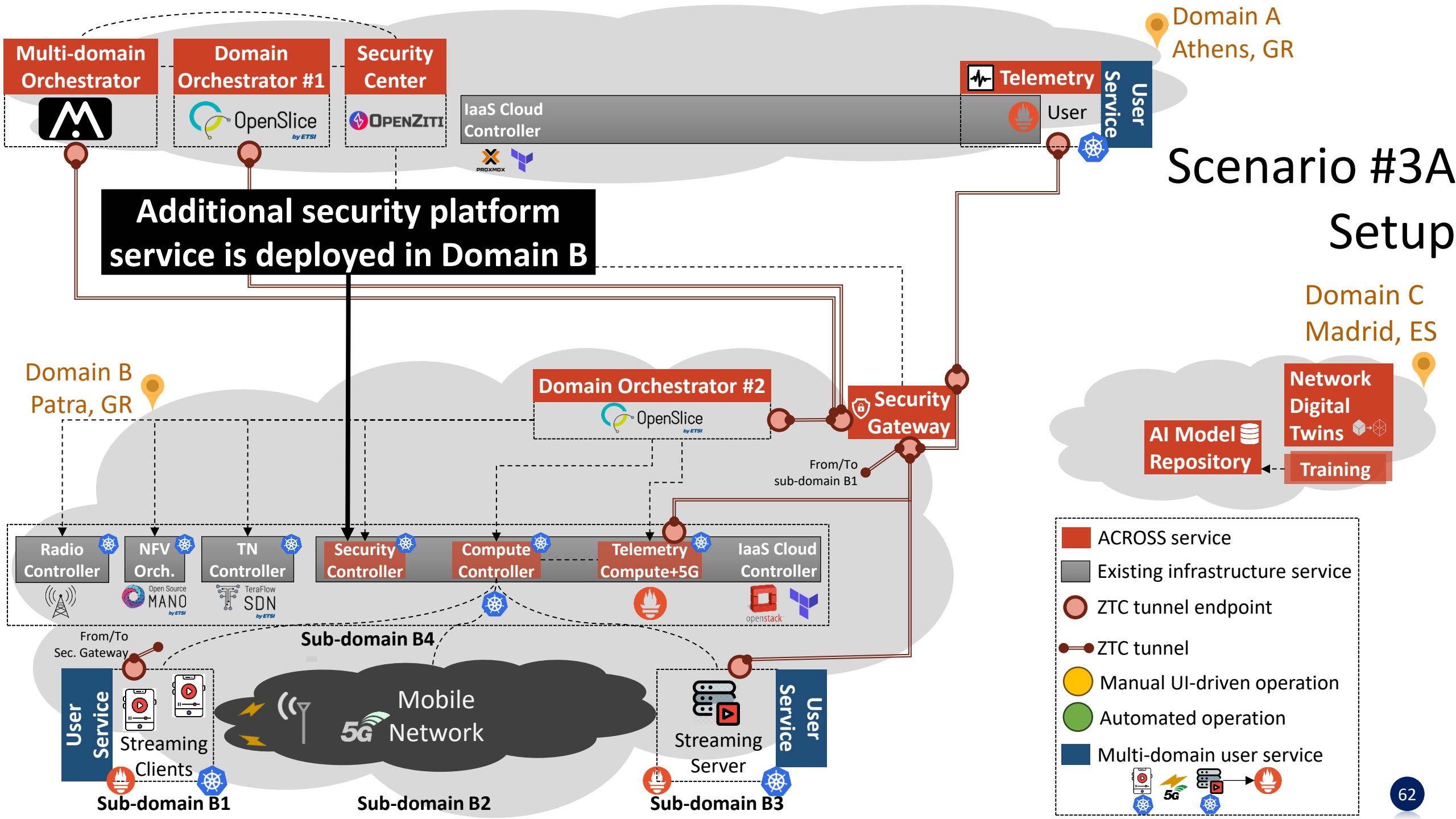


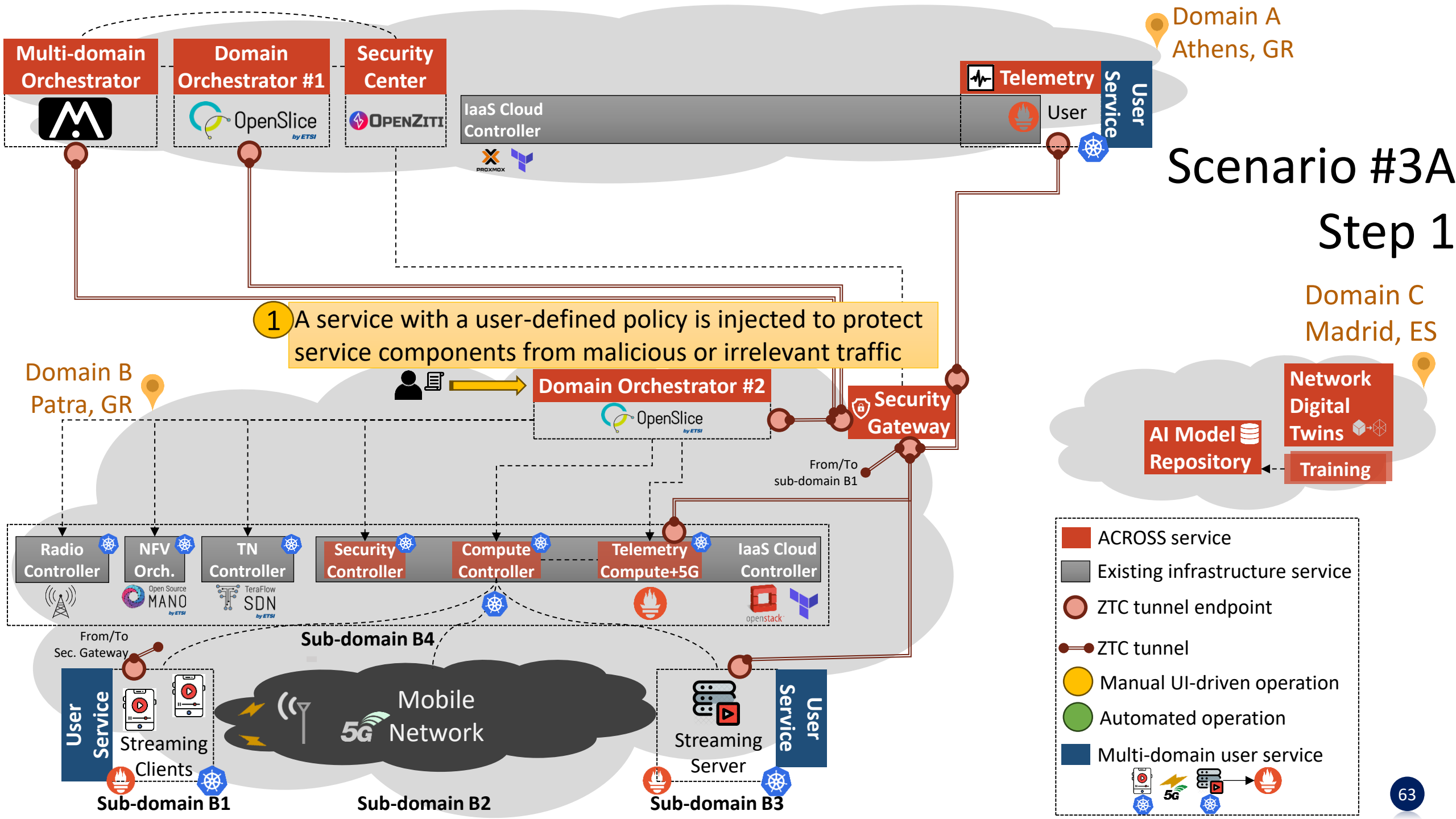
The platform should offer means to facilitate both on-demand service security and proactive SLA preservation

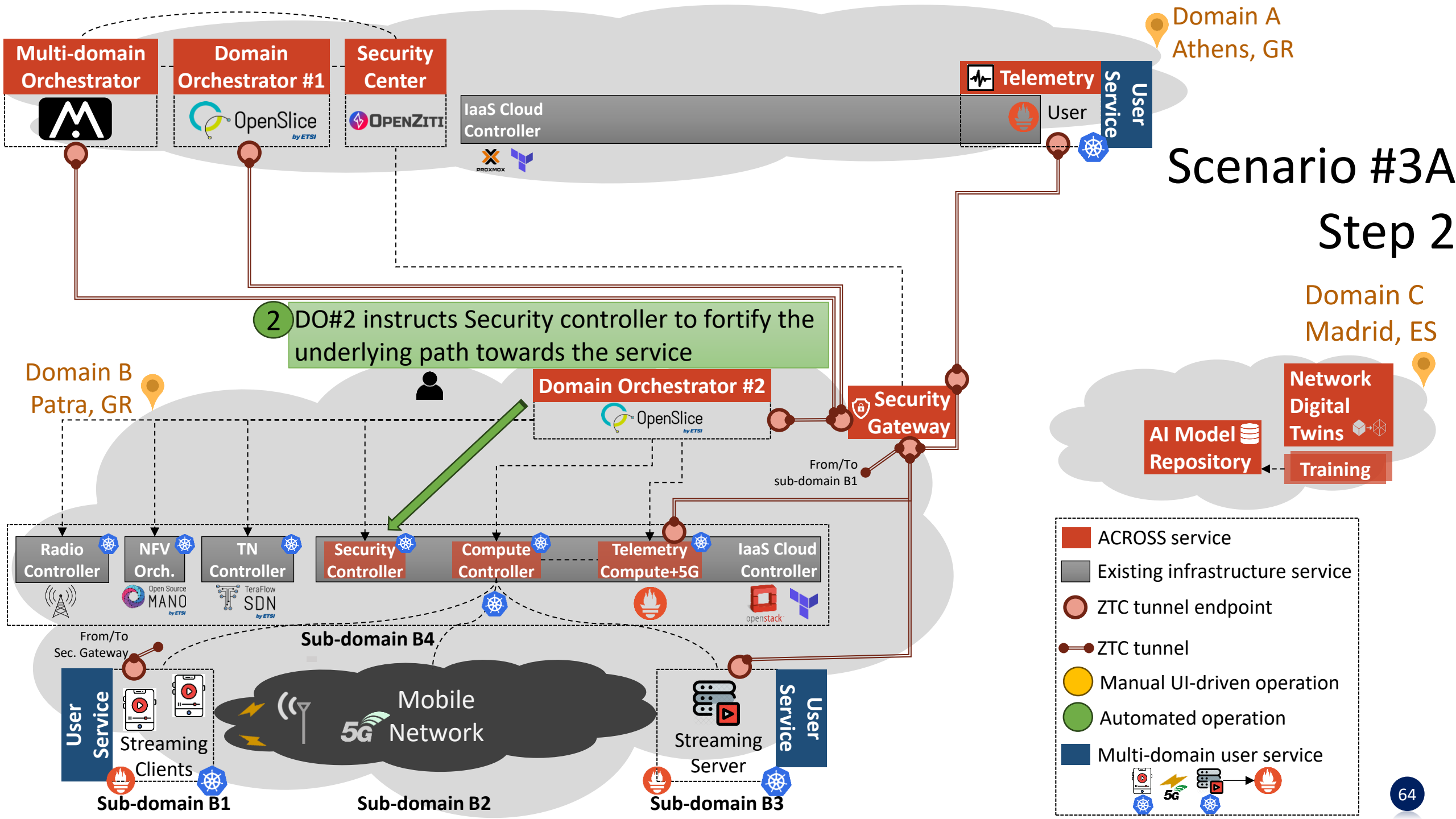


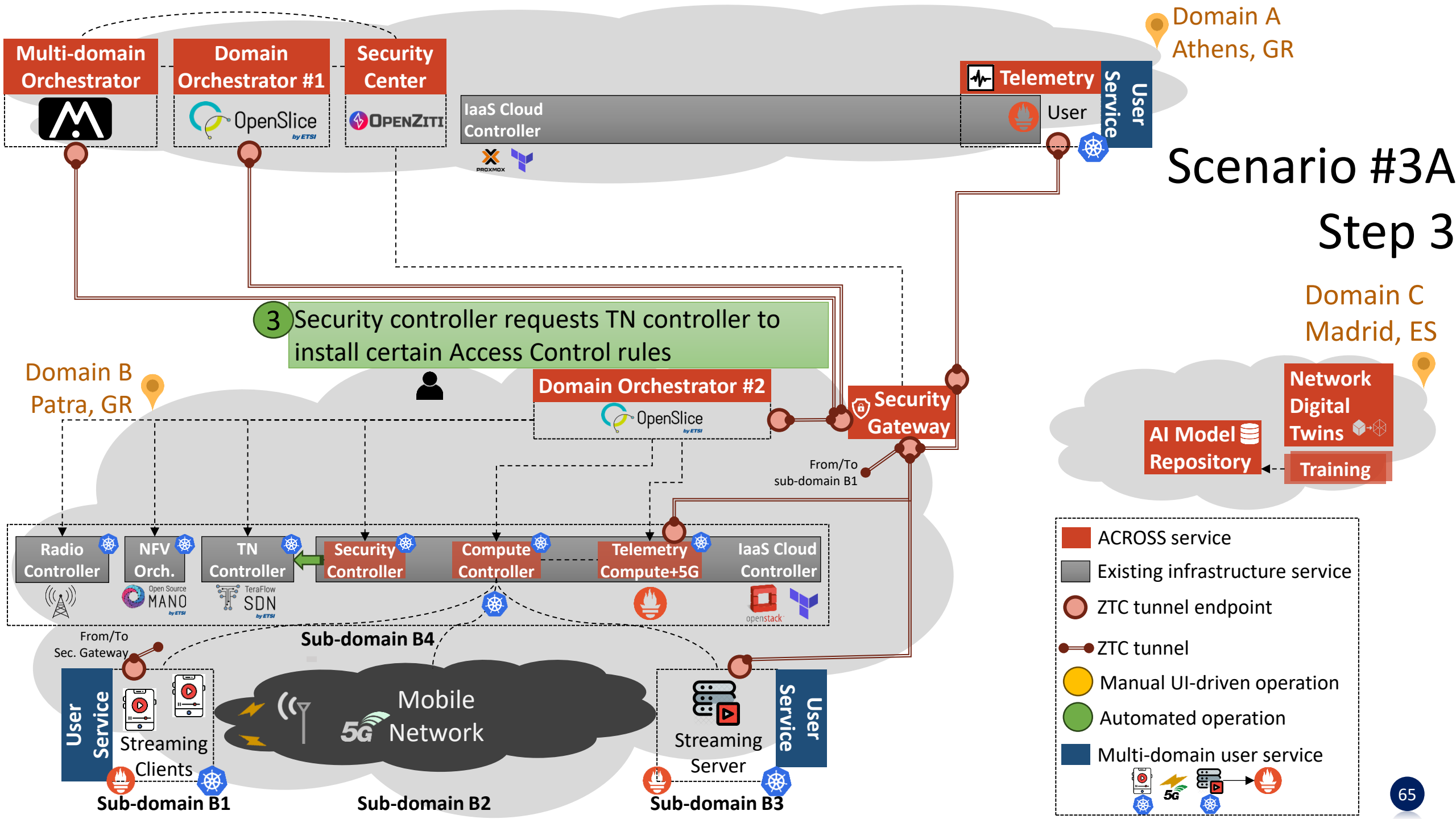
- Additional services are employed in Domain A (Automation and Intelligence for SLA) and Domain B (Service Security)
- A closed loop is designed and employed

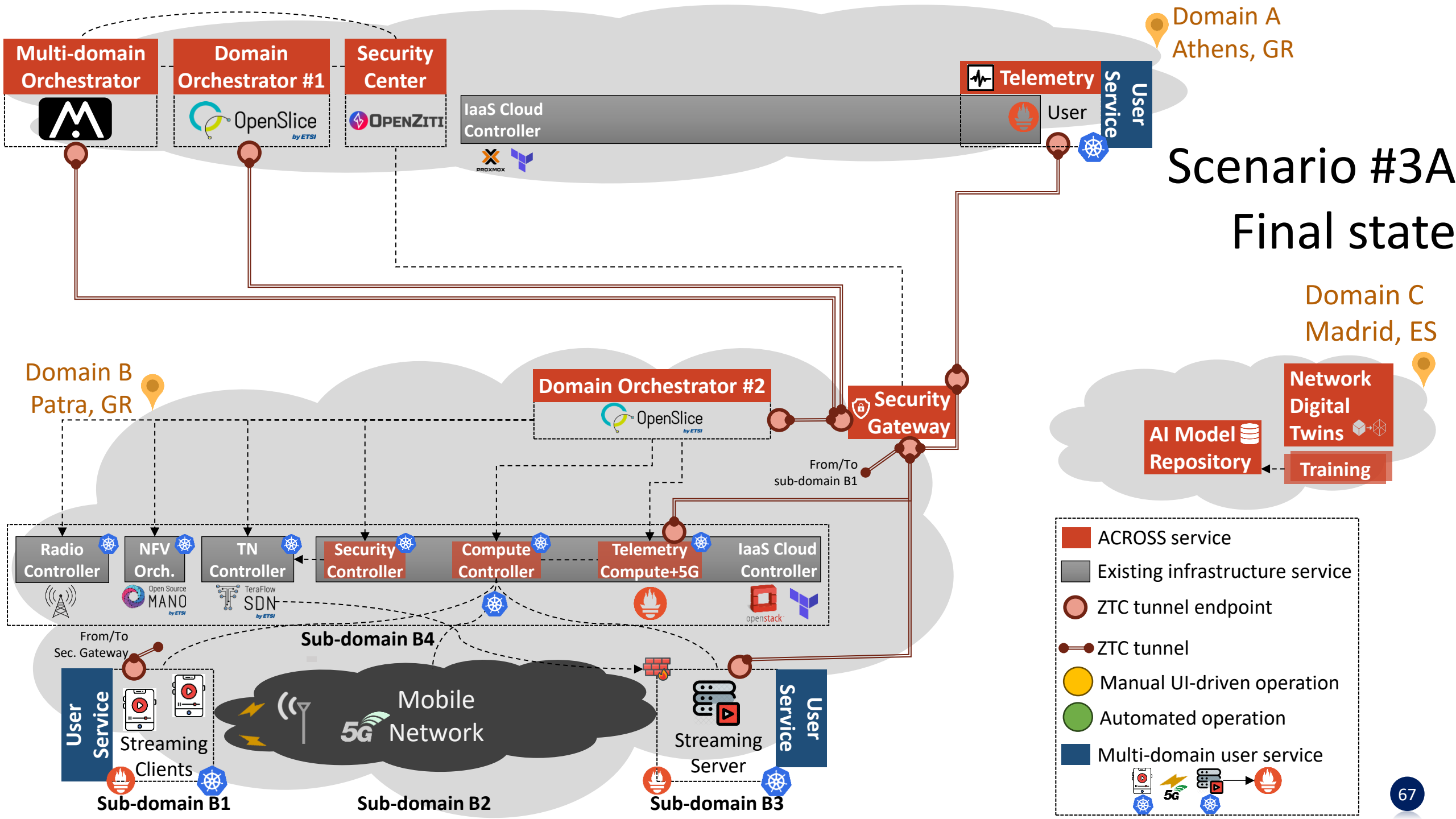




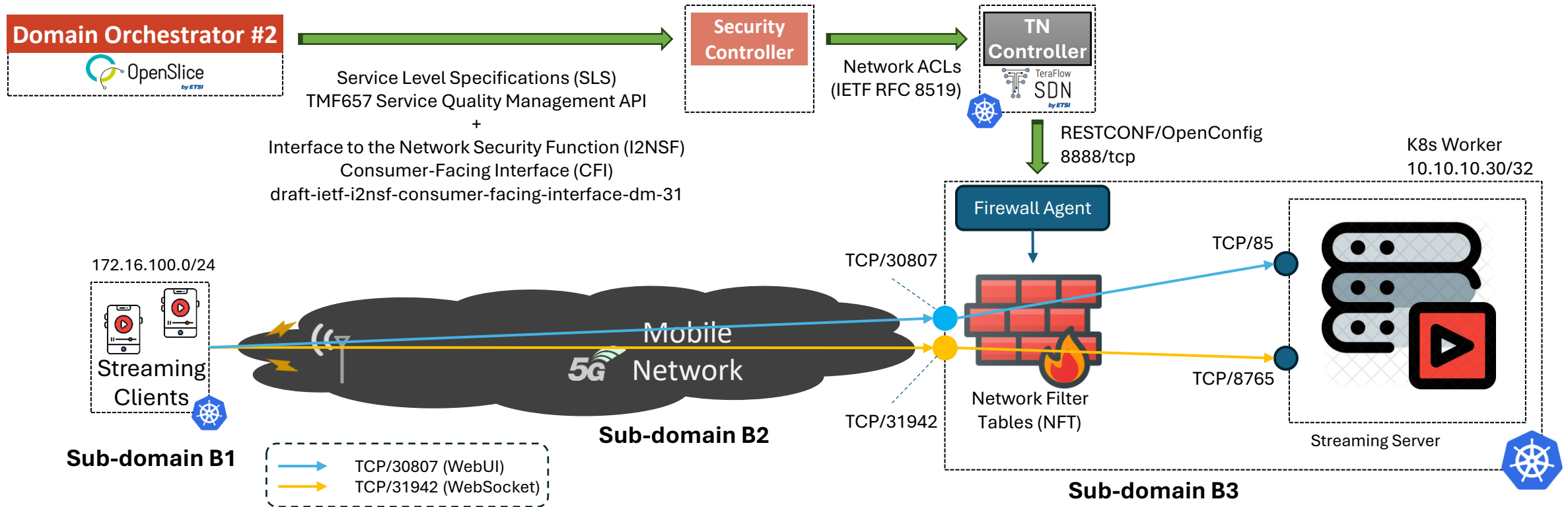








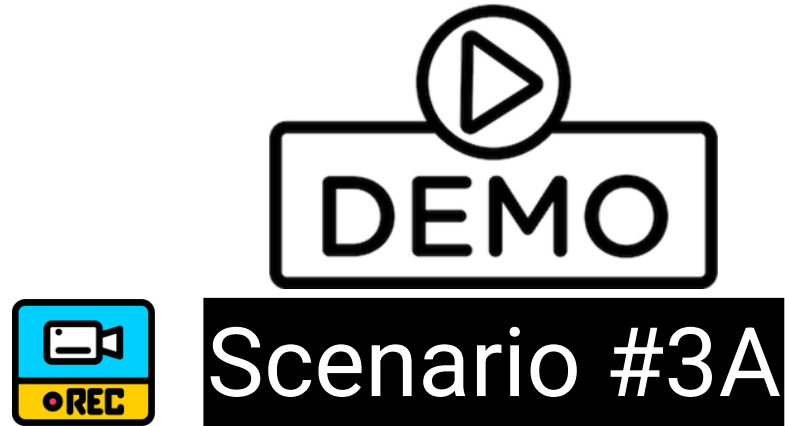
PoC Scenario #3A – Firewall Agent details



ACL Ruleset

#ID	Prio	Src Addr	Dst Addr	Proto	Src Port	Dst Port	Action	Comment
0	0	172.16.100.0/24	10.10.10.30/32	TCP	*	30807	ACCEPT	Allow clients on demand
.....								
-2	-300	*	10.10.10.30/32	TCP	*	30807	REJECT	Default deny WebUI
-1	-300	*	10.10.10.30/32	TCP	*	31942	ACCEPT	Default allow WebSocket

PoC Scenario #3A – Demo time

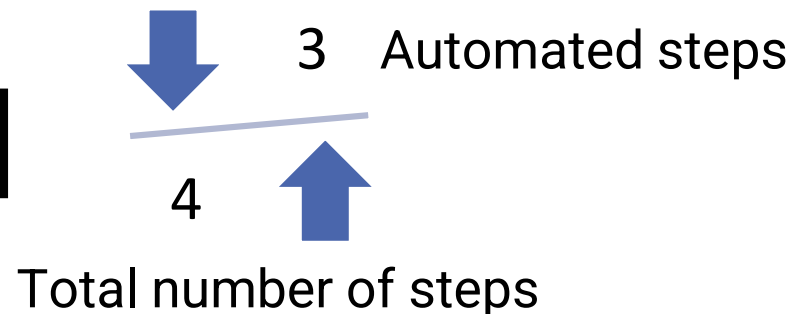


PoC Scenario #3A – Remarks (1/2)

Policy-based runtime service adaptation to control access towards service components

- DO#2 service designed with rule injection at certain state of the LCM
- DO#2 integration with Security controller and the underlying TN controller
- In-network dynamic filtering of traffic towards end-user services

Amount of Automation = 75%

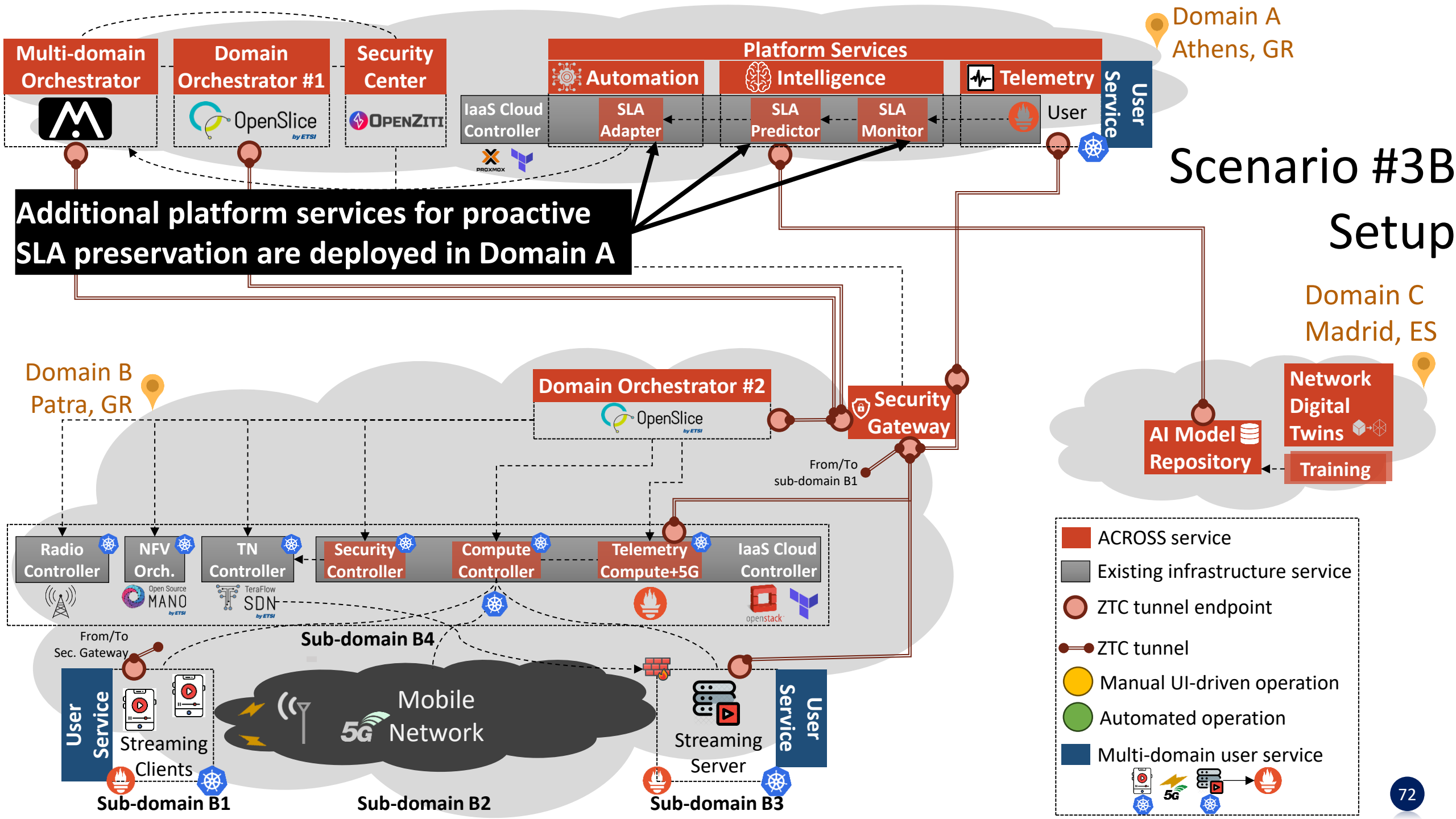


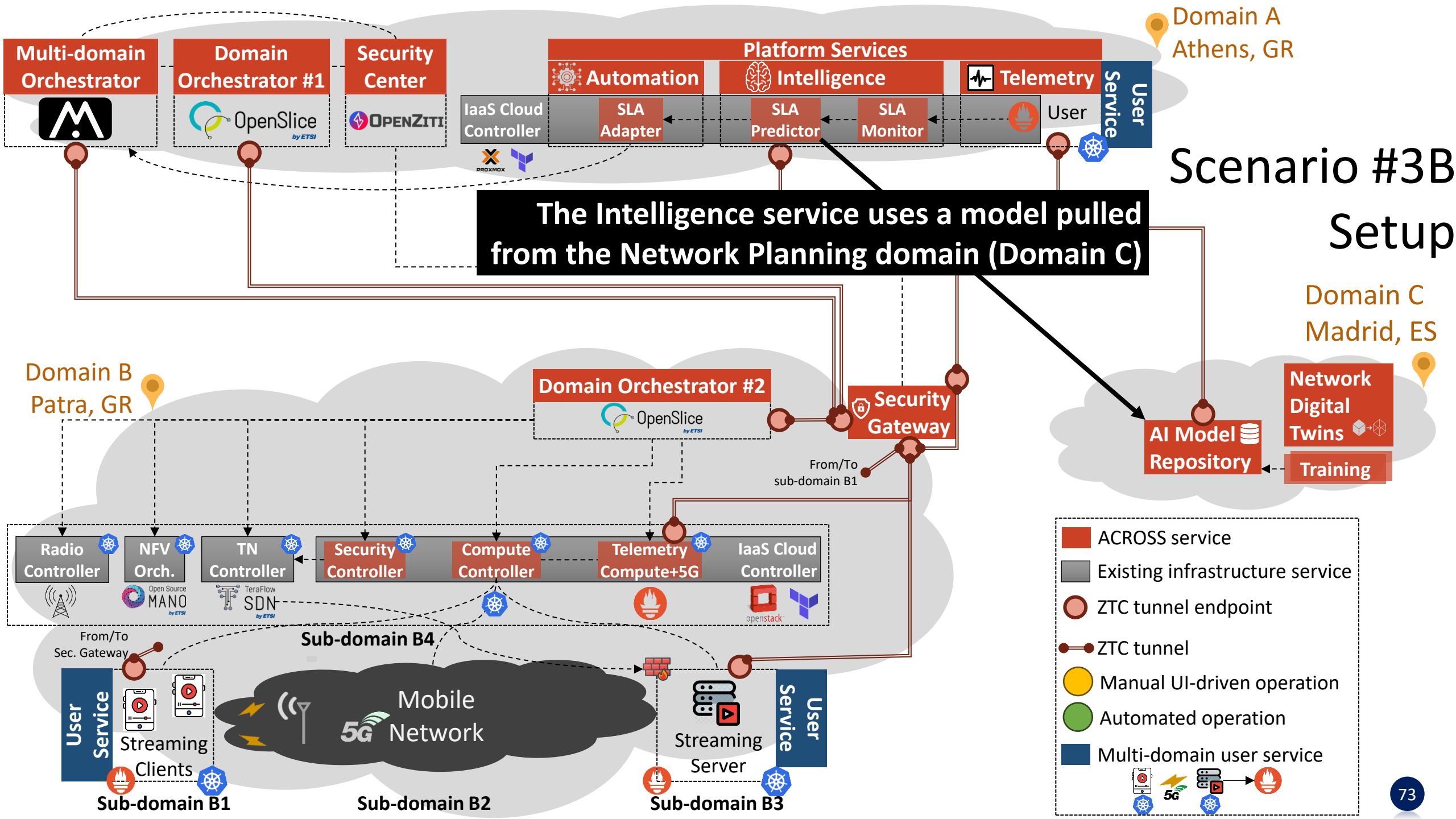
PoC Scenario #3A – Remarks (2/2)

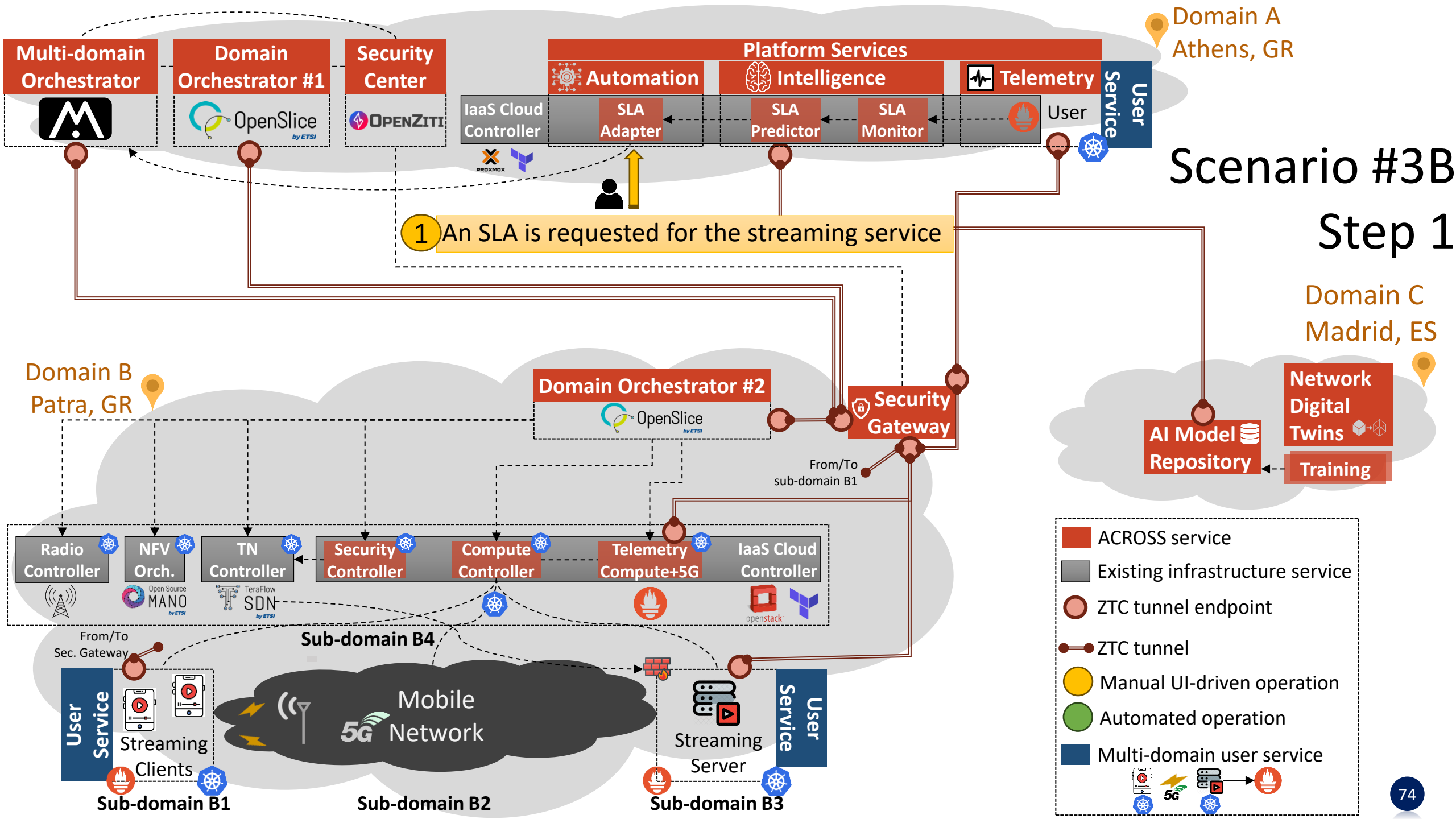
Amount of Automation = 100% is possible using gitops, but we opted for a user-designed service with embedded security policy that can be ordered on demand

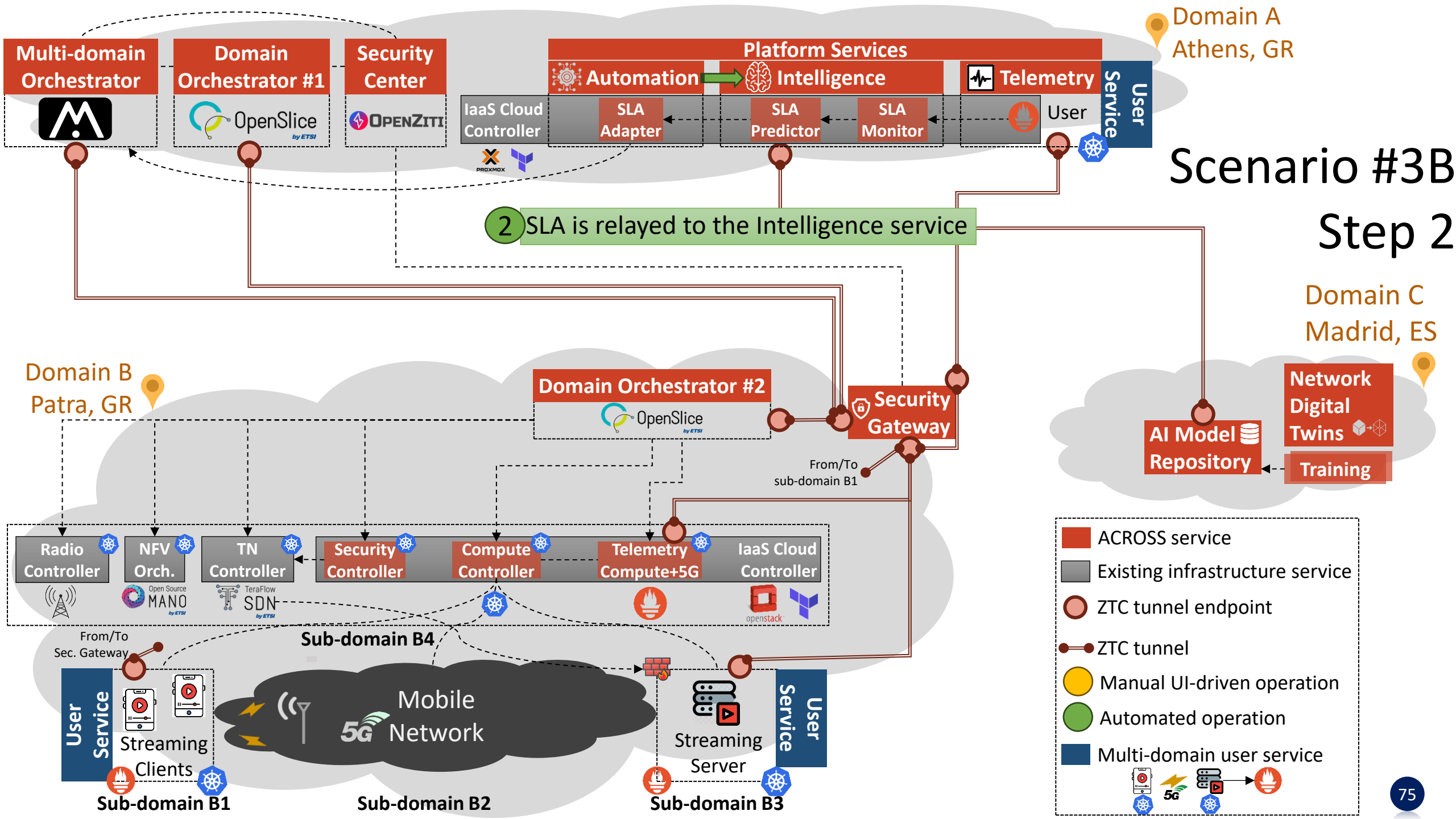
→ Automated service order upon an event (e.g., when the end user service gets installed in domain B3)

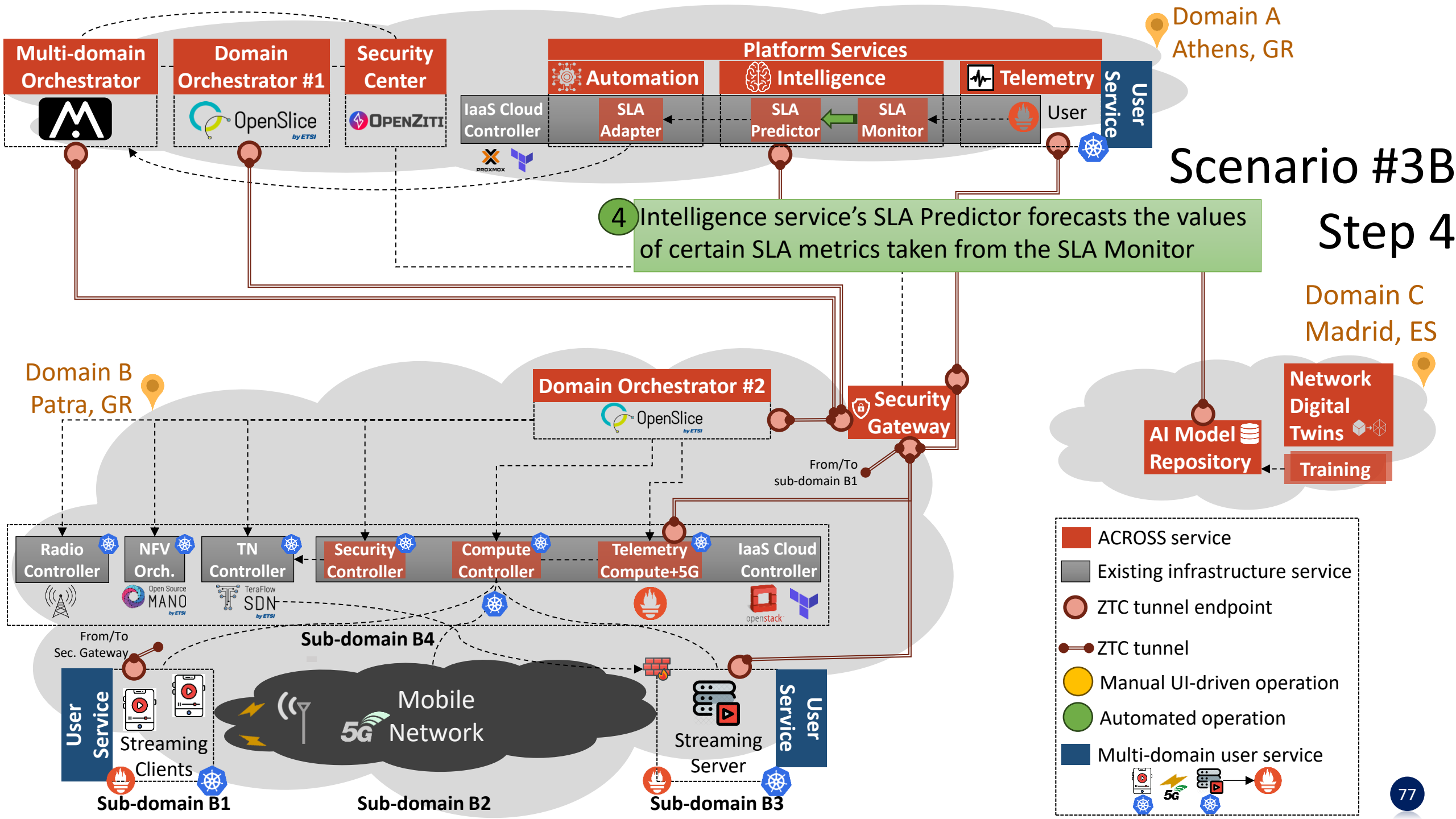
DO supports tight integration with gitops platforms

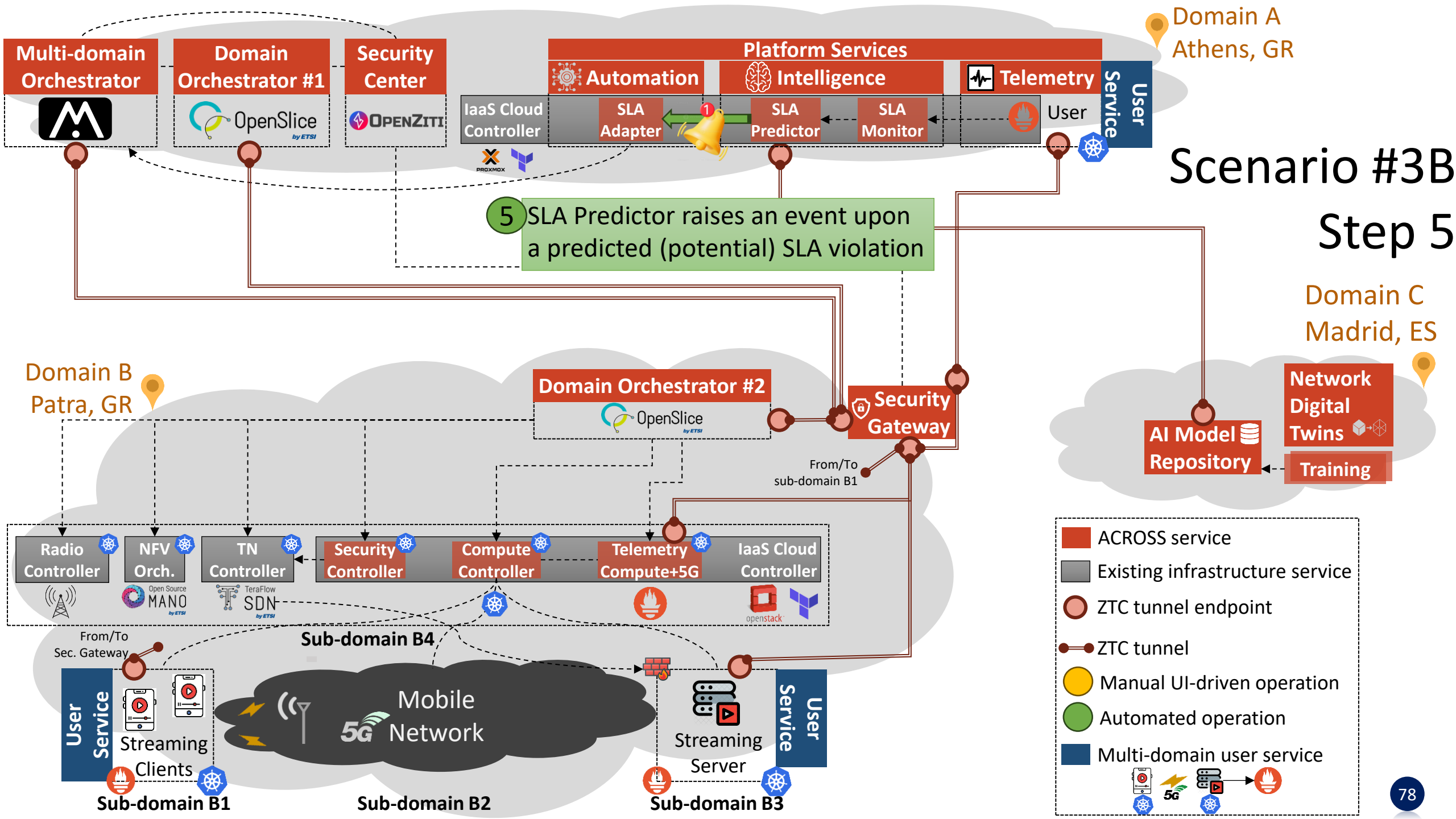


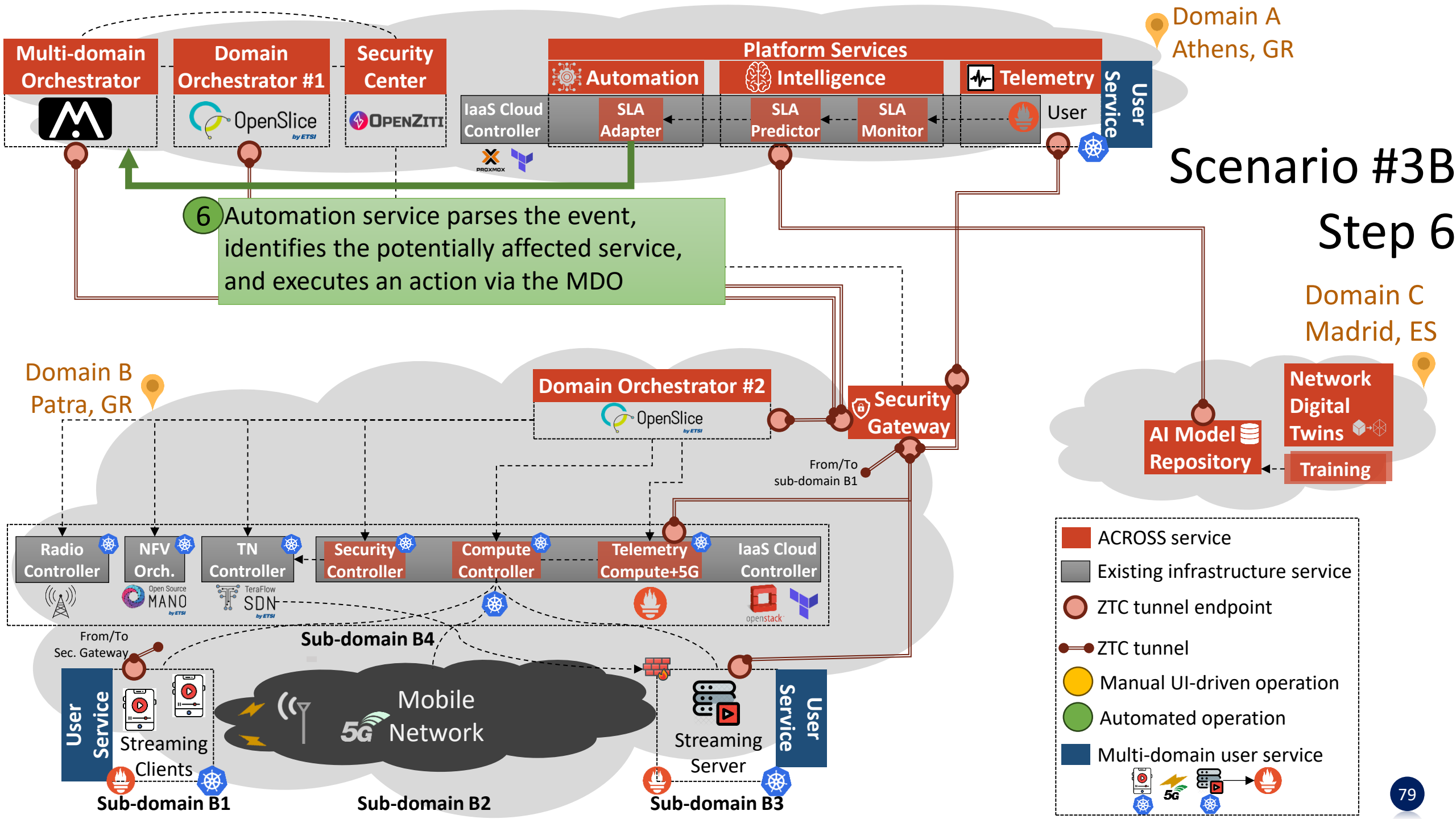


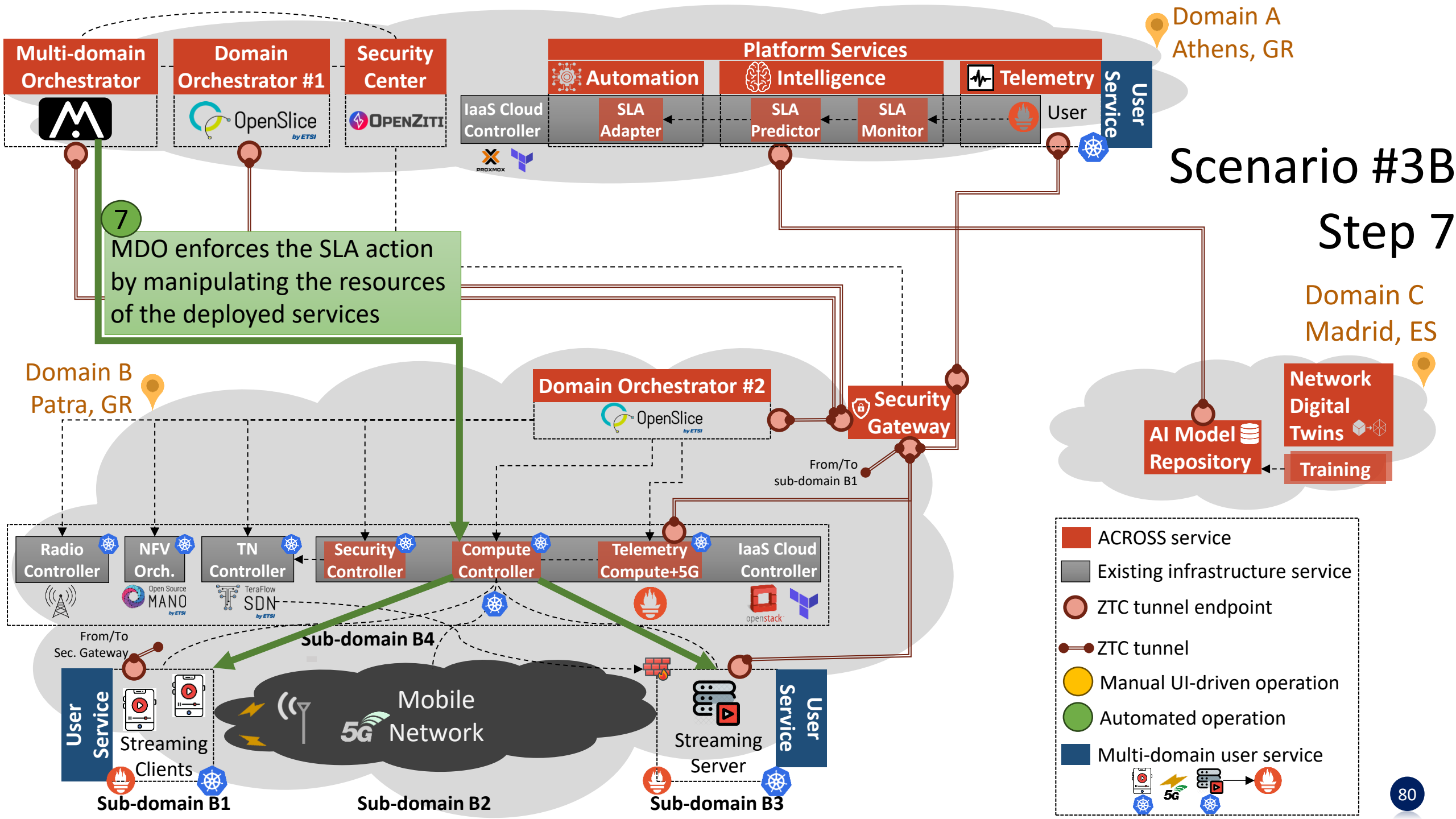




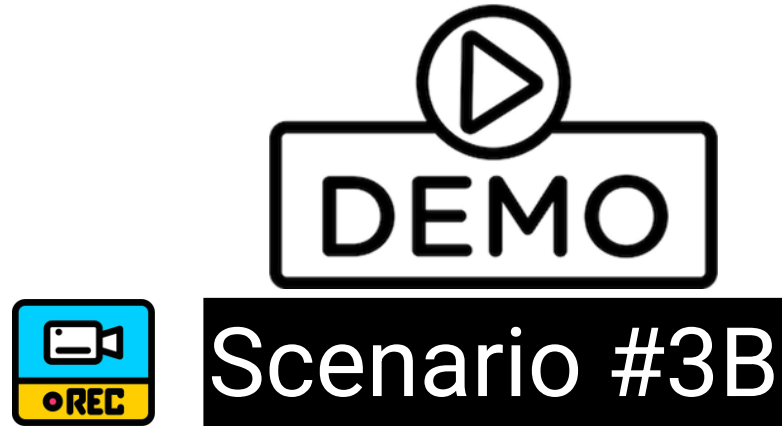








PoC Scenario #3B – Demo time

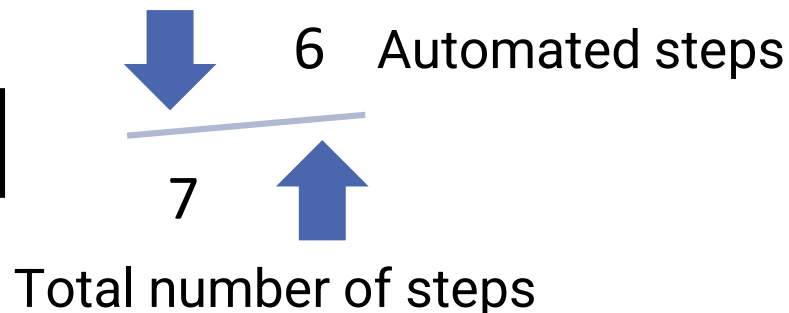


PoC Scenario #3B – Remarks (1/2)

Proactive AI-based SLA preservation using a multi-domain closed loop

- NDT used for (offline) training of a relevant Analytics model
- Intelligence platform service pulls the Analytics model from Domain C
- A real-time Intelligence service predicts violation of certain SLA metrics in Domain A
- Automation integrated with Intelligence platform service to receive SLA violation alerts
- Automation service integrated with MDO to enforce service adaptation upon an alert

Amount of Automation ≈ 86%



PoC Scenario #3B – Remarks (2/2)

Amount of Automation = 100% is possible using gitops, but we opted for an explicit user-triggered SLA request

PoC Findings

Identified gaps in current standards, future work,
and/or other ZSM proposals

PoC – Findings and Potential Gaps

- The Security Center and Security Gateway components of the PoC are fully-aligned with the concept of the ETSI ZSM Integration Fabric as per the **ETSI GS ZSM 002 v1.1.1 (2019-08)**: “Zero-touch network and Service Management (ZSM); Reference Architecture”
 - ➔ The proposed approach goes one step beyond by adding security and trust by design
- The proposed end-to-end (compute, 5G, telemetry, end-user) service provisioning approach is fully aligned with **ETSI GS ZSM 003 v1.1.1 (2021-06)**: “Zero-touch network and Service Management (ZSM); End-to-end management and orchestration of network slicing”
- The proposed NDT environment approach is aligned with **ETSI GS ZSM 018 v1.1.1 (2024-12)**: “Zero-touch network and Service Management (ZSM); Network Digital Twin for enhanced zero-touch network and service management”

PoC – Future Work

- Tighter integration between the orchestration platform and the NDT could be studied



An AI model drift detector could be:

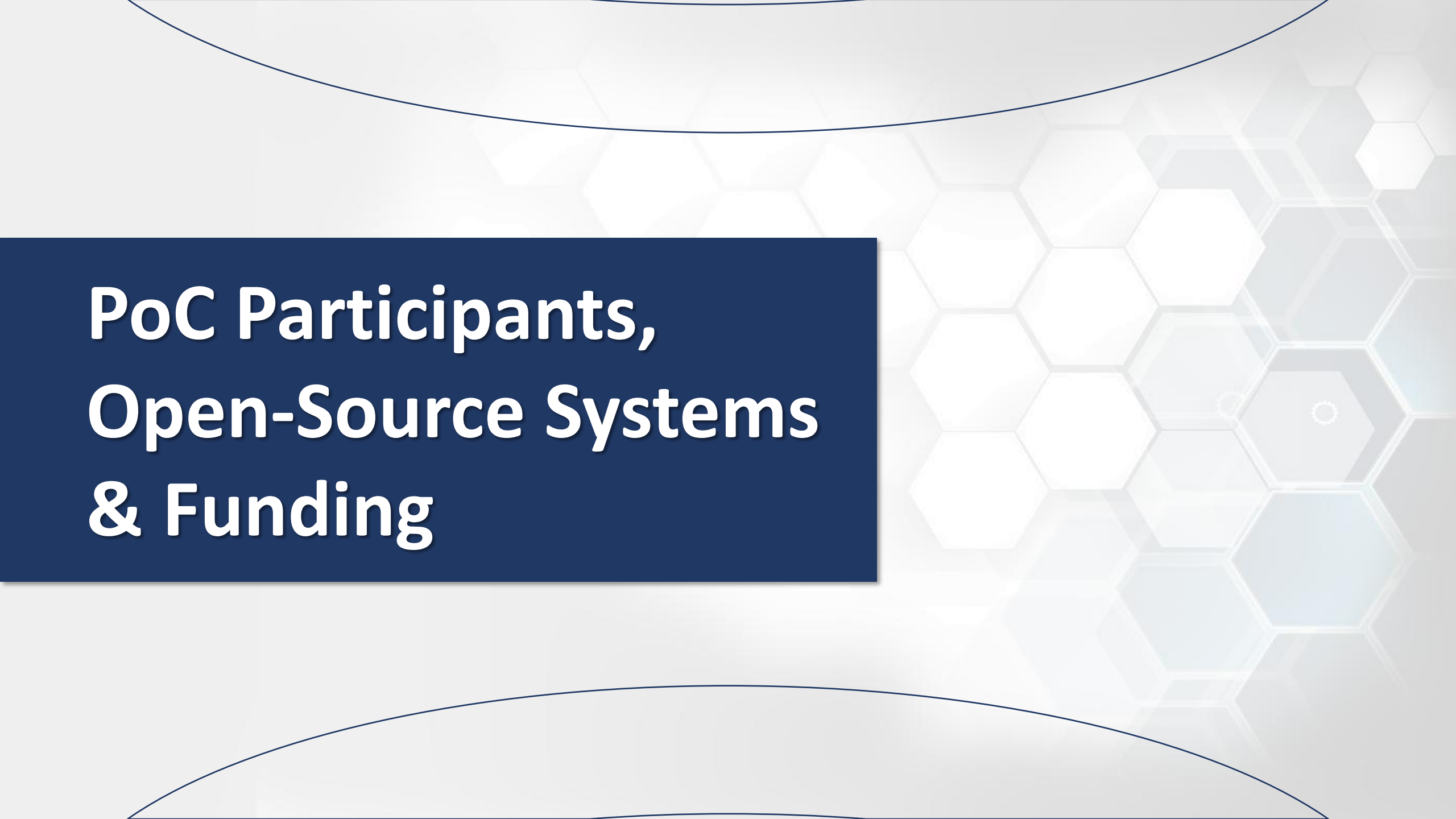
- (a) linked with a real service in a domain via the Secure Integration Fabric
- (b) detect data drift of existing AI models in real-time
- (c) Ask NDT to re-train the model with additional data
- (d) rollout (hot swapping) a new version of the model in the real system for increasing its accuracy

PoC Report

PoC Report Date



To be submitted by November 28, 2025

The background features a light gray hexagonal pattern that becomes more prominent on the right side. Two thin, dark blue curved lines arch over the top and under the bottom of the slide.

PoC Participants, Open-Source Systems & Funding

PoC Participants



PoC – Open-Source Systems and Related Standards

Open-source component



Multi-domain service orchestrator
<https://maestro-mkdocs.readthedocs.io/> (Soon under ETSI OSL)



Operations Support System (OSS) for Network-as-a-Service
<https://osl.etsi.org/>



NFV Orchestrator
<https://osm.etsi.org/>



Disaggregated SDN Controller
<https://tfs.etsi.org/>



Programmable platform for Zero-Trust Networking
<https://openziti.io/>

Partner



*NOVA and UBITECH used OpenZiti, no contribution so far



PoC – Open-Source Systems and Related Standards

Open-source component

Analytics training and inference service for SLA forecasting
(To be released soon)

tmforum

TMF-compliant Automation service for SLA preservation
(To be released soon)

Open Security and Trust Orchestrator (OpenSTO)

<https://github.com/CTTC-PONS/OpenSTO>

Partner



Thank You! Questions?



Across

Automated zero-touch cross-layer provisioning framework for 5G and beyond vertical services



across-web



[@horizon_across](https://twitter.com/horizon_across)



[@across-horizon-europe](https://www.linkedin.com/company/across-horizon-europe)

HORIZON-JU-SNS-2022 **ACROSS** project with GA number 101097122



coppilot

Collaborative Open Platform (COP) for seamless end-to-end orchestration across service domains, fostering a standards-aligned, market-oriented, and cross-sector computing environment



cop-pilot-web



[@cop-pilot-horizon](https://www.linkedin.com/company/cop-pilot-horizon)

HORIZON-CL4-2024-DATA-01-03 **COP-PILOT** project with GA number 101189819