




Get Smart

The Challenges in Data-Driven Network Management

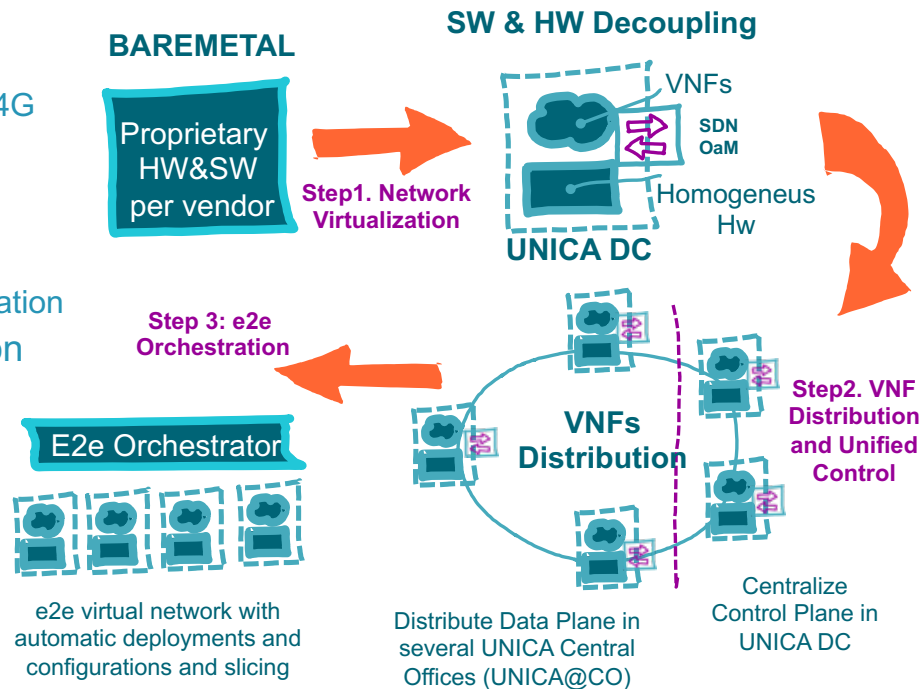


Diego R. López
Telefónica



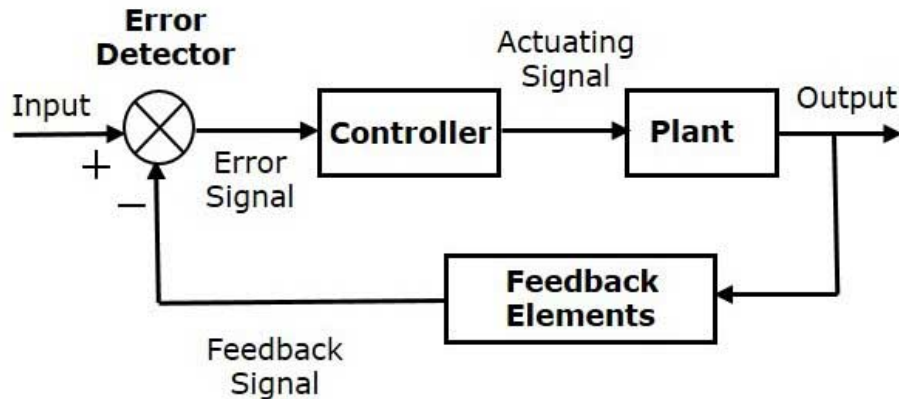
Addressing the Complexity Challenge

- Networks becoming increasingly complex
 - 5G foresees a x10 densification of sites compared to 4G
 - Best user experience demands heterogeneity in access technologies
 - The continuous challenge of centralized proposals, way beyond the usual OTT
 - And not suitable to be managed using traditional operation
- Adapt results from the IT experience in virtualization
 - Acknowledging the differences
 - Topology awareness
 - The conservation principle
 - Openness
 - Integrity and auditability
 - Isolation
 - Exploring new paths
- Towards zero-touch service management



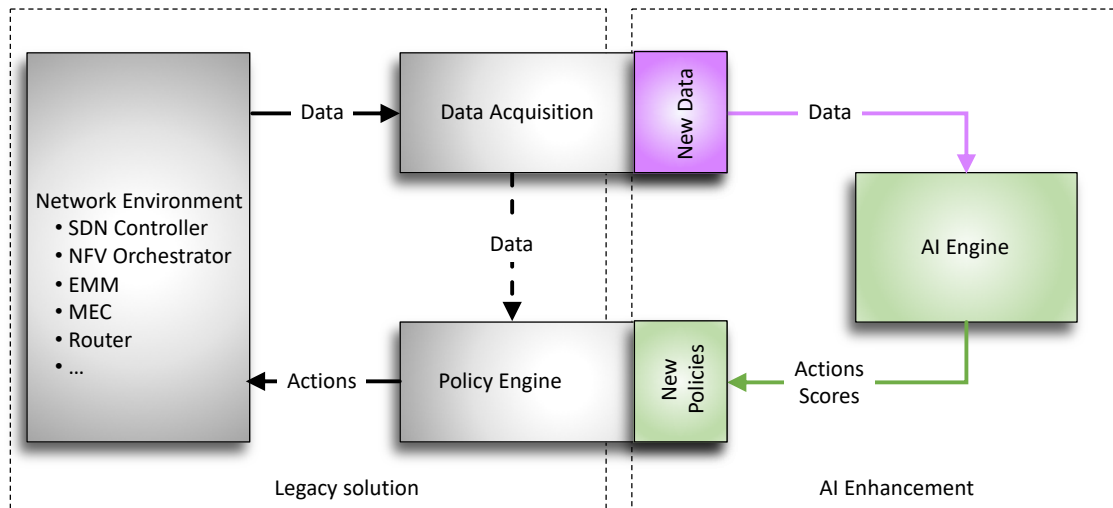
Automatics 101

- The use of closed loops do not imply such a radical change
 - Automatics have been around for a long time
 - An essential aspect of industrial processes
- The native complexity of networks has made more difficult their application
 - Metcalfe's law
 - Laser effects
 - The invariants



- Software network technologies have become an essential enabler
 - Look, there is a *controller*!
- Essential abstractions at all elements
 - Feedback, input, detection, actuation

Smarter Closed Loops

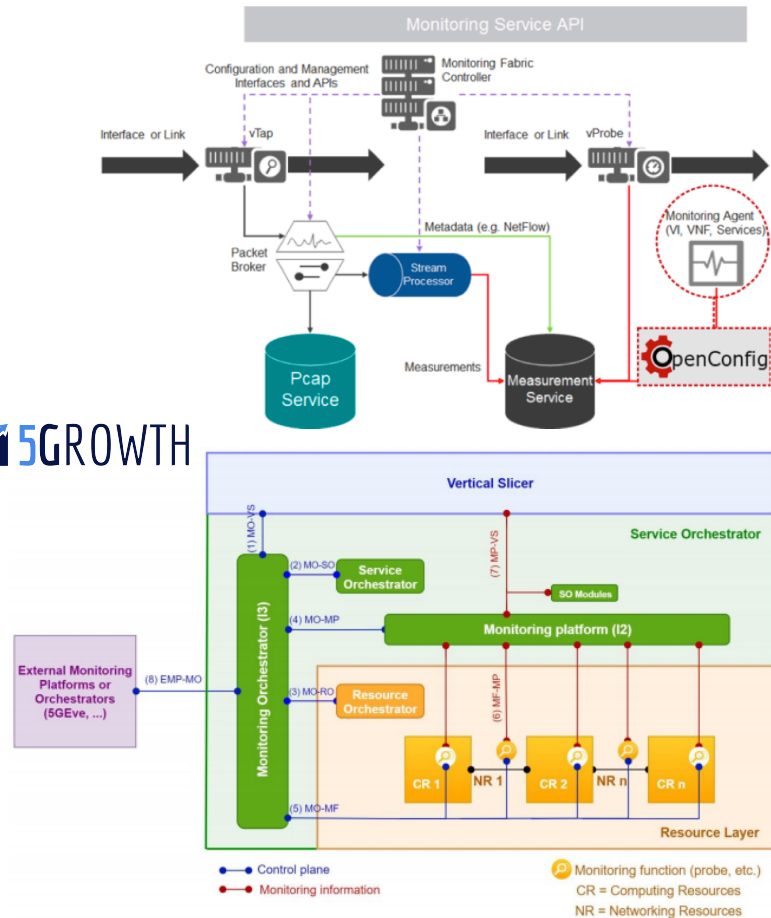


- Not such a radical change
 - Tools to derive further insights from data and improve policies
- Extended capabilities, but do not expect Skynet
- The key issues are not in the engine(s)
 - But in the data and action flows
 - Including distribution and placement of the engine(s)
- And in flow management and application

The Data Stream

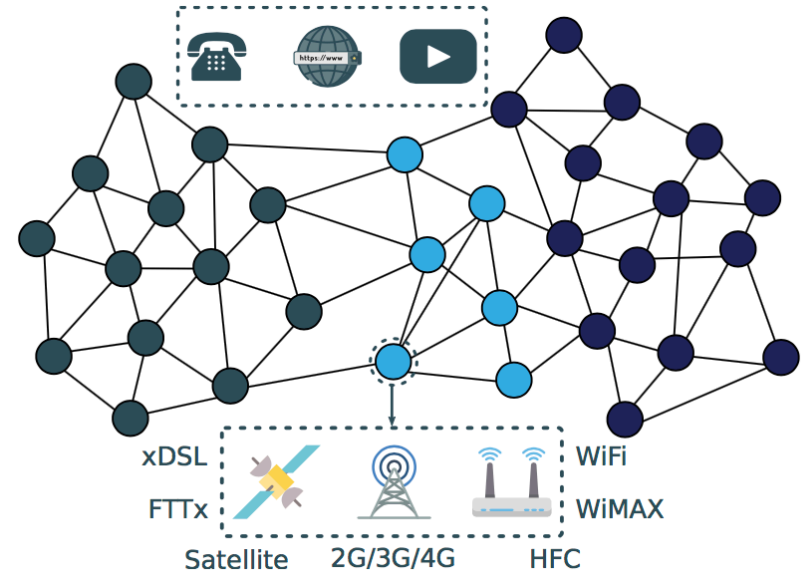
- No matter how intelligent: Crap in means crap out
 - Usable: Adaptation (formats, scales...)
 - Sufficient: Topology (sources, aggregators...)
 - Safe: Provenance (origin, timestamps...)
 - Steady: Continuity (pace, availability...)
- An enhanced data fabric seems the logical approach
 - Supporting resource, orchestration and function sources
 - Combining current network monitoring tools and recent telemetry developments

5G GROWTH



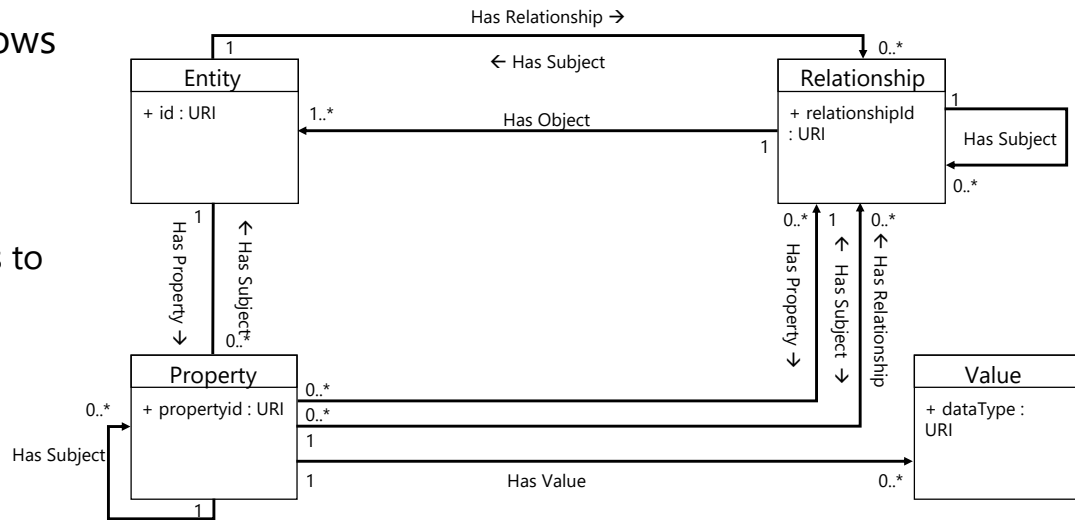
The Data Aggregation Scenario

- Support the integration of different data flows
 - Open
 - Automated
 - Secure
 - Scalable
- Deal with heterogeneity at all levels
 - Data sources
 - Data models
 - Deployment styles
 - Supporting infrastructures
- Not just data
 - Metadata becomes essential, including semantic mappings
 - What seems to claim for a data stream ontology
 - Not that far away: data modeling is a first step



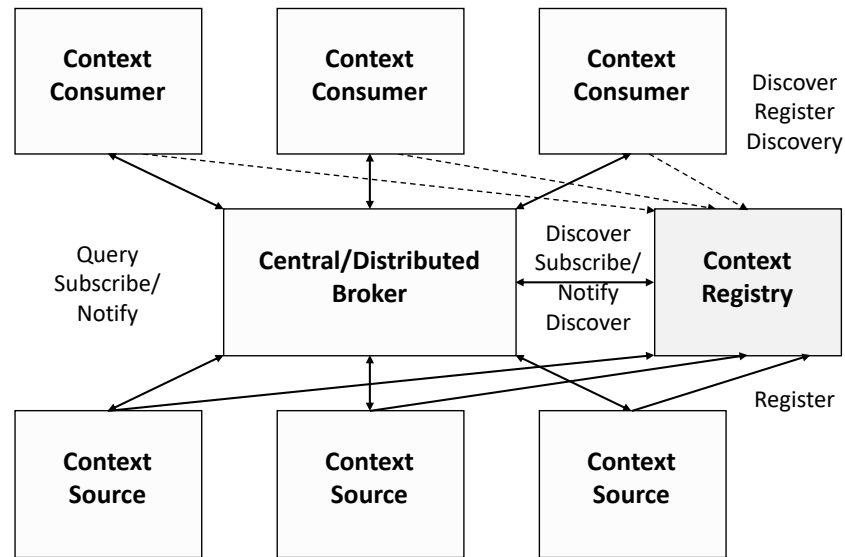
Applying a Semantic Model

- Use the model to describe data flows
 - Sources
 - Consumers
 - Elements in the flow
- And including
 - The identification of the relationships to the flow data model
 - Provenance metadata
 - Security
- Note we are not talking about modeling the whole systems
 - Only the data they provide and/or consume
 - Usable to analyze and normalize flows
 - Without the need of explicit standard alignment
- Extend descriptors
 - Include a protocol for registration, announcements, discovery, etc.

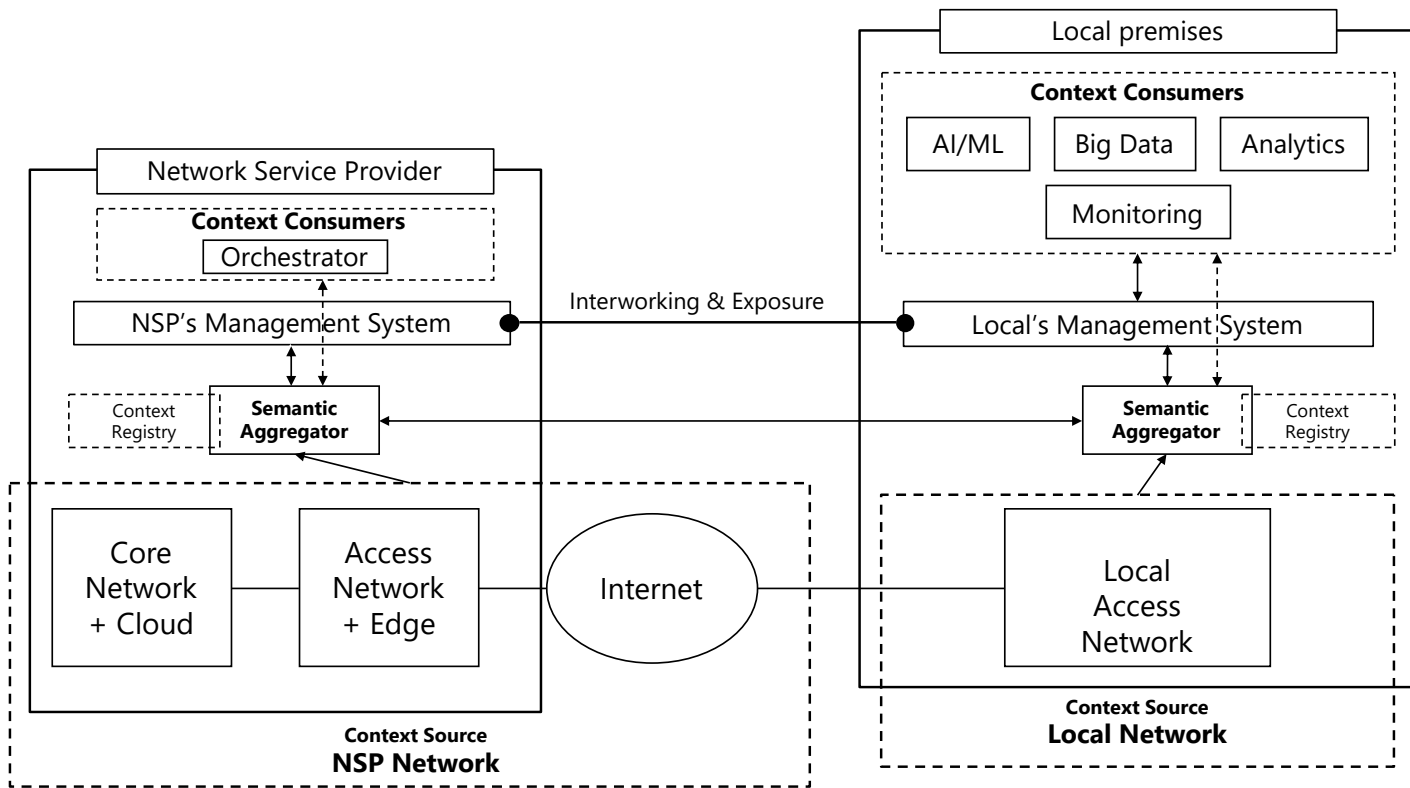


Using CIM

- Focused on mechanisms to deal with context information from many different sources
 - Sharing that information through interoperable data publication platforms.
 - Agnostic to the architecture of the applications sharing information
 - Based on an information model describing entities and relationships
- Originally focused on IoT scenarios
 - Suitable for adaptation to other ones

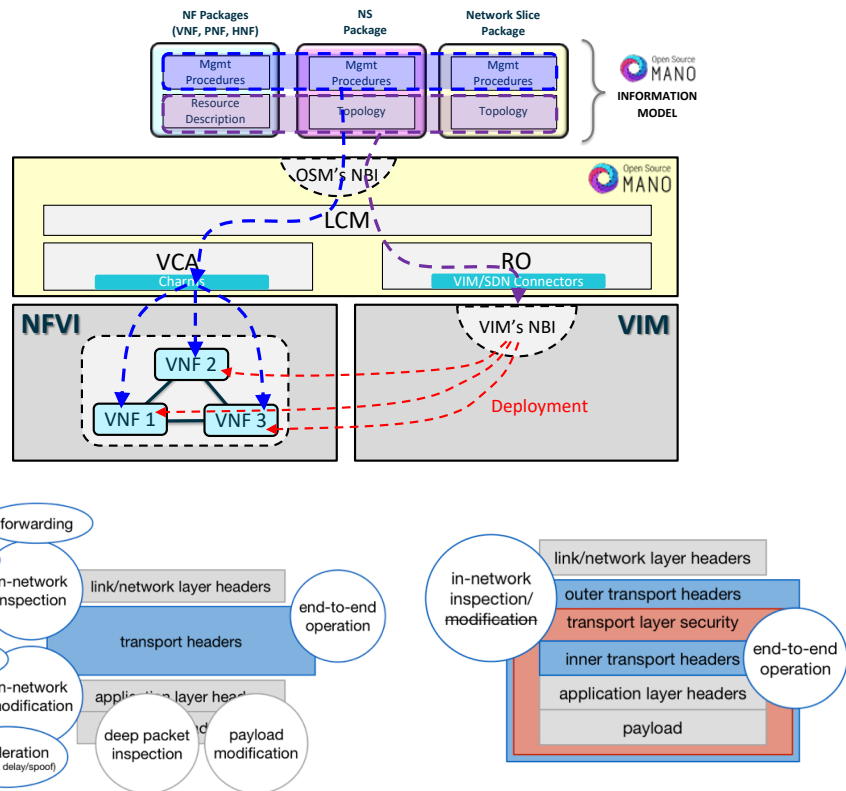


Supporting Federated Models



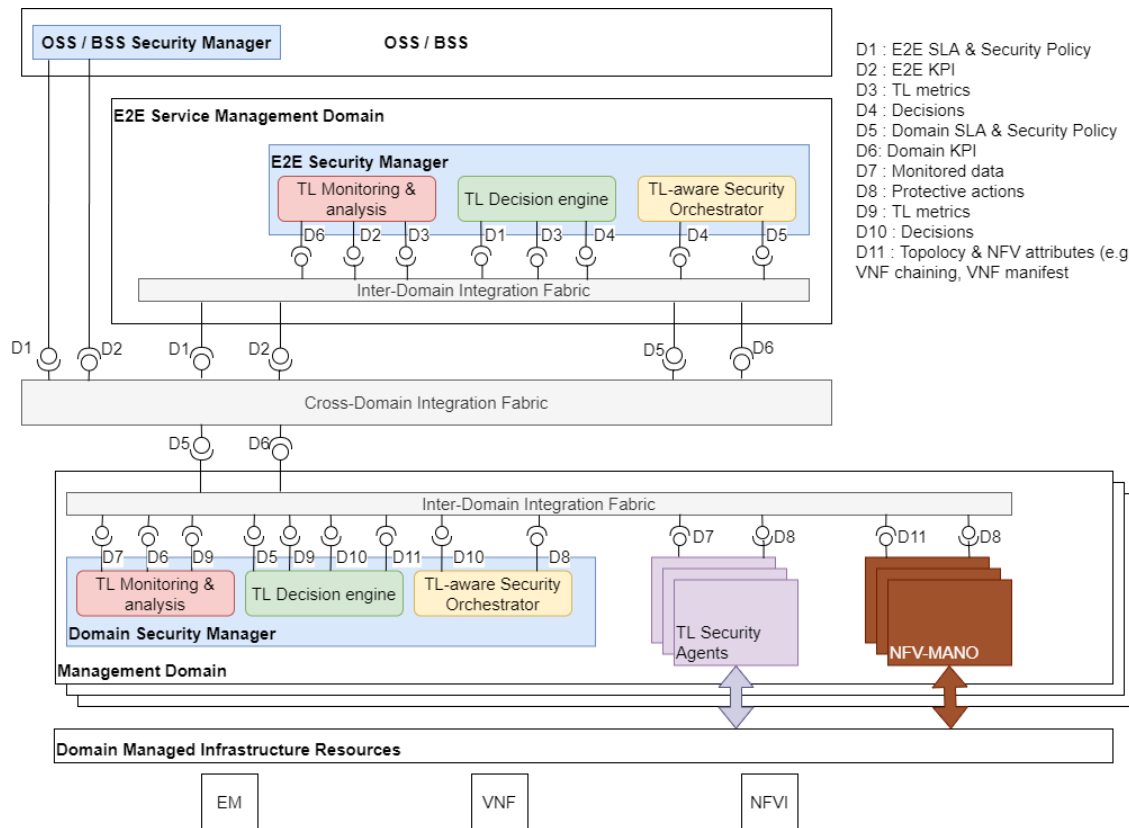
The Action Stream

- OAM actions at a wide variety of different domains
 - Challenging, given the current state-of-the-art
- Initial strategies
 - Domain specific
 - Recommendation systems
 - Autonomic protocols
- SBA approaches and capability models
 - Reusable functionality description
 - Abstractions of network element functionalities usable as building blocks
 - Combined to provide more powerful features
 - Registration mechanisms to support CI/CD
 - Inter-domain collaboration for E2E management



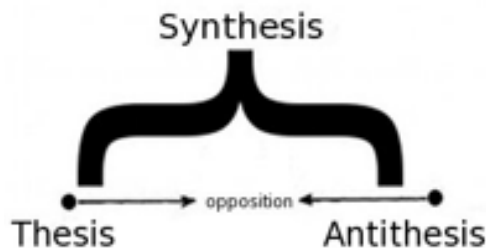
Multi-Domain Capability-Based Security

- ▶ Each domain exposes a series of capabilities
- ▶ Consumed by other domains
 - ➔ Including the E2E layer
- ▶ More a *choreography* than an *orchestration*
 - ➔ More on this later, in connection with architecture issues
- ▶ Emerging standards
 - ➔ ETSI NFV SEC architecture
 - ➔ ETSI ZSM framework
 - ➔ IETF I2NSF models



The Process in the Loop

- The dialectic way
 - Thesis: Translate intent into action
 - Understanding intent statements
 - Mapping onto technologies
 - Antithesis: Support environment constraints
 - Policies provided by network management
 - The archetypal SLA enforcement
 - Synthesis: Conflict resolution
 - Among action requests
 - And with management constraints

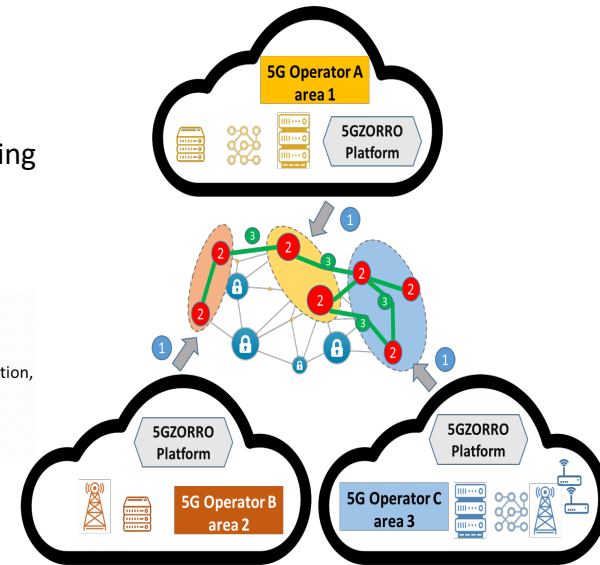


- Audit track and intelligibility
 - The who, the what, the when
 - And the why
- And security
 - Deal with adversarial AIs
 - And consider circuit breakers

Trusted Data in Support of Intent

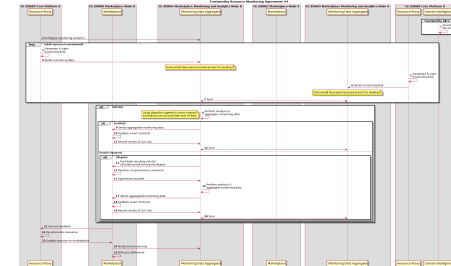
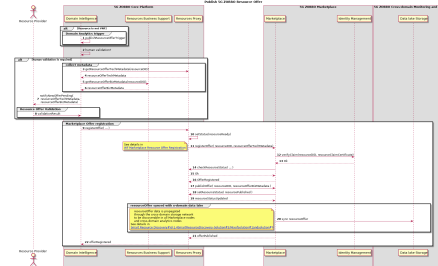
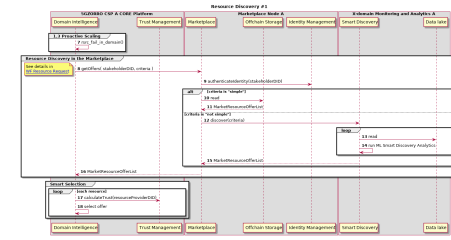
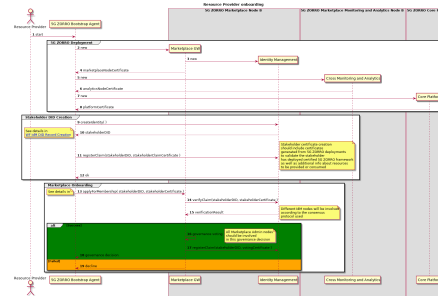
- *A common platform available at each participating domain*
 - Based on service meshes for elasticity
 - Operational data lakes for service discovery, brokering and SLA monitoring
 - DLTs and Smart Contracts for auditability, licensing and disintermediated trading
 - Trusted Execution Environment to support trust without privacy loss
- *An intent-based API*
 - For interacting with the platform
 - Available to all stakeholders: users and/or providers
 - Dynamic composition of resources

- 1 Zero Touch Resource Discovery using DLT/BC
- 2 Intelligent 3rd party resource selection, request and access/usage
- 3 Trust establishment among multi-parties



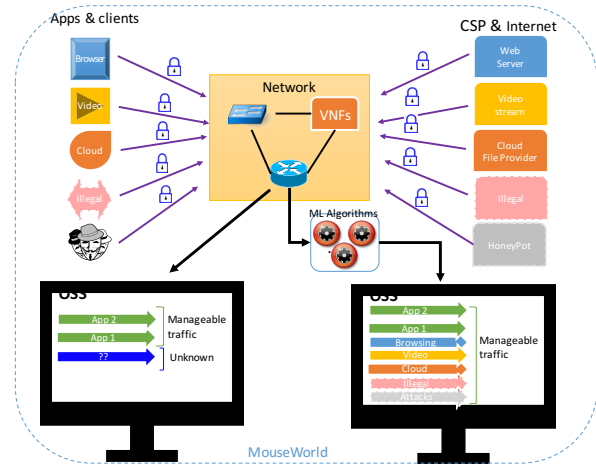
Smart Lifecycle Management

- *Support for resource lifecycle*
 - Of any nature: IaaS, FaaS, PaaS...
- *Providers publish offers*
 - Once they are *onboarded* and enrolled in the trust fabric
- *Consumers discover and select offers*
 - Satisfying their intent expressions
 - Based on trust evaluation
- *Both establish agreements and monitor performance*
 - Enforceable
 - Auditable
 - Privacy-preserving
 - Elastic

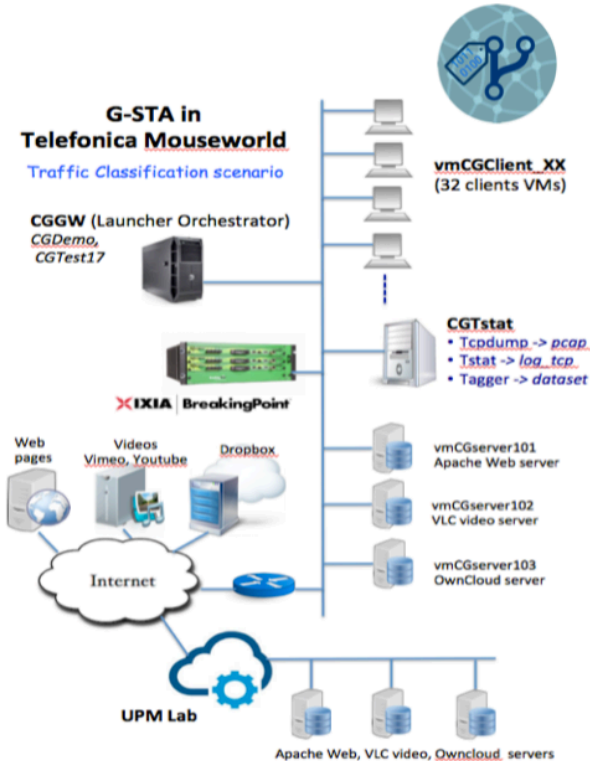


Trustworthy Datasets

- A serious lack of usable datasets
 - For training or validation
 - Data as an asset
 - Privacy concerns
 - None or limited tagging
- Generation of synthetic datasets
 - Traffic samples generated in a controlled way
 - Configurable mixes of synthetic and real traffic
- And metadata management
 - Different scenarios, from high loads to security threats
 - Training and validation loops
- Relying on Software Network principles
 - Repeatability and reproducibility
 - Controlled variations



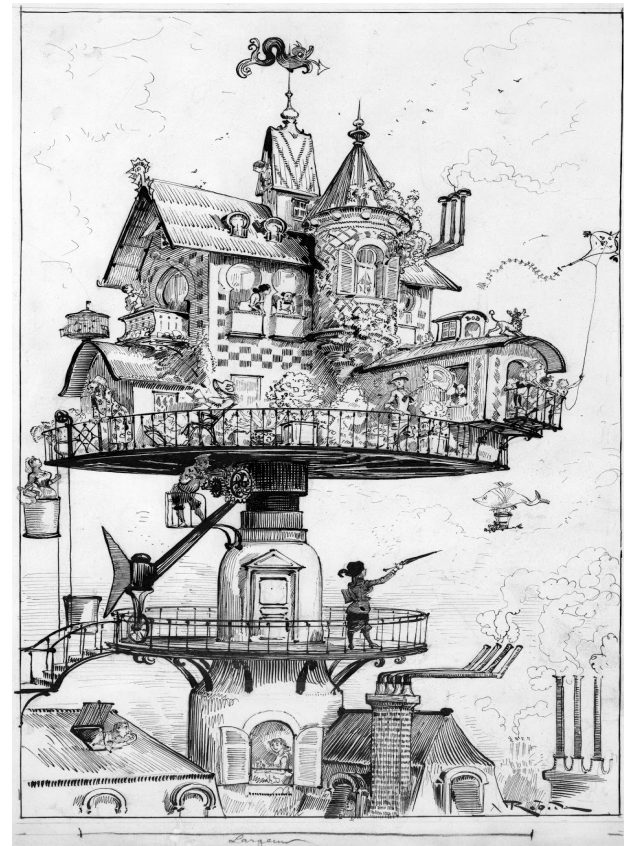
The *Mouseworld* – Synthetic Traffic and Beyond



- ▶ Traffic at all network segments
- ▶ Clients, servers, middleboxes and network functions of many natures
 - ➔ Plus raw traffic captures and other external sources
- ▶ Traffic analysis to produce (labelled) datasets
 - ➔ NetFlow
 - ➔ IPfix standard
 - ➔ TStat
- ▶ Train and validate
 - ➔ ML solutions, supervised and unsupervised
 - ➔ Data-driven modules (AI, Analytics...)
- ▶ Repeatable and controlled conditions and variants
 - ➔ SDN/NFV based architecture

A Matter of Balance

- Network heterogeneous and distributed nature **with**
A holistic view of services and infrastructure
 - Topologies, protocols and models for distributed AI elements
- User requirements **with**
Operational policies
 - Intent dialectics and elastic policy enforcement
 - Compositional mechanisms to combine requests in multi-tenant environments
- Regulatory matters **with**
Security
 - Data sovereignty and identity management for all entities
 - Non-repudiation and accountability
- Closed loop operation **with**
Infrastructure criticality
 - Keep humans in the loop, retaining ultimate understanding and control
 - AI intelligibility and security mechanisms to guarantee proper operation
- Sensing **with**
Acting
 - Open and extensible mechanisms for data and action streams
 - Converged data models for definition and monitoring
 - Converged control action representations



Get the Future Now



5G PPP
PUBLIC-PRIVATE PARTNERSHIP



The research conducted by INSPIRE-5Gplus receives funding from the European Commission H2020 programme under Grant Agreement N° 871808. The European Commission has no responsibility for the content of this presentation.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 856709.

#RECONNECTA

Telefonica