6G SERIES WORKSHOP BY HEXA-X-II

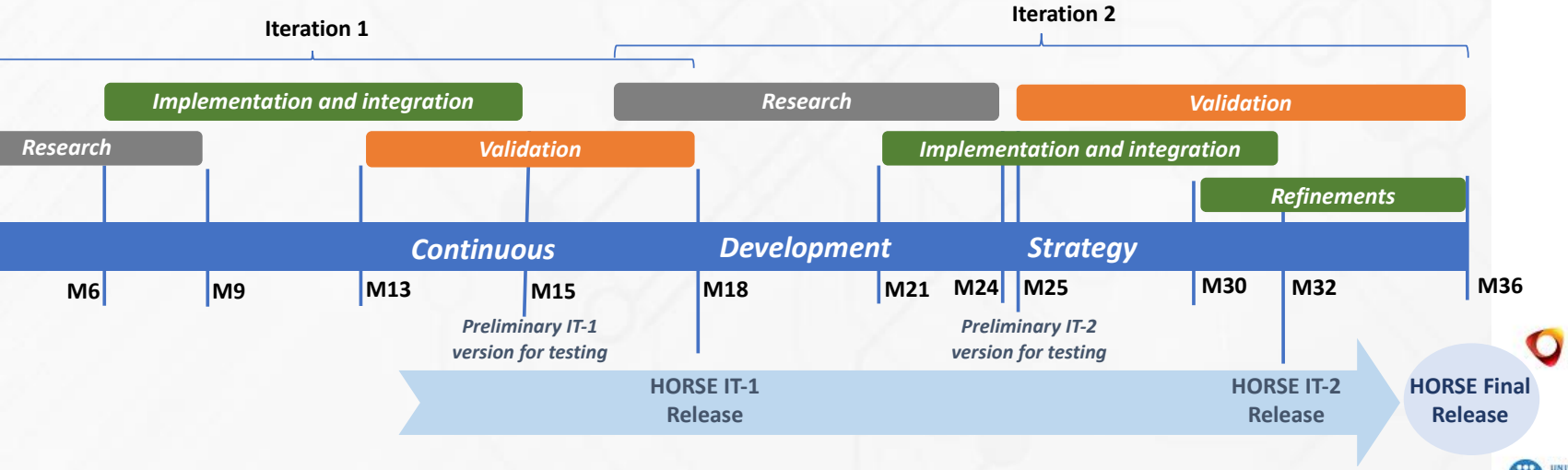
Josep Martrat – ATOS/EVIDEN

February 14th on-line

HORSE OVERVIEW

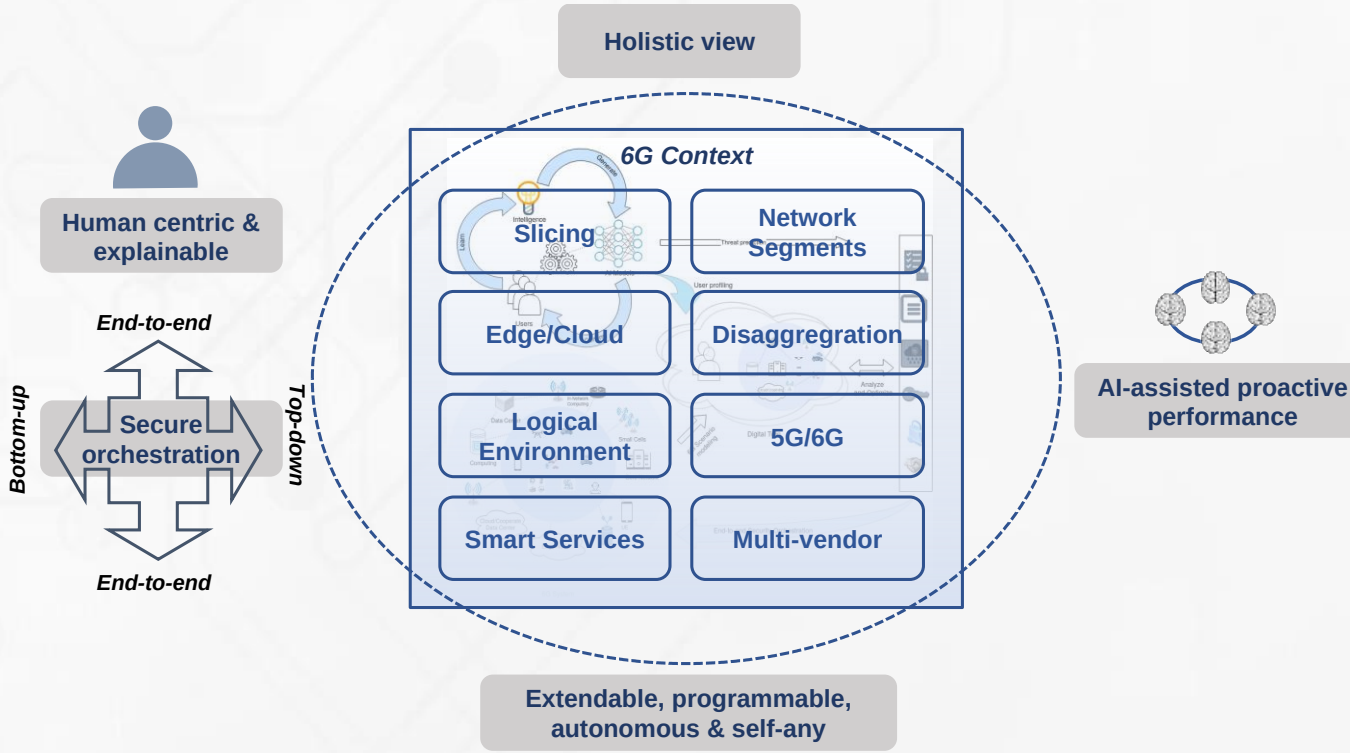
Holistic, Omnipresent, Resilient Services for Future 6G Wireless and Computing Ecosystems

- HORSE addresses challenge towards **6G infrastructure operation for smart connectivity and service management**, including **security workflows** showing its effectiveness at the intersection of 6G connectivity, computing infrastructure management and security.
- HORSE include predictive threats detection and impact analysis, proactive business-wise threats and breaches mitigation actions, programmable networking, use of network digital twins (NDT) with Network Function Virtualisation, intent-based networking, AI-based techniques, in-network computing, and cross-layer management as they emerge in the 6G realm.



PROJECT CHALLENGES

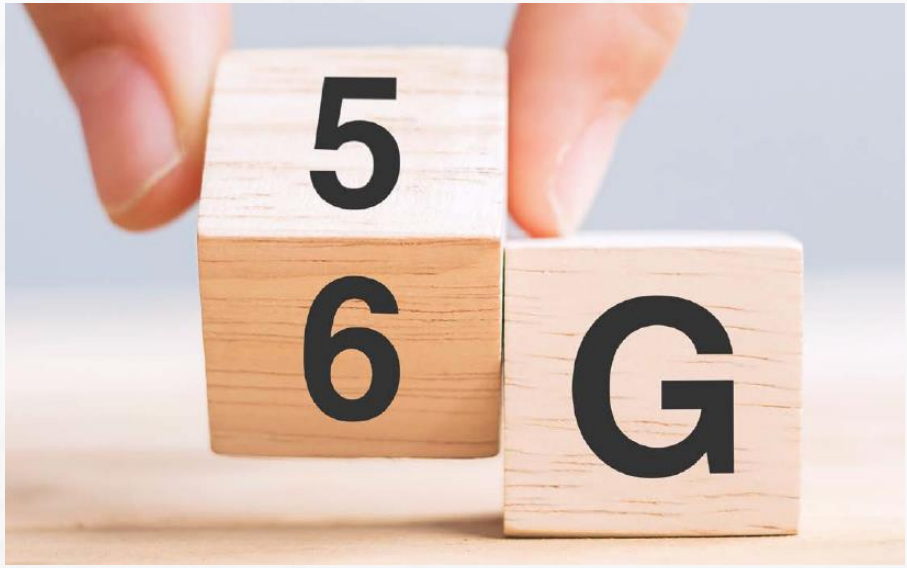
1. Creating a holistic vision of the dynamically evolving 6G system- 6G UCs
2. Orchestrating top-down, bottom-up, and designing end-to-end security solutions
3. Providing a human-centric approach to security workflows
4. Engineering the system to be able to predict failures and attacks
5. Designing the system to self-evolve, be autonomous, and extendable



SOME TRENDS TO FUTURE 6G SYSTEMS

biased list*

- Complete network virtualisation
- Disaggregation with a ‘cloud-native’ approach
- Multi-vendor situation, multi-domain and at scale
- Heterogeneous resources, inclusion of far edge and extensive MEC usage
- Network openness & exposure APIs for 3rd party
- Increase penetration of NPN



- Intelligent, predictive, AI adoption for
  - network self management and more autonomous. Secure lifecycle management
  - security threat analysis and reaction. Trustworthy net, security composition

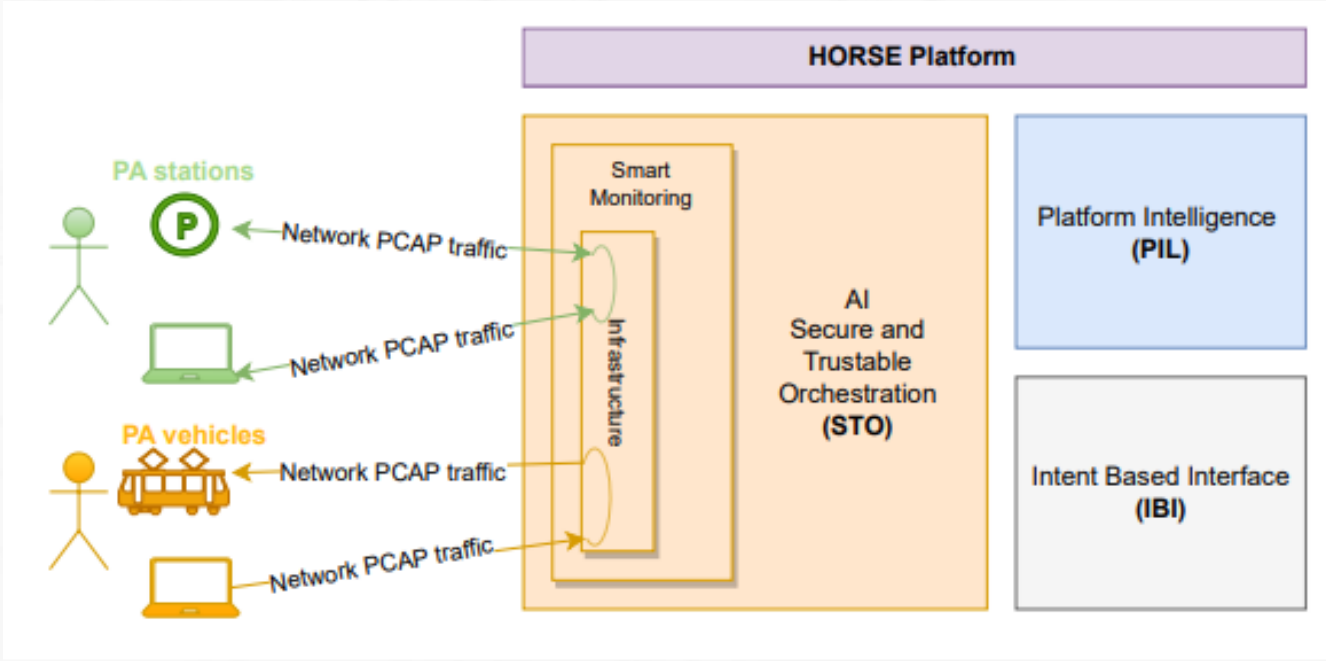
*not included decarbonisation & sustainability goals, new radio, NTN integration, etc

PILOT1 - LIGHT RAIL/URBAN METRO CASE

- use case requires and combines many radio access technologies on the city, metro/tram stations, and depending on the service type ultra-reliable and stable coverage and connectivity, ultra-low latency
- Critical data signalling/control operation
- On-boarded (CCTV) video cameras
- Move Legacy e.g. GSM-R to FRMCS
- Others; PID station & trains, ticketing

Requires PN and NPN combinations

Require multiple RATs, non-3GPPP networks, etc



PILOT2 - INDUSTRIAL XR DESIGN&PRODUCTION CASE

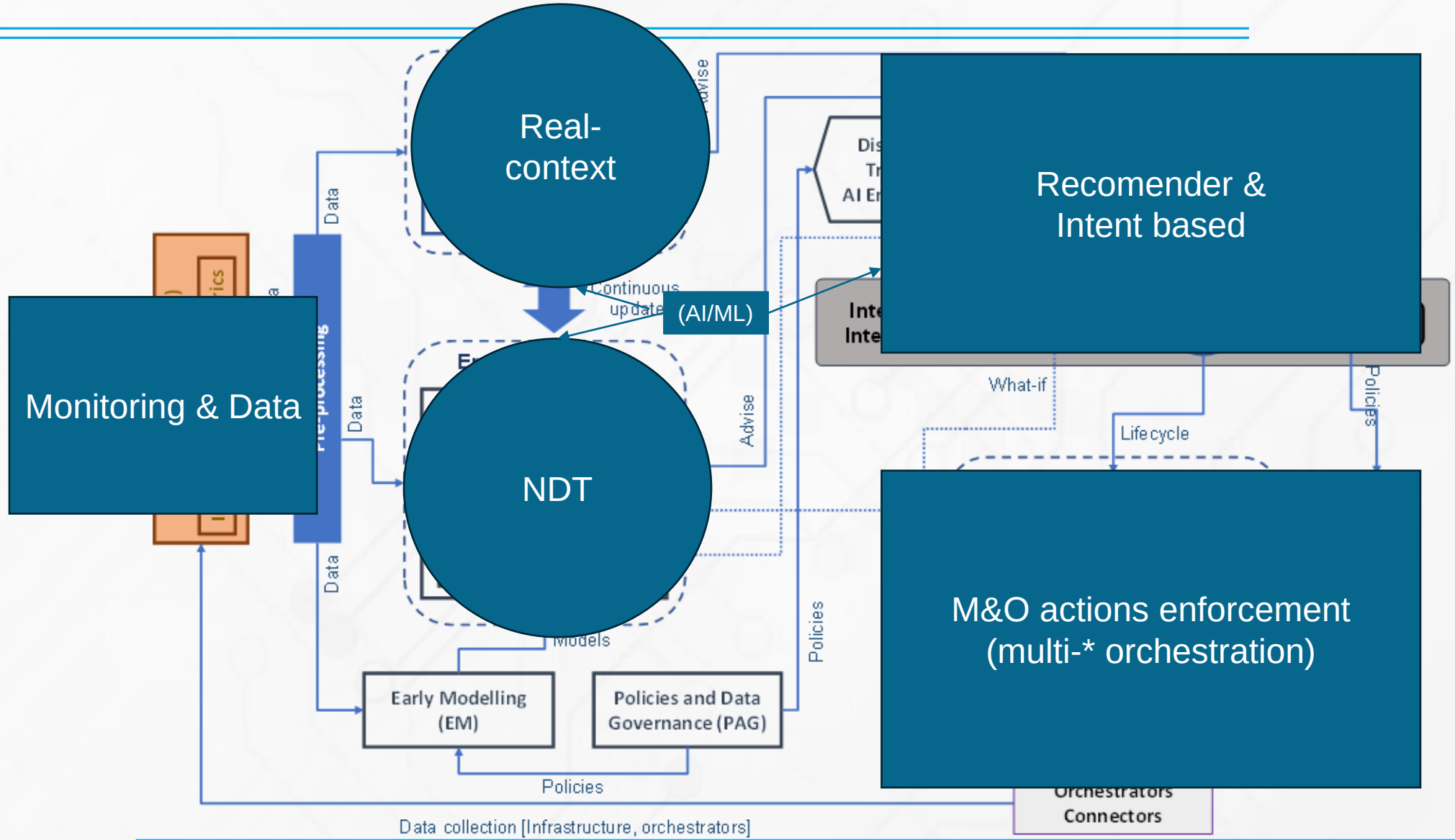
- use case require many wireless connections on the factory floor, ultra-reliable and stable coverage and connectivity, ultra-low latency, and excellent data rates on both the downlink and the uplink with multi-user collaborative mobility
- Evolution study of XR & webRTC

Use Case	Key Requirements
Motion control	Very low latency, high service availability
Control-to-control communications	Very low latency, integrity, service availability
Mobile control panels with functional safety applications	Short bursts of data, periodic and deterministic
Massive wireless sensors and control-to-sensor/actuator communications	Low volume bursts of data, low power utilization, very low latency
Mobile robots and AGVs	Low latency, accurate positioning, high data throughput
Remote access and maintenance	High availability, small bursts of data
Closed-loop process control	Very low latency, high service availability, determinism
Process monitoring	Very low latency, integrity, service availability
Plant asset management	Positioning, service availability
Augmented reality	High data throughput, low latency

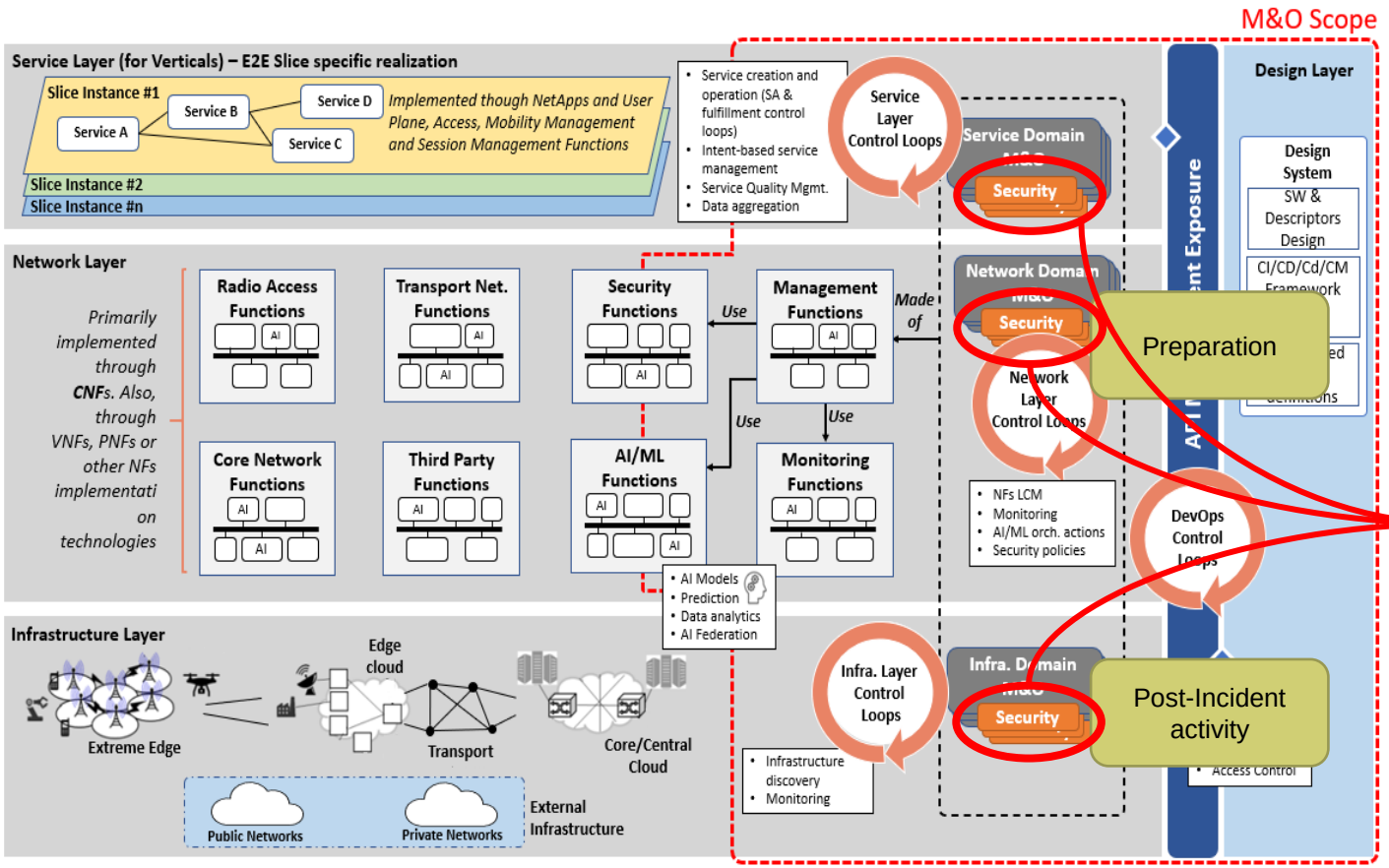
KPIs to Assure
QoS: Throughput, latency, bit error rate
Dependability: Service availability/reliability
RF coverage and quality
Interference and jamming
Interworking with current technologies; TSN integration
Security
Positioning accuracy
Power efficiency

5G-ACIA's Role in Defining Industry 4.0 Use Cases

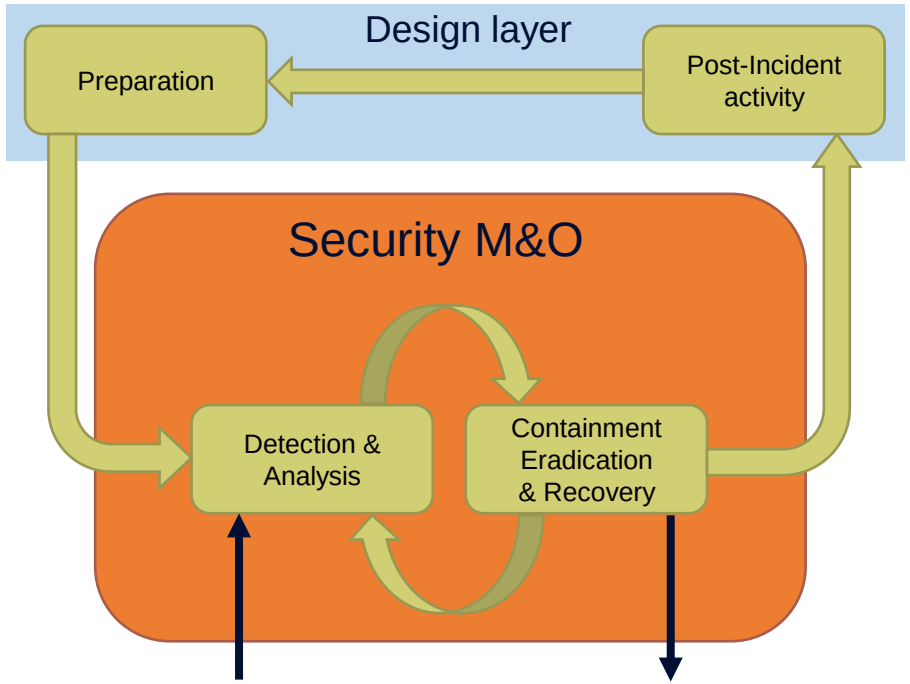
SIMPLIFIED HORSE ARCHITECTURE



M&O Considerations



from Hexa-X Deliverable D6.2, “Design of service management and orchestration functionalities”



Inputs: data from
- Running service
- Layer N-1 M&O Security
- Layer N+1 M&O Security
- Other (e.g.: human input)

Outputs
- Configuration of managed service
- LCM actions of managed service
- Delegation to N-1 M&O security
- Escalation to N+1 M&O security
- Escalation to human admin

- M&O architecture is ready to handle security requirements
- Cybersecurity guidelines can be applied through this architecture to enhance security
- The architecture allows the automation of security processes to improve efficiency

WHAT ARE THE CASES FOR THE ENABLERS?

- DDoS attack from a **far_edge** groups over DNS element, issue on general control plane
- DoS **signaling** attack in nGCore from SMF / UPF (PFCP traffic), impacting on data plane & **slicing**
- **Openness** API vulnerability protection – e.g. RNAA attack (Resource owner-aware Northbound API Access). E.g. NEF expose the 3GPP network capabilities via APIs
- Poison **dataset attack used for AI** to make decisions or analytics in management functions

- ✓ Prediction and prevention of security threats
- ✓ For each attack; module affected and analysis of mitigation actions
- ✓ Analysis of «what-if» scenarios to support autonomous decision-making

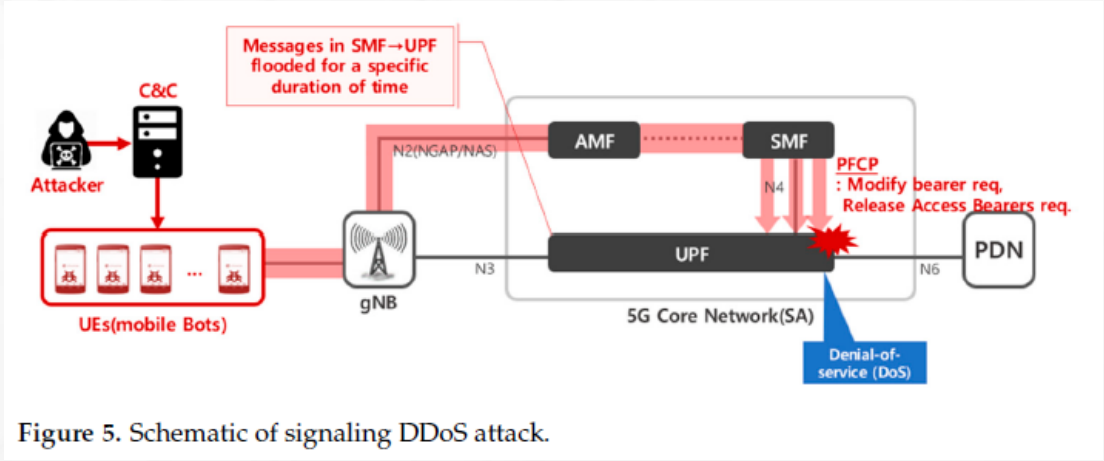
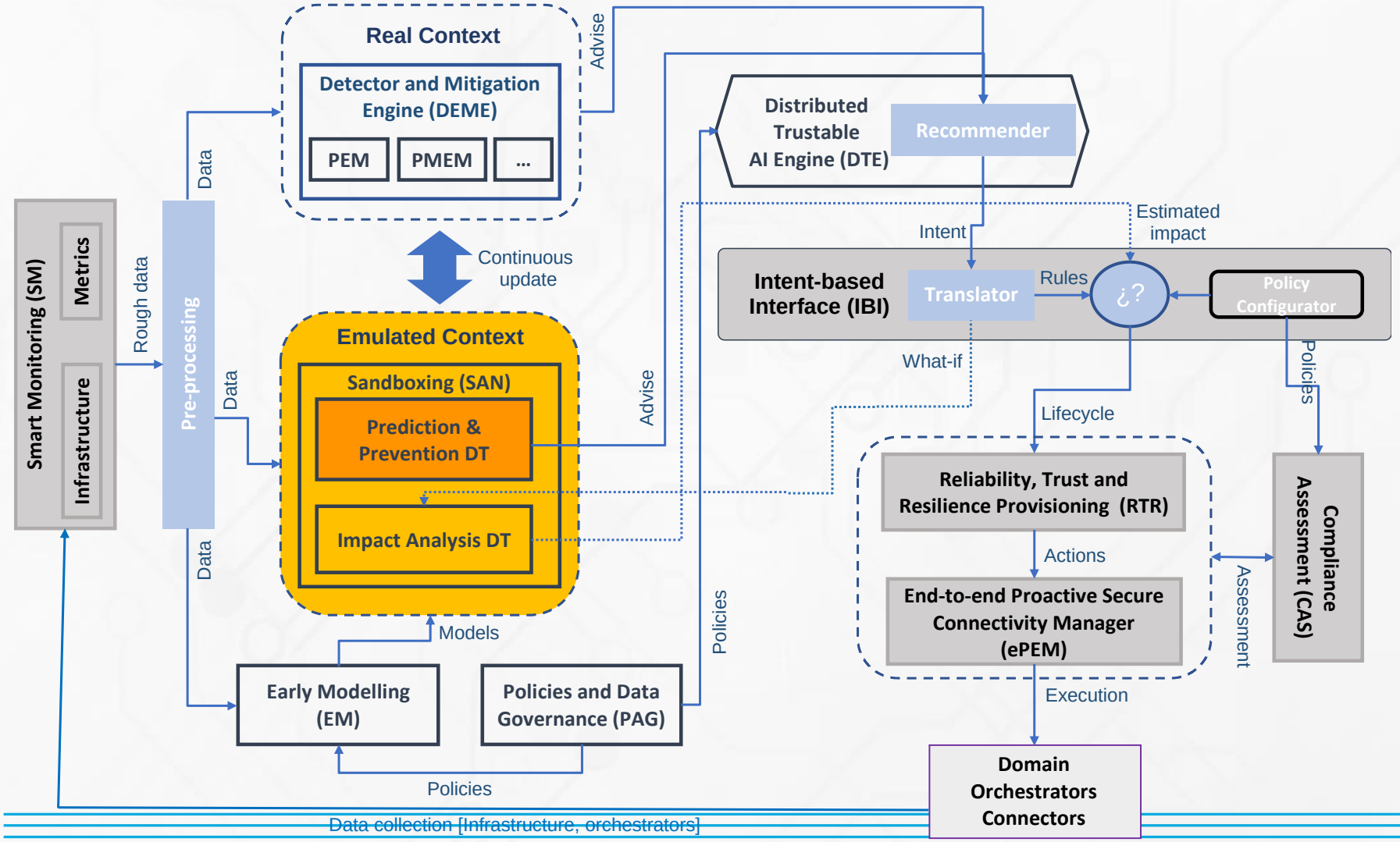


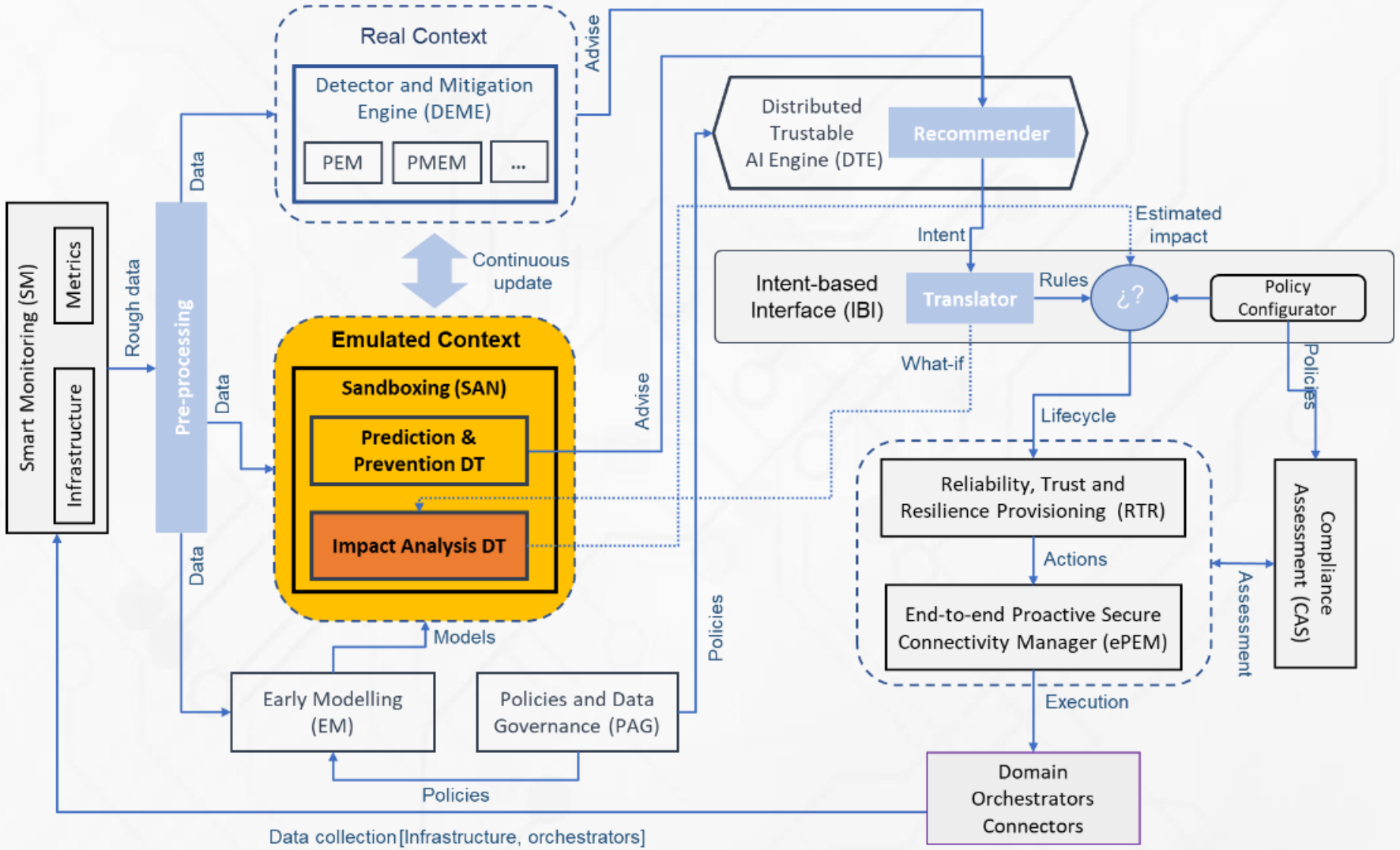
Figure 5. Schematic of signaling DDoS attack.

PREDICTION AND PREVENTION DIGITAL TWIN

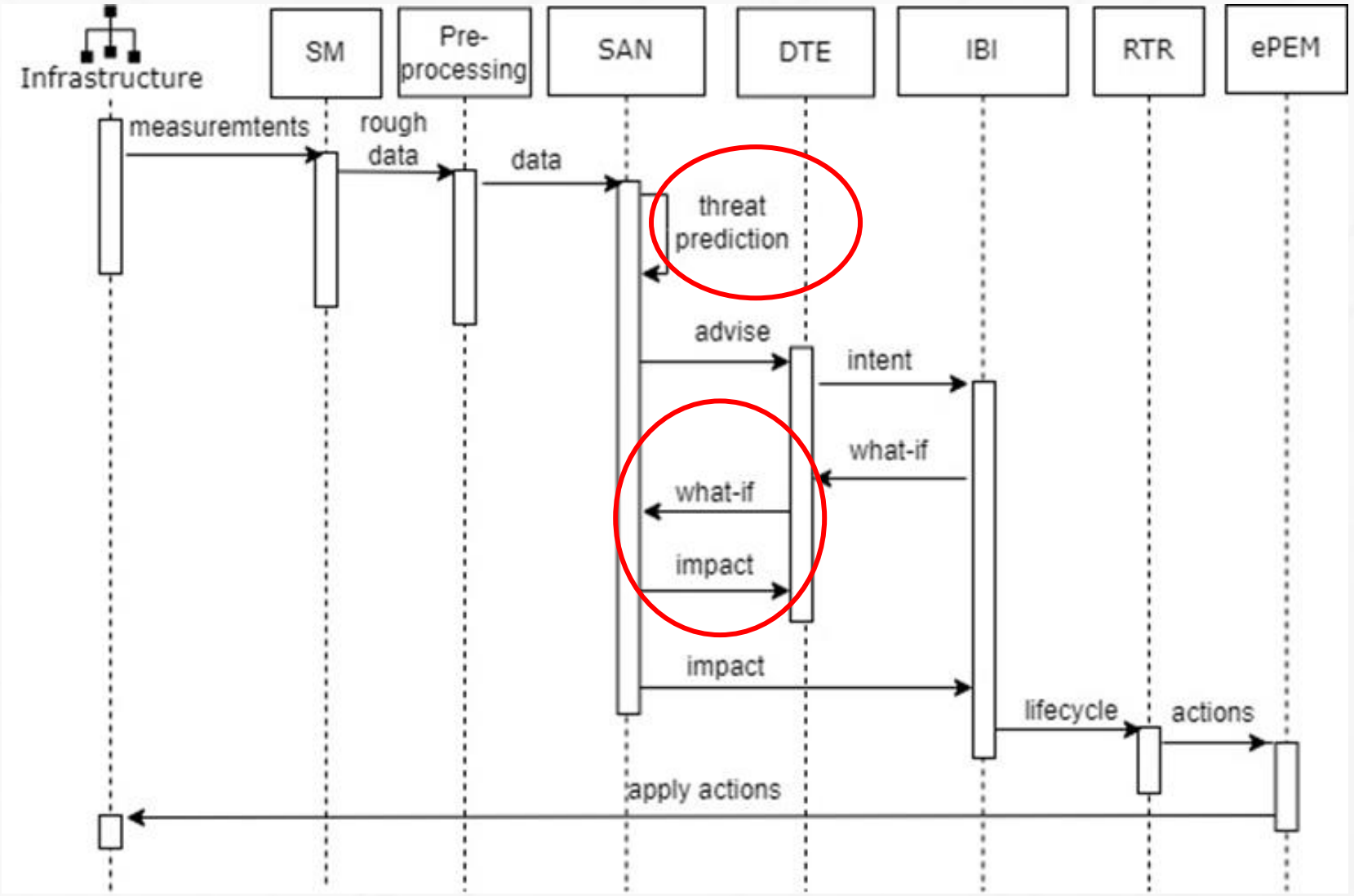
Secure M&O: Digital Twins for prediction & Prevention and «what-if» + Intent-Based Interface



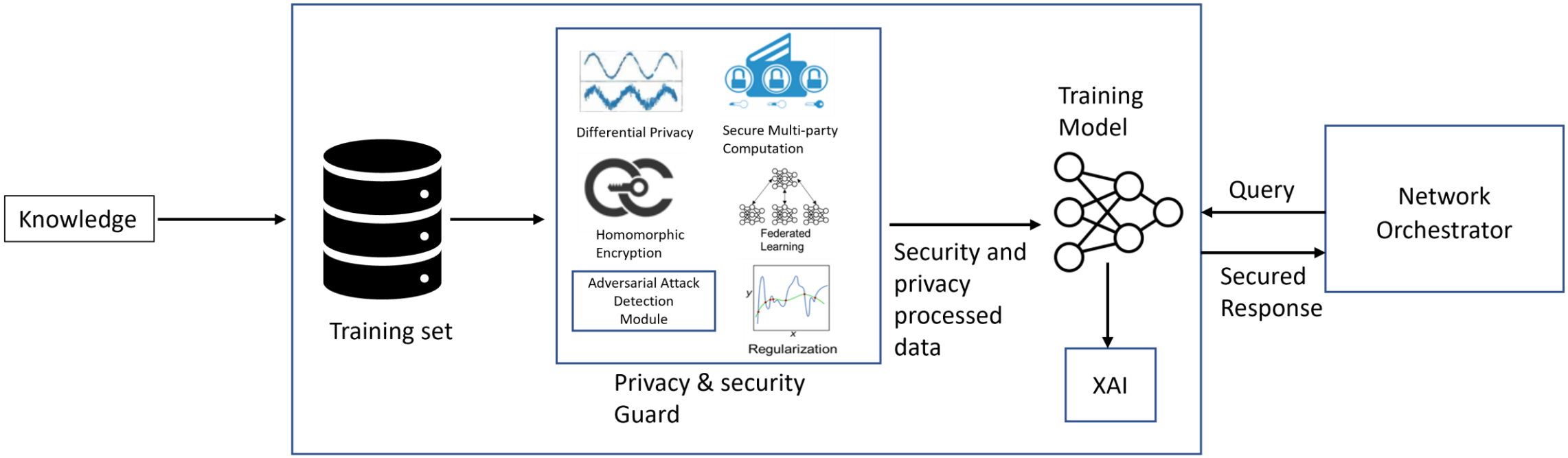
IMPACT ANALYSIS DIGITAL TWIN



THREAT PREDICTION WORKFLOW



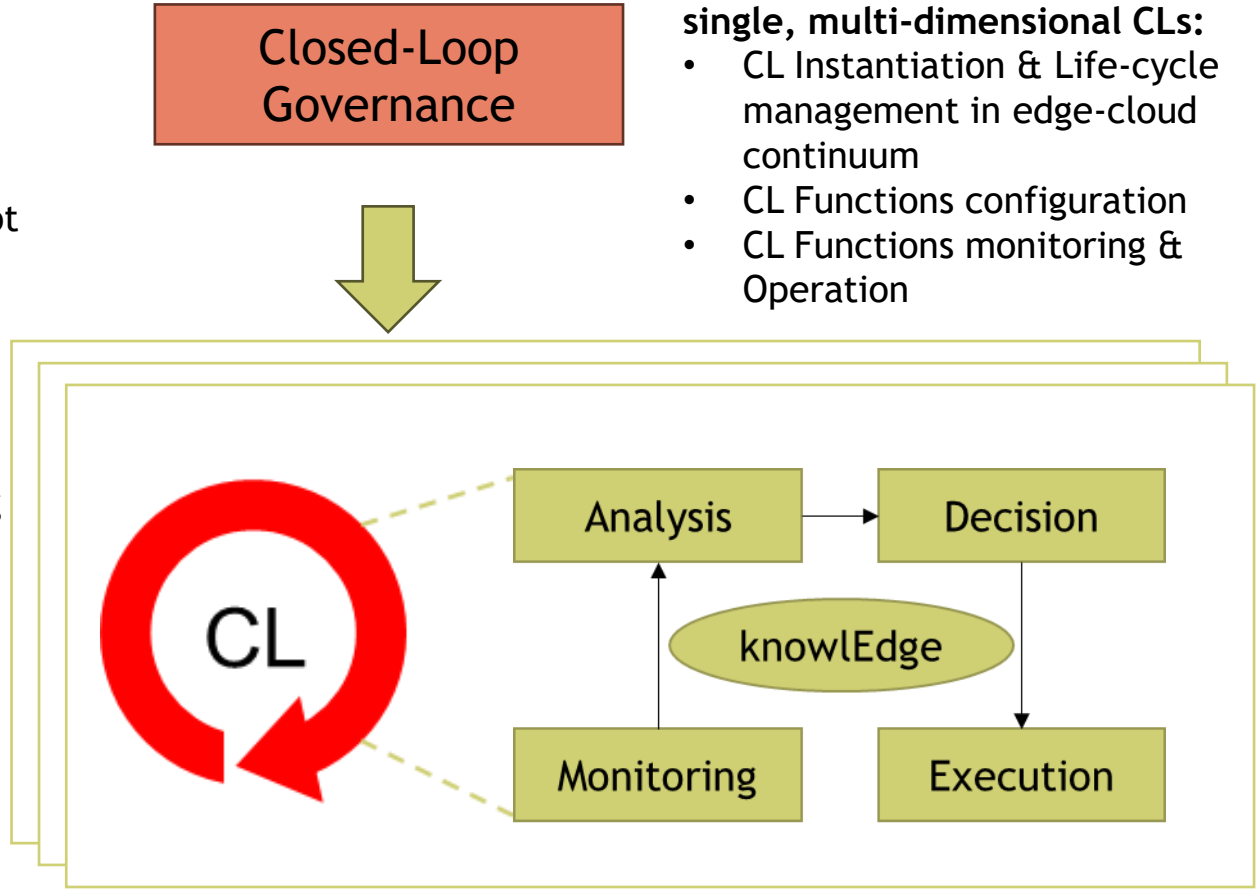
Enabler #8: Trustworthy AI/ML-based control



- An example of interaction between a Network Orchestrator and a Trustworthy AI/ML function in the management plane
  - Tighter integration with the functionality being part of the orchestration is also viable

Enabler #10: Zero-touch closed loop governance

- **Motivation**
  - 6G networks will increase in complexity due to the inclusion of many technologies, multiple domains, variable topologies and levels of virtualization
  - High variety of devices, services, requirements and levels of isolation will need to be managed together on a shared infrastructure
  - Automation is already present in current networks but will not be enough for the next levels of complexity [CBS+22]
- **Enabler's objectives**
  - Limiting or even removing operating staff from network management loops is imperative to speed up operations, increase network performance on the basis of dynamic conditions and reduce operational costs
  - Governance for programming and monitoring the provisioning of Closed-Loop (CL) functions to automate CL's delivery and adaptation at various level of abstraction (e.g., per-technology, per-domain, per-tenant, etc.)
- **Enabler's high-level description**
  - Automation in provisioning, configuration, and operation of Multi-dimensional CLs for mobile network automation with different time granularities (real-time, short-medium-long term), domain scopes (radio resources, core functions, transport networks, edge/cloud) and architecture layers (physical infrastructure, network and service layers).
  - AI/ML models for prediction within CL
  - ML sandbox domains with Network Digital Twins models developed in Enabler 9 for space exploration in CLs



Automated Orchestration of single, multi-dimensional CLs:

- CL Instantiation & Life-cycle management in edge-cloud continuum
- CL Functions configuration
- CL Functions monitoring & Operation

Closed Loop Governance

SOME DESIGN PRINCIPLES ARE PROPOSED IN THE PROJECT

- Network Digital Twin sandbox is considered a 6G enabler to achieve system requirements: M&O and security
- A sandboxing component is continously fed with status information from the network (topology, load, traffic, logs, services, users)
- NDT should be emulators, and not simulators!
- NDT are isolated, can run in parallel and look «back and forward» in time
- A user can directly test «intents» via a proper interface

Specific HORSE KPIs in secure M&O and NDT:

- Development and validation of AI-assisted threat detector and mitigation engine
- Development and validation of AI-assisted models to prevent multiple attacks

THANK YOU FOR YOUR ATTENTION

horse-6g.eu

HORSE project has received funding from the Horizon Europe research and innovation programme under grant agreement N° 101096342

PROJECT CONSORTIUM