HORSE VISION ON DIGITAL TWINS FOR 6G SECURITY

Fabrizio Granelli

Hexa-X-II Workshop on 6G - January 26, 2024 Online

HORSE PROJECT INFO

- Call: HORIZON-JU-SNS-2022
- Type of Action: HORIZON-JU-RIA
- Name: **Holistic, Omnipresent, Resilient Services for Future 6G Wireless and Computing Ecosystems**
- Acronym: HORSE
- Current Phase: Grant Management
- Number: 101096342
- Duration: 36 months
- Duration: 01 Jan 2023 – 31 Dec 2025
- Estimated Project Cost: €5,347,562.50
- Requested EU Contribution: €4,999,756.25
- Project Officer: Pavlos FOURNOGERAKIS

THE HORSE PROJECT - HORIZON-JU-SNS-2022-STREAM-B-01-04

- **Holistic, Omnipresent, Resilient Services for Future 6G Wireless and Computing Ecosystems**
- HORSE project will address a grand challenge towards **6G infrastructure operation for smart connectivity and service management**, and beyond, showing its effectiveness at the intersection of 6G connectivity, computing infrastructure management and security.
- HORSE proposes a novel human-centric, open-source, green, sustainable, coordinated provisioning and protection evolutionary platform, which can inclusively yet seamlessly combine advancements in several domains, as they get added to the system.
- It is envisioned that HORSE will also include predictive threats detection and impact analysis, proactive business-wise threats and breaches mitigation actions, programmable networking, semantic communications, Network Function Virtualisation (NFV), intent-based networking, AI-based techniques, in-network computing, and cross-layer management of physical layer features as they emerge in the 6G realm.
- HORSE outcomes will be validated in two highly innovative, performance demanding and representative scenarios, tentatively distributed operation of transport systems and multiuser remote rendering in extended reality.

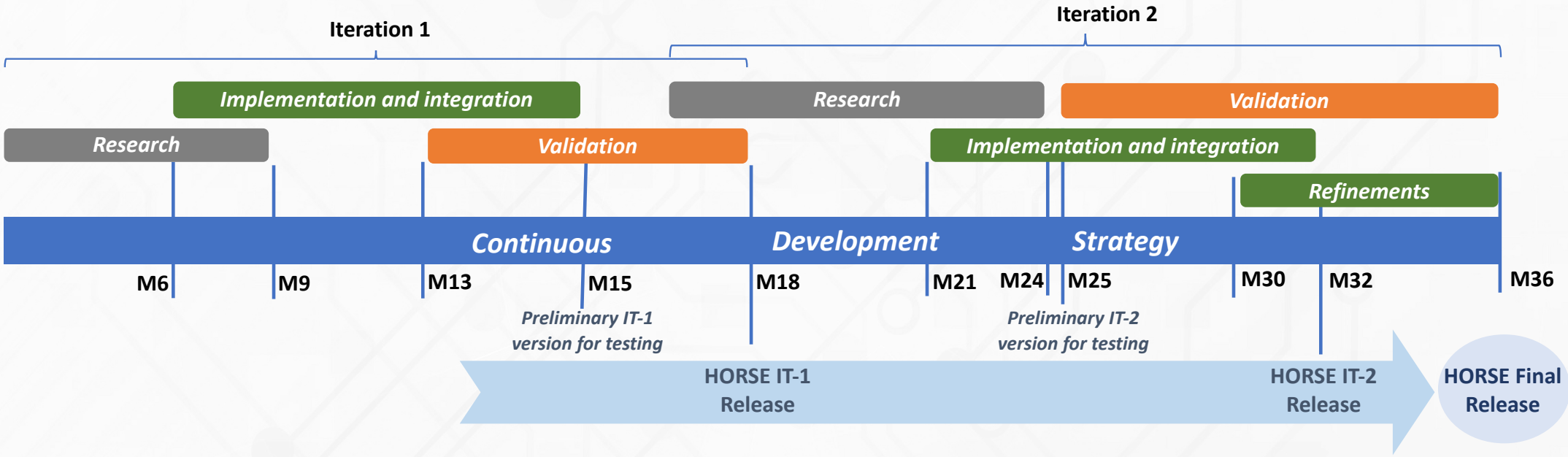
HORSE PARTNERS & EUROPEAN DIMENSION

HORSE CHALLENGES & OBJECTIVES

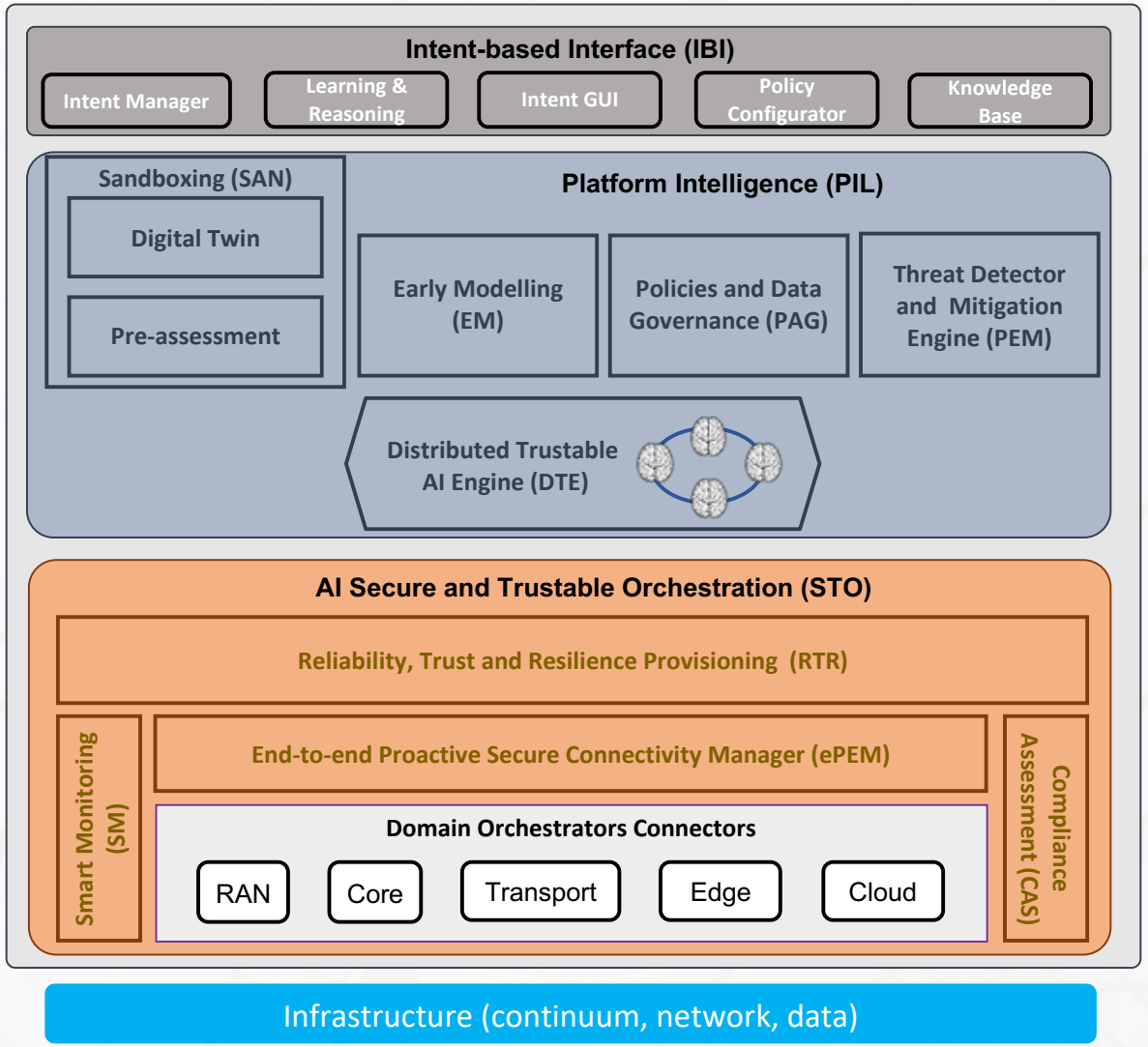
- **Challenge 1:** Creating a holistic vision of the dynamically evolving 6G system
- **Challenge 2:** Orchestrating top-down, bottom-up, and end-to-end security solutions
- **Challenge 3:** Providing a human-centric approach to security workflows
- **Challenge 4:** Engineering the system to be able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

- **Objective 1:** Comprehensive analysis of foreseeable 6G scenarios (WP2)
- **Objective 2:** Designing the necessary end-to-end security solutions (WP3, WP4)
- **Objective 3:** Development of a human-centric, holistic, omnipresent, and resilient smart services management and operation programmable platform for the 6G end-to-end landscape (WP3, WP4)
- **Objective 4:** Deploying AI technologies driving a completely predictive approach to security management, fully addressing high services, systems, risks, and threats dynamicity (WP3, WP4)
- **Objective 5:** Characterize the user profile and the 6G system as a digital twin, to feed the AI distributed decision processes, responsible for improving the standard of trust and security the user wants to reach out (WP3, WP4, WP5)
- **Objective 6:** Designing the system interface to be intent-based to implement the role of the “Human-In-The-Loop” which will ensure the system can translate the user's service demands into secure network services operation (WP5)
- **Objective 7:** Deploy, demonstrate and validate HORSE in selected use cases (WP5)
- **Objective 8:** Creating impact and promoting of open access to the HORSE platform for broad and sustainable exploitation of results (WP6)

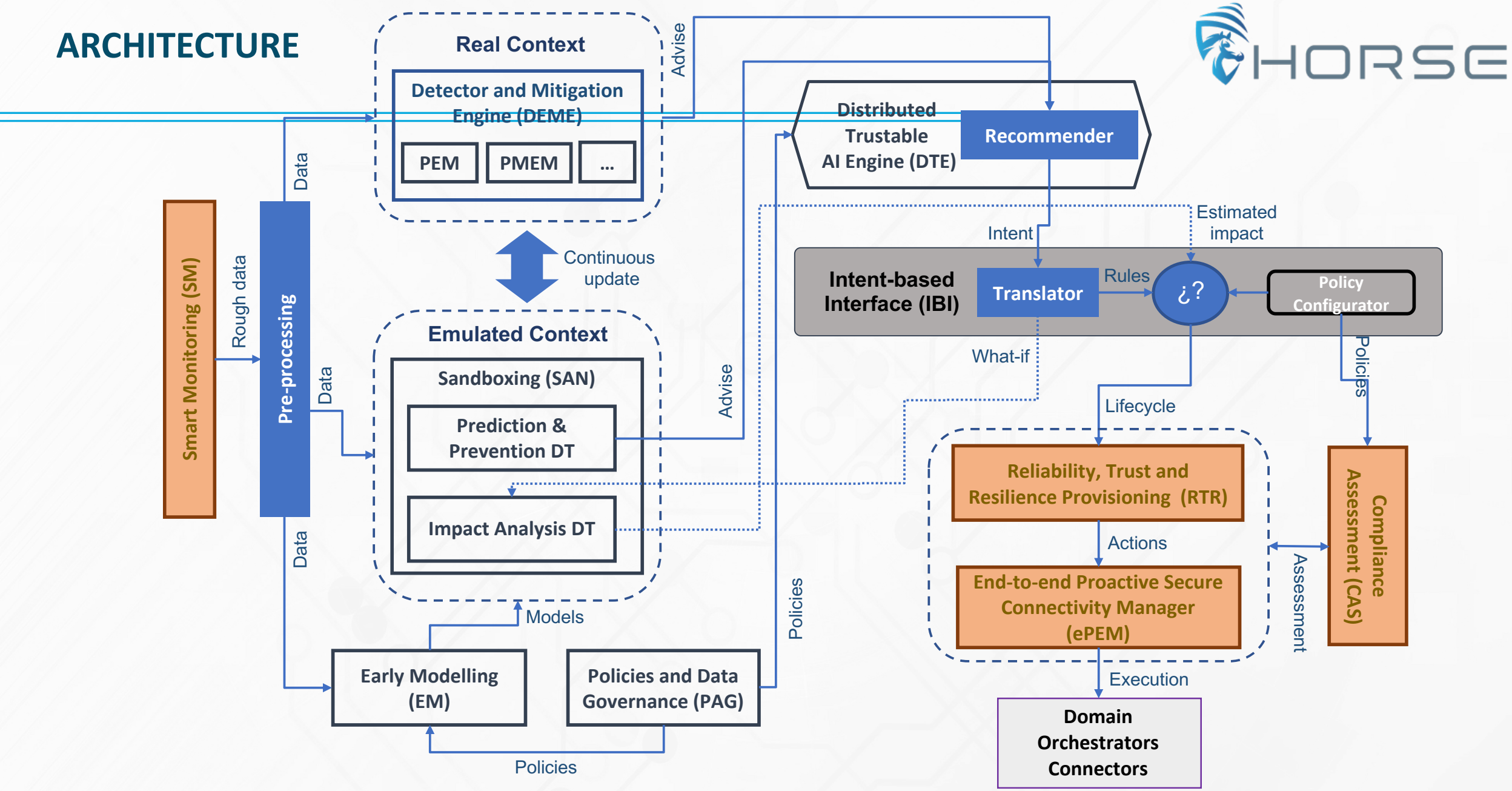
HORSE METHODOLOGY



HORSE FUNCTIONAL ARCHITECTURE

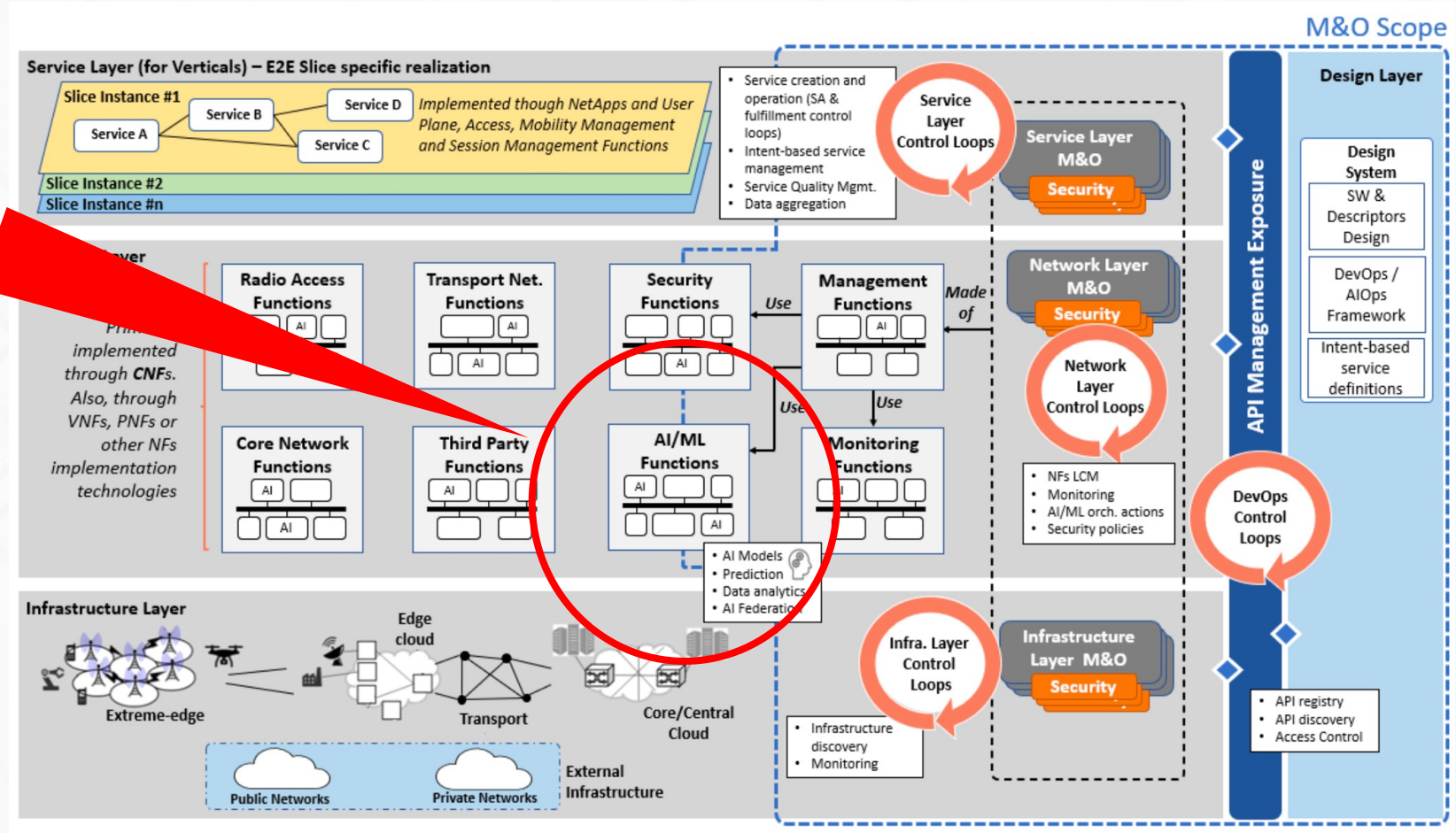


ARCHITECTURE



WHAT ARE THE 6G ENABLERS?

- Secure Orchestration
- Intent-Based Interface
- Network Digital Twins for prediction, prevention and «what-if»



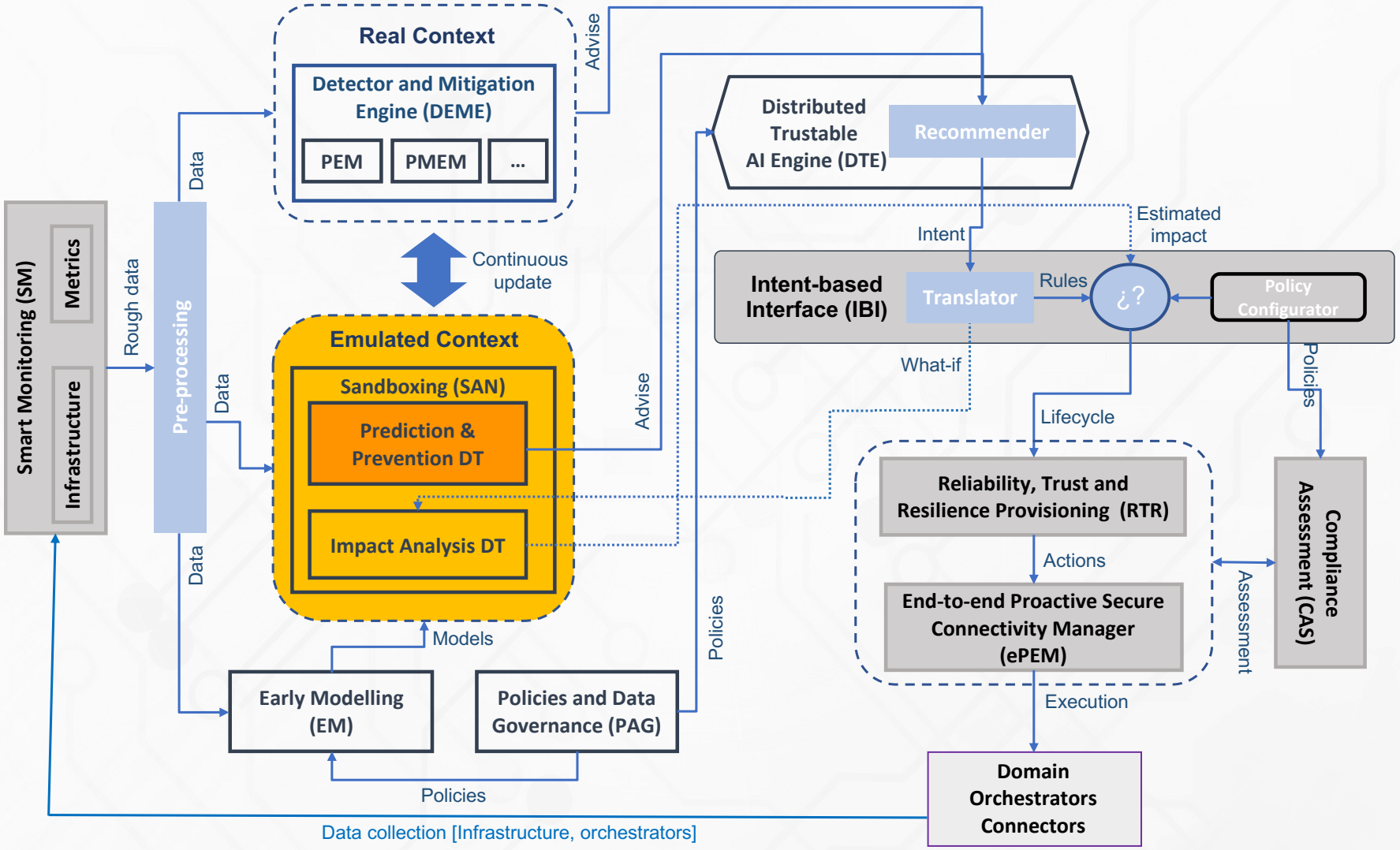
from Hexa-X Deliverable D6.2, “Design of service management and orchestration functionalities”

WHAT ARE THE USE CASES FOR THE ENABLER?

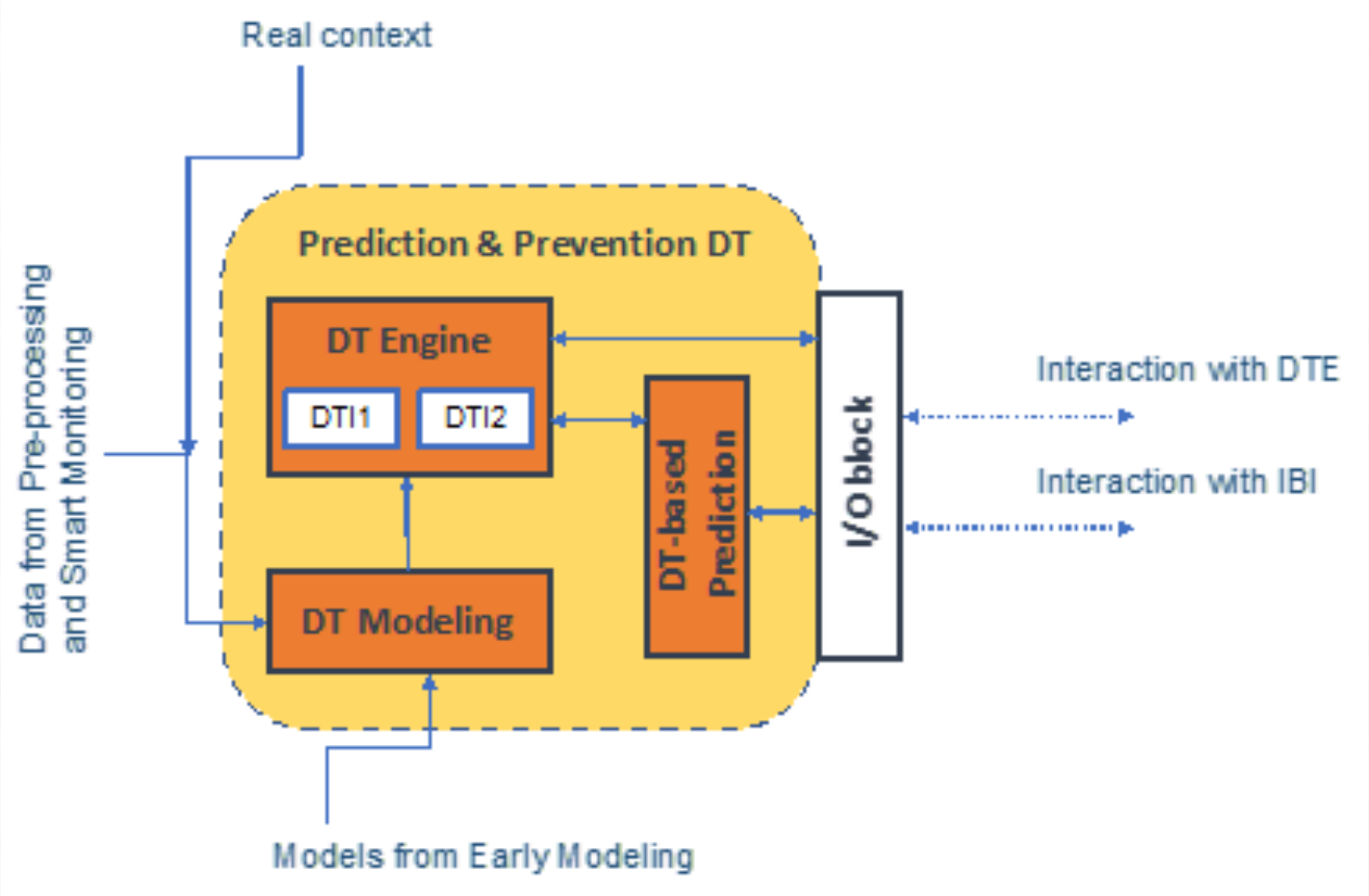
- Analysis of the network status to detect anomalies
- Prediction and prevention of security threats
- Analysis of «what-if» scenarios to support autonomous decision-making

- … but also:
- Using the Digital Twin to train AI/ML

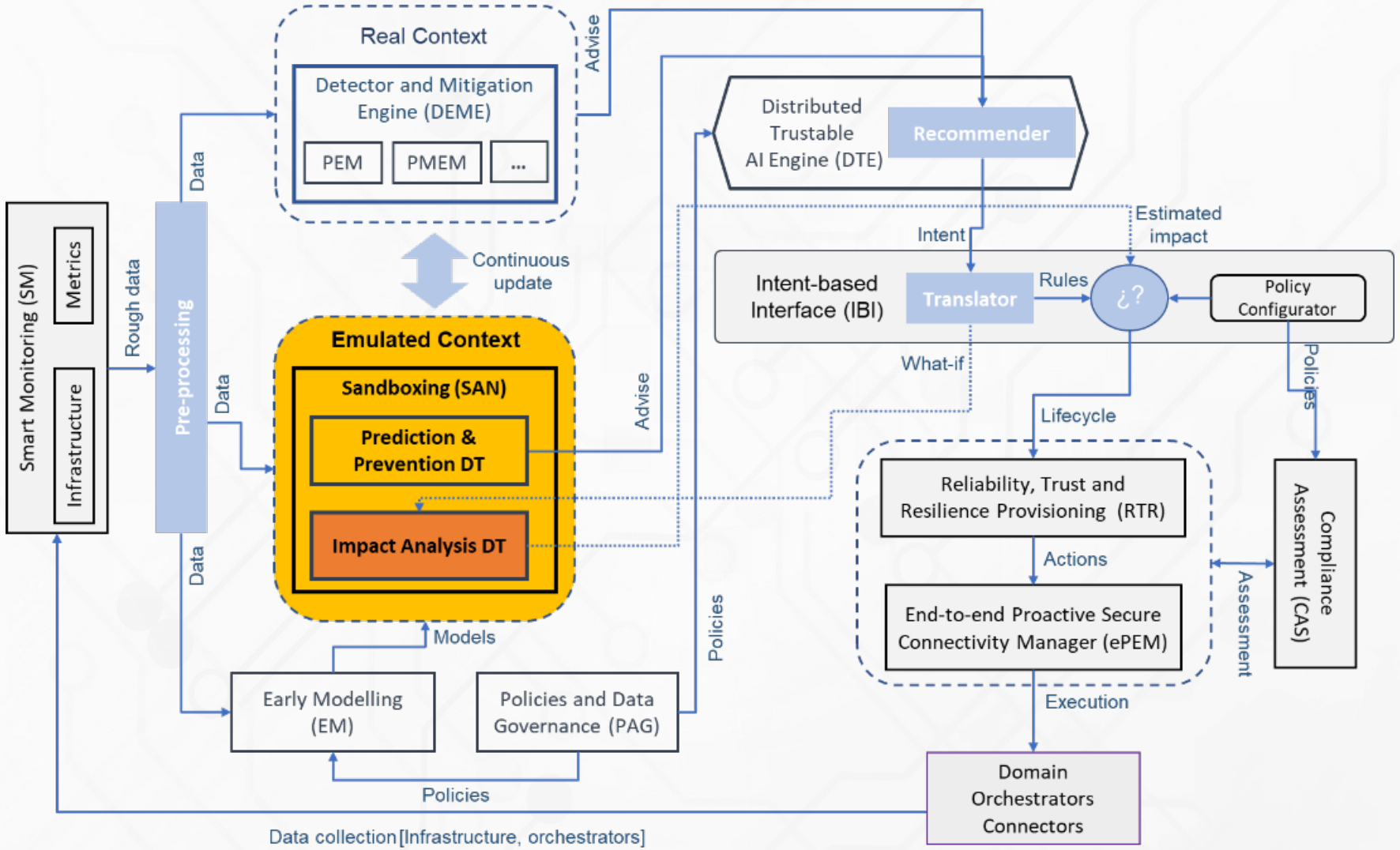
PREDICTION AND PREVENTION DIGITAL TWIN



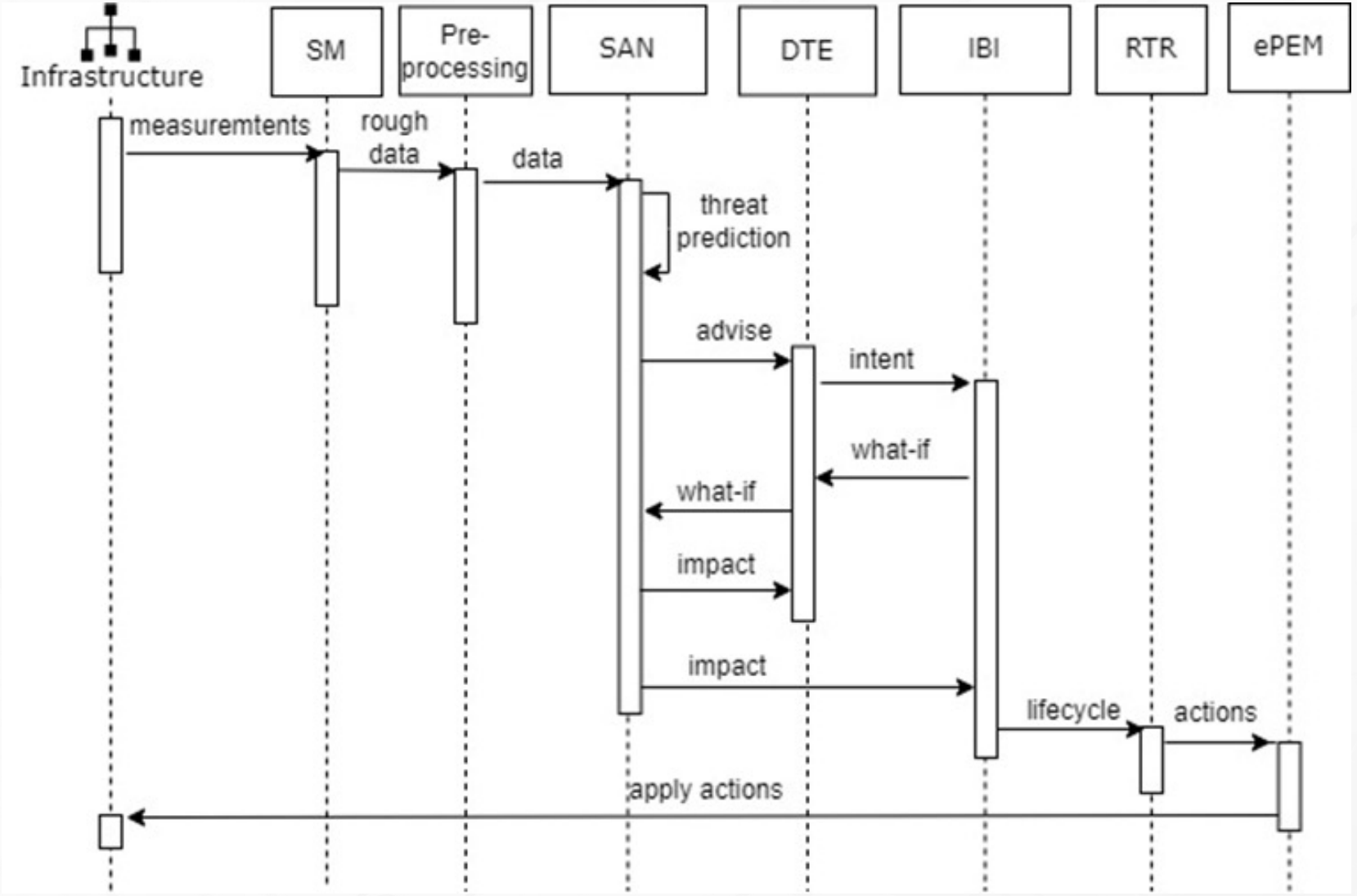
PREDICTION AND PREVENTION DIGITAL TWIN



IMPACT ANALYSIS DIGITAL TWIN



THREAT PREDICTION WORKFLOW



WHAT ARE THE ASSUMPTIONS ABOUT SUPPORT OR MEANS FROM THE E2E SYSTEM FOR THAT ENABLER THAT ARE NOT DEVELOPED BY THE PROJECT?

- Availability of proper interfaces to provide a continuous sychronization between the Physical and the Digital Twin (topology, load, traffic, services, users)
- … an actual 6G network infrastructure!

WHAT DESIGN PRINCIPLES ARE PROPOSED IN THE PROJECT?

- A sandboxing component is continously fed with status information from the network (topology, load, traffic, services, users)
- A module is capable of building one or more Digital Twins
- Digital Twins should be emulators, and not simulators!
- E.g. capable of analyzing also software bugs
- Digital Twins are isolated, can run in parallel and look «back and forward» in time
- The network manager can get precise predictions on the impact of different solutions and even prevent dangerous situations
- A user can directly test «intents» via a proper interface (man-in-the-loop)

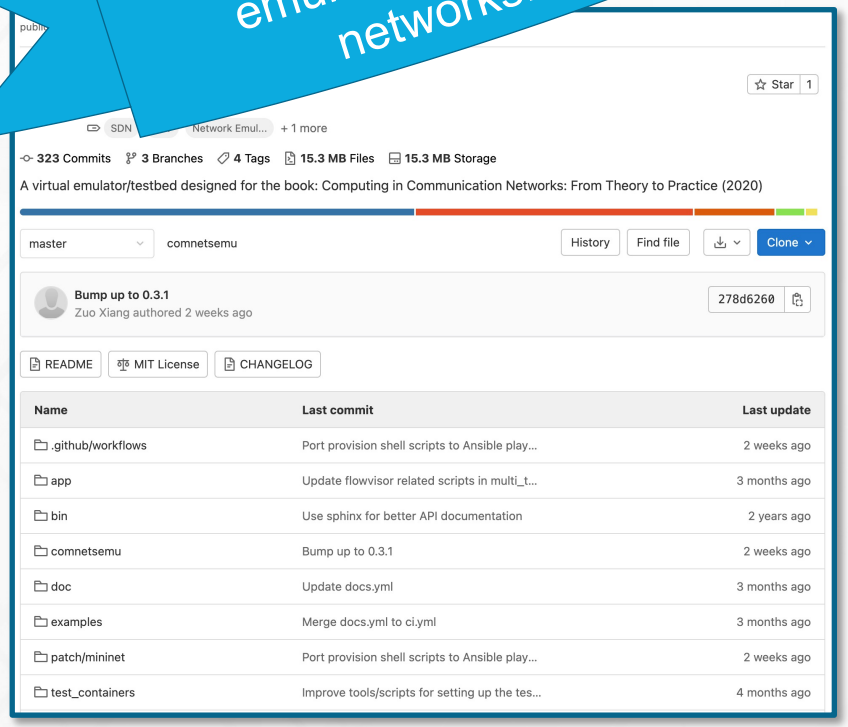
WHAT (SUB) SYSTEM ARCHITECTURE(S) ARE PROPOSED? WHAT METHODOLOGY IS CONSIDERED FOR THE ENABLER INTEGRATION IN THE (SUB) SYSTEM?

- The proposed sandbox might represent a (set of) Network M&O AI/ML functions
- Such AI/ML functions will enable AI- and ML-powered prediction, prevention and «what-if» analysis
- Current focus on security, but it could be extended to other areas

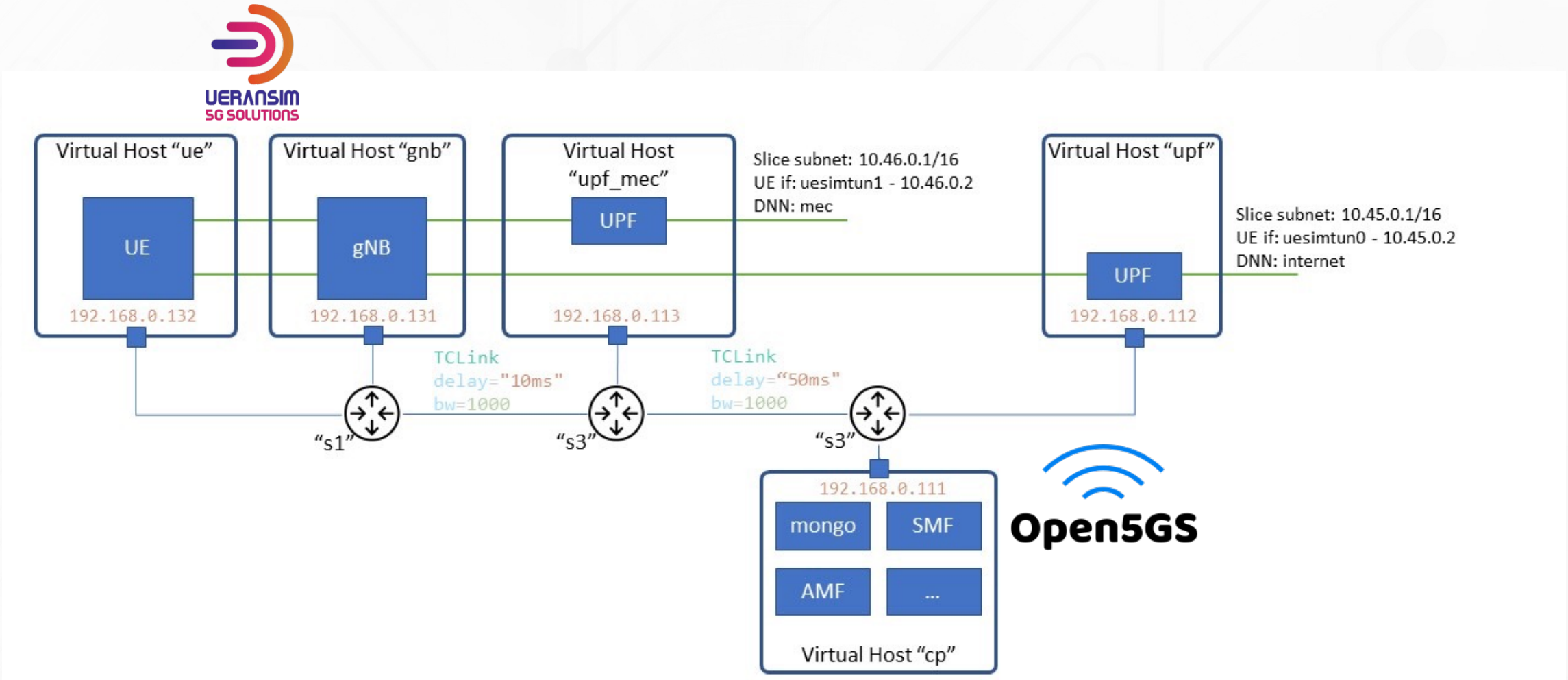
A TOOL FOR DIGITAL TWINNING

- Comnetsemu (SDN+NFV network emulator)
- Free, opensource (by UTrento and TU Dresden):
- https://git.comnets.net/public-repo/comnetsemu
- We have a running 5G emulation

We have the right tool for emulating modern networks!



DEPLOYING UERANSIM AND OPEN5GS ON COMNETSEMU



DOES THE PROJECT ELABORATE ON SOME SPECIFIC METHODOLOGY FOR EVALUATING 6G KPIS AND KVIS?

- The Digital Twin sandbox might be considered a 6G enabler to achieve system requirements: security

- Specific HORSE KPIs:
- Development and validation of AI-assisted threat detector and mitigation Engine
- Development and validation of AI-assisted models to prevent physical layer attacks

STATUS AND ACTIONS TAKEN FOR THE STANDARDIZATION IMPACT

- Contributed to ETSI ENI GR 035
  - Introduction of the concept of Digital Twinning for increased autonomicity
- IRTF NMRG
  - application of AI to network management: https://datatracker.ietf.org/doc/draft-pedro-nmrg-ai-framework/04/
- ETSI ETI, ENI, SAI, ZSM
- 3GPP SA3
- IETF / IRTF

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