Partners: NFR, NFI, EAB, APP, ASA, CTT, EBY, ICC, NXW, NDK, NGE, OPL, ORA, VTT, TID, WIN, TUD, TUK, SIS, UC3, BI, LMF

Hexa-X-II D2.2 Deliverable

D2.2 summary slides: Foundation of overall 6G system design and preliminary evaluation results

Hexa-X-II

hexa-x-ii.eu

2023-12-29

Table of Content

Chapter 2
Requirements of 6G E2E system

Use case requirements of 6G E2E system

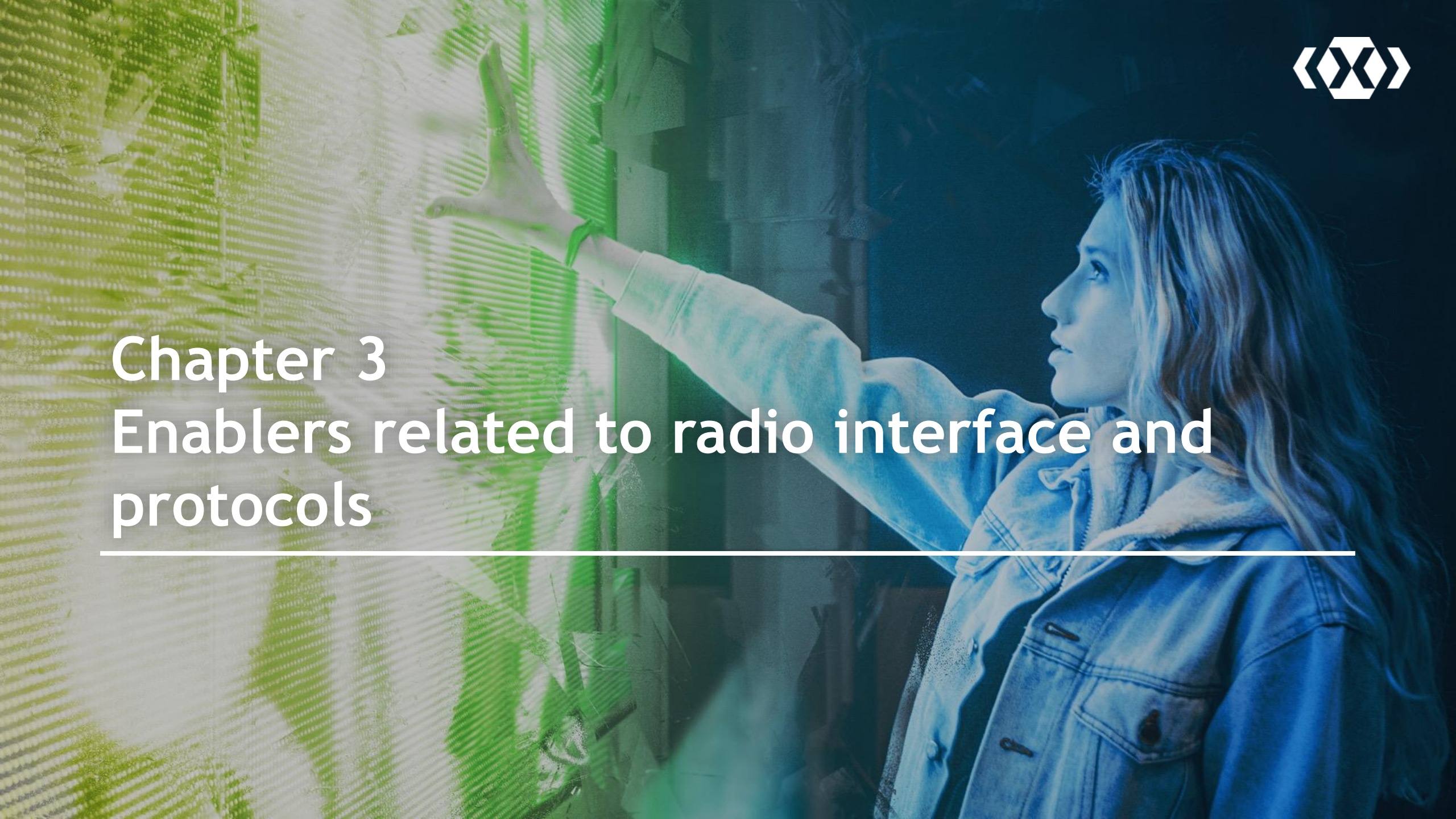
- Capabilities of the system in terms of what it should do and relevant to a selected list of 6G use cases.

Requirements\Use case	Ubiquitous Network	Real-time digital twin	Seamless Immersive Reality	Cooperating mobile robots	Human centric services	Network assisted mobility
Ubiquitous connectivity	X	X		X	X	X
Indoor coverage	X	X	X	X	X	
Extreme connectivity (high bitrate)			X			
Mobility support	X		X	X	X	X
Pervasive AI/ML		X	X	X	X	X
Efficient sleep states	X		X		X	X
Compute as a Service		X	X	X		X
Intent-based interfaces		X		X		
Reliability		X		X	X	X
Positioning/sensing		X	X	X	X	X
Ultra-low-cost	X					
Energy neutral	X					
Predictable low-latency E2E communication		X	X	X		X
Security/Privacy	X	X	X	X	X	X
Resilience	X	X		X		X
Service continuity	X		X			X

Operational requirements of 6G E2E system

A set of requirements which will not be directly visible to end-users, but provide functionality to efficientlyt fulfill use case requirements for operators.

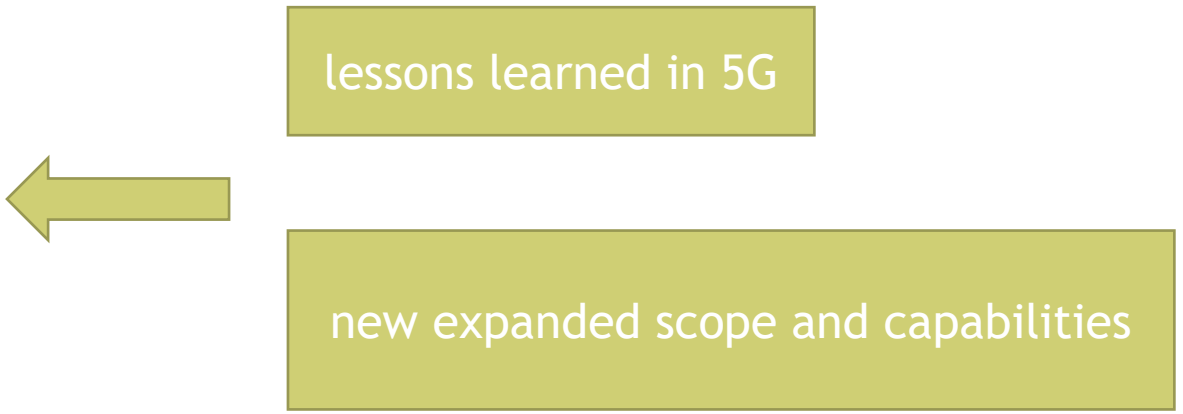
- Flexible radio protocols
- Mobility procedures
- Improved access convergence
- Native AI/ML capabilities
- Multi-connectivity
- Intent-based management
- Seamless orchestration across the compute continuum
- 6G service delivery across multiple digital service providers
- New 6G capabilities exposure



Chapter 3
Enablers related to radio interface and protocols

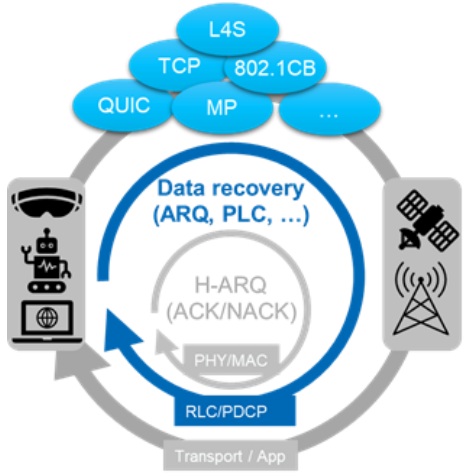
Ambition for 6G radio interface and protocols

- Bear all essential functionality, features and options that go hand in hand with fundamental 6G requirements common and essential to all use cases (e.g., both high-end and low-end UEs covering a wide range of use-cases) in mind from “day one”,
- Easily extensible for further enhancements in the 6G timeframe, instead of over-optimized for the baseline; building on top modular components that ease protocol scalability to cover more advanced radio requirements needed by the use cases,
- Simplicity in comparison to previous generations,
- Optimize for actual scenarios and needs in the fields, not only for extreme performance or corner cases, e.g., to avoid unnecessary configurability,
- One flexible protocol stack for different scenarios that maximizes the use of single protocol components for different scenarios,
- Ensure a fast and reliable protocol operation (e.g., supporting fail-safe mechanisms when needed),
- Keep separation of concerns in multi-layer protocol stack, without compromising performance by artificial boundaries,
- Better consideration of spectrum sharing of other technologies, privacy/security, resilience/availability, energy efficient operation of network and device, friendliness to cloud implementation, network scalability (e.g., adding/removing network nodes as needed).



Radio user plane - Introduction to data recovery

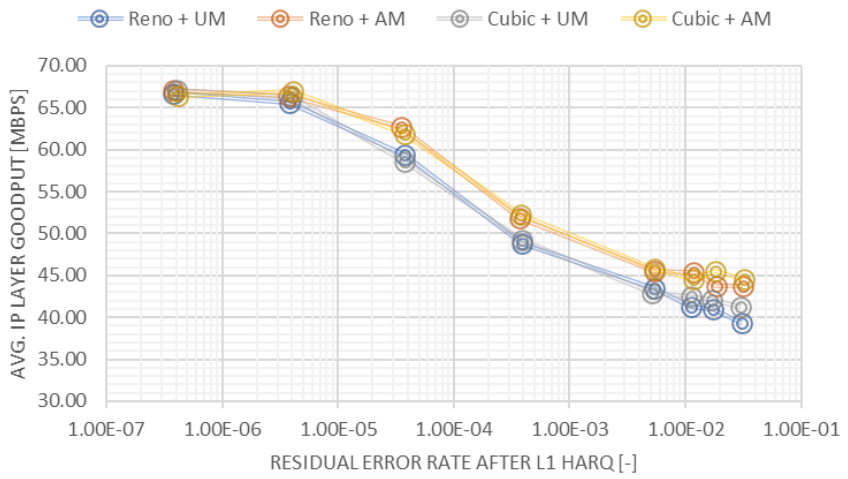
- The 6G data recovery and reordering mechanisms shall supplement transport and application layer mechanisms of the 6G-era.
- The innovations for the data recovery mechanisms should target:
  - Reducing overall latency
  - Investigating cross-layer interactions to enhance performance
  - Reordering requirements
  - Further enhancements towards new use-cases, e.g. XR/ metaverse



E2E mechanisms for data recovery and reordering (PLC is short for packet-level coding).

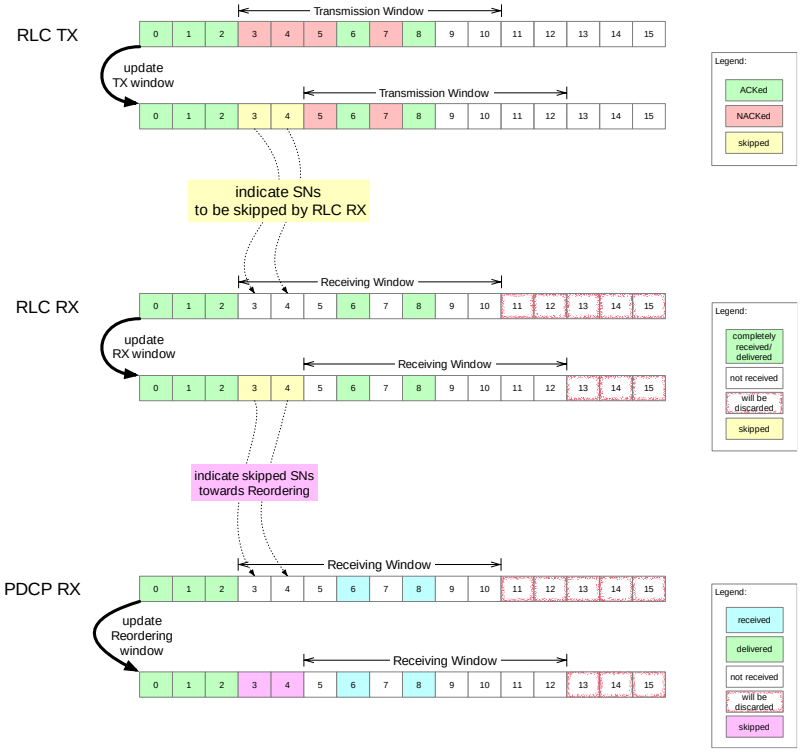
Radio user plane - Data recovery mechanisms

Relation between ARQ data recovery performance and goodput



- TCP user goodput is plotted as a function of the residual error rate, i.e., the residual error after HARQ process considering the control channel imperfections.
- It is seen that if HARQ residual error rate is higher than approximately 1x10-5 then having a second data recovery layer starts to have a significant impact on experienced user goodput.

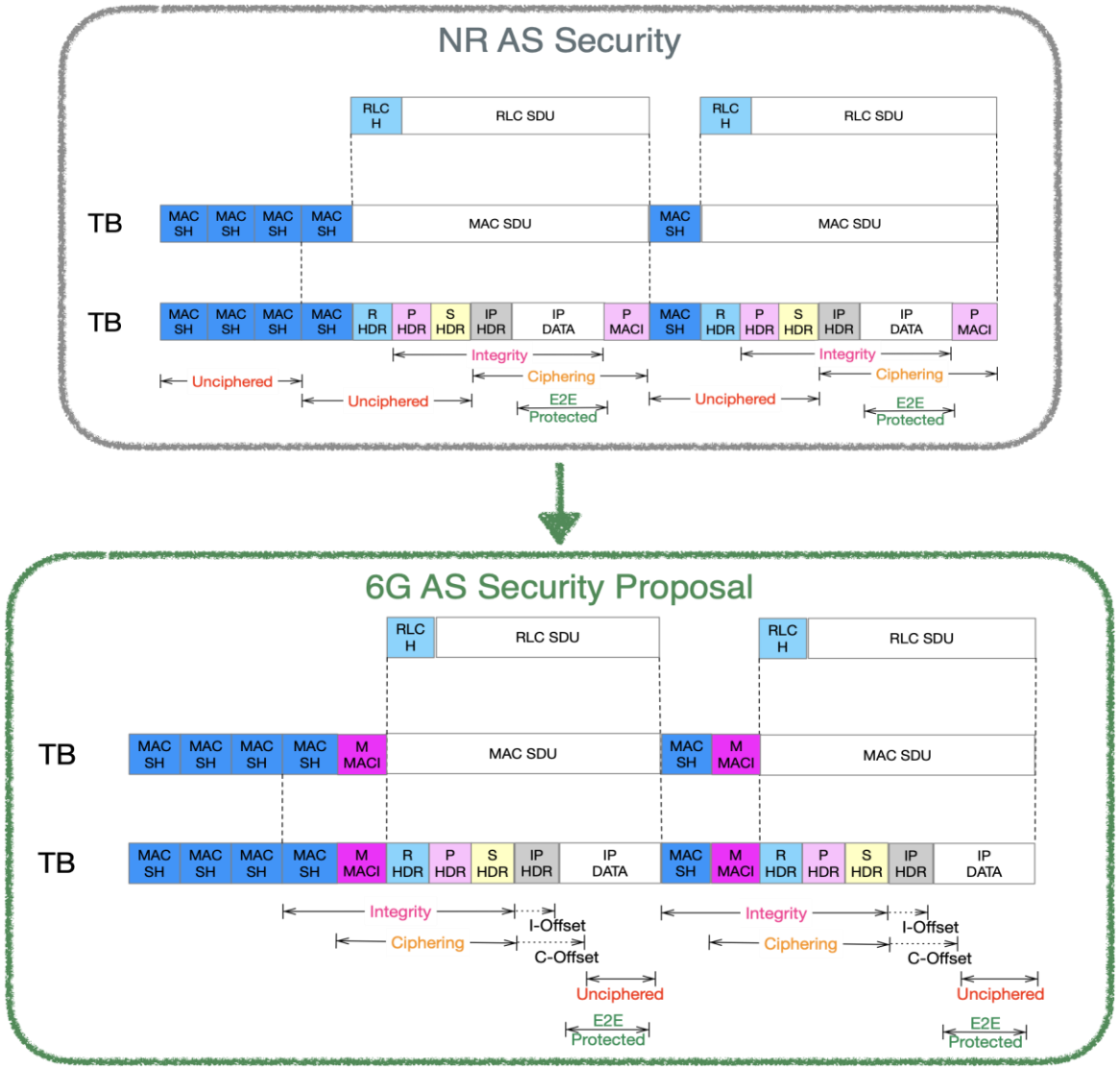
Cross-layer interaction enhancements example for data recovery



- Enhance the RLC AM protocol to allow for window moving operations and the skipping of the reception some RLC SNs (i.e., similar to RLC UM).
- Upon reception of NACK SNs from the RX RLC entity, the TX RLC entity does not always retransmit the NACKed SNs. Instead, it sends information back to RX RLC entity that the NACKed SNs shall be skipped.

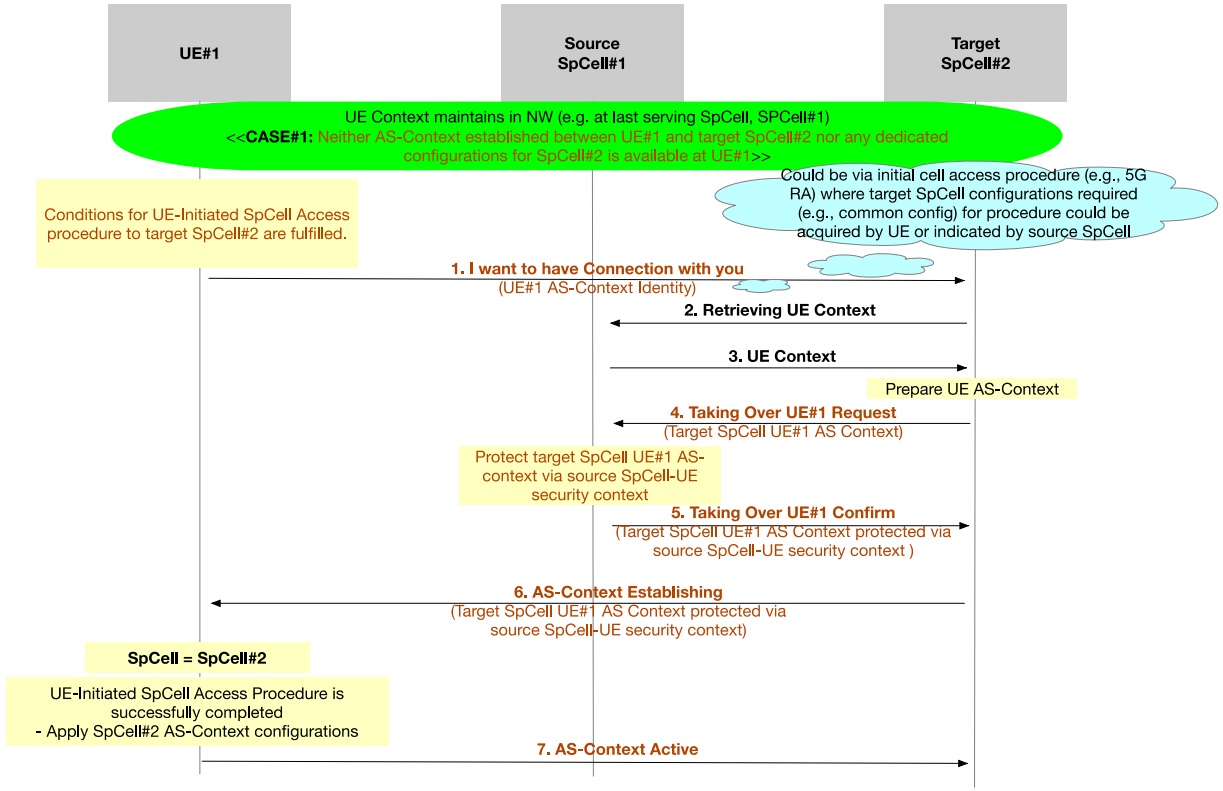
Radio user plane - Chiphering and integrity protection

- In NR, ciphering and integrity protection are both optional and are configured independently by the network via RRC signaling. This results in ciphered and optionally integrity protected IP headers and payload, while the L2 headers (i.e., SDAP, PDCP, RLC and MAC) are uncyphered and partially not integrity protected (i.e., only PDCP and SDAP headers are integrity protected).
- To overcome potential threads like metadata eavesdroppers, inserting forged MAC CEs, etc., this enabler proposes to move the Ciphering and Integrity functionality from PDCP to MAC.
- **Integrity protect** all **L2 headers** (i.e., SDAP, PDCP, RLC, MAC SH except for MAC CEs).
- Ciphering and integrity protecting of the partial or full IP data is still possible.



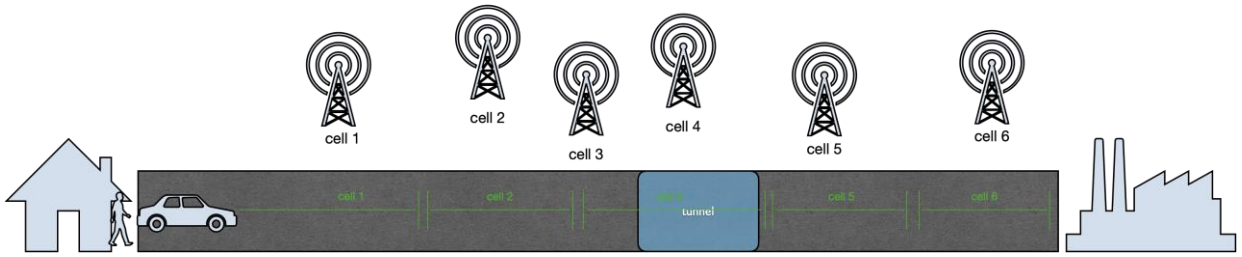
Radio control plane (1)

Enhanced SpCell change procedure with UE initiation



- Enhanced SpCell change to allow **UE to initiate SpCell Access directly** without waiting for RRC preparation.

Data Driven Mobility



- The user and mobility context of the UE may be captured in **the UE Triggered Contextual Events.**
  - **Radio/Environment Events** consider UE capability of understanding e.g., indoor condition, tunnel detection, etc.
  - **User Traffic Events** consider the expected traffic activity.

Radio control plane (2)

Multi-layer downlink radio resource control

- A need to develop a simplified and easy-to-use high-performance Radio Resource Control (RRC) framework that can handle the ever-increasing flexibility of layer 1 and layer 2.

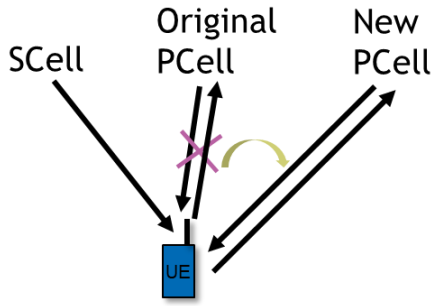
RRC

MAC CE

L1 DCI

Mobility procedure in radio access network

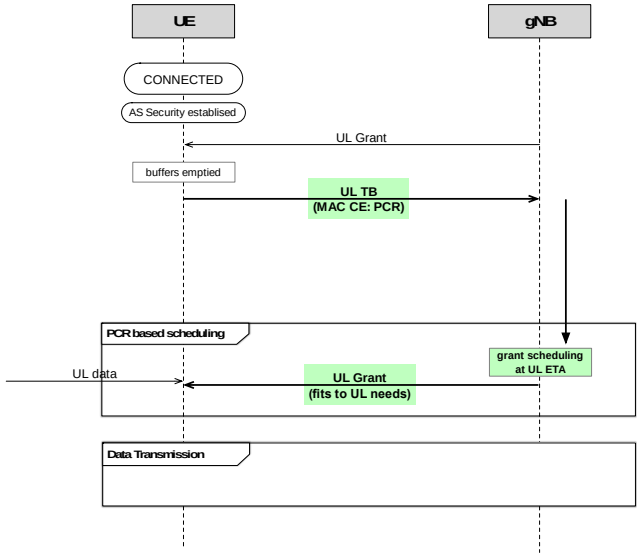
- 6G mobility procedure in the case of a single multi-connectivity solution (e.g., carrier aggregation) should not allow a single point of failure and long recovery time



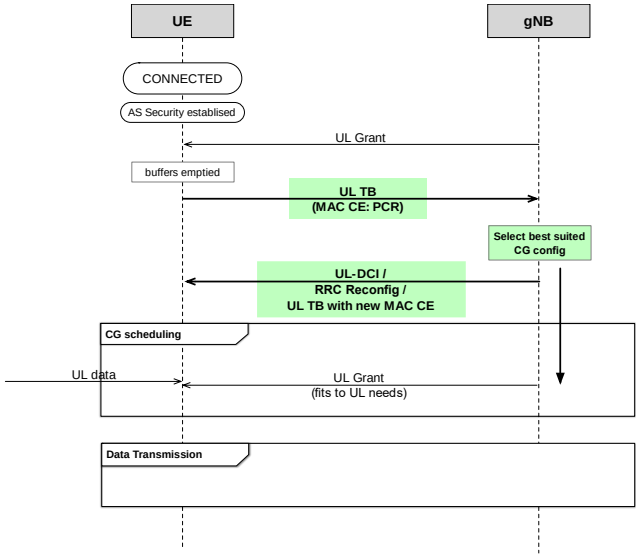
Application-NW interaction for service differentiation and QoS/QoE management

- Periodic Cadence Report - PCR - is a new mechanism of reporting from UE to NW
  - UE indicates what traffic pattern to expect via PCR in order to:
    - Enhance Dynamic Grant scheduling by the NW in addition to or instead of BSR
    - Enhance Configured Grant configuration and/or selection

Dynamic Grant Example

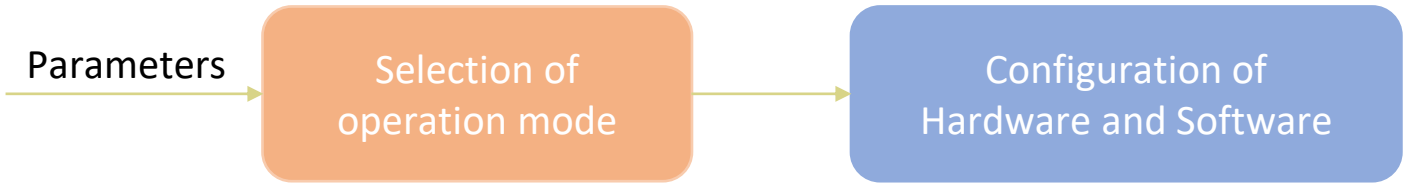


Configured Grant Example



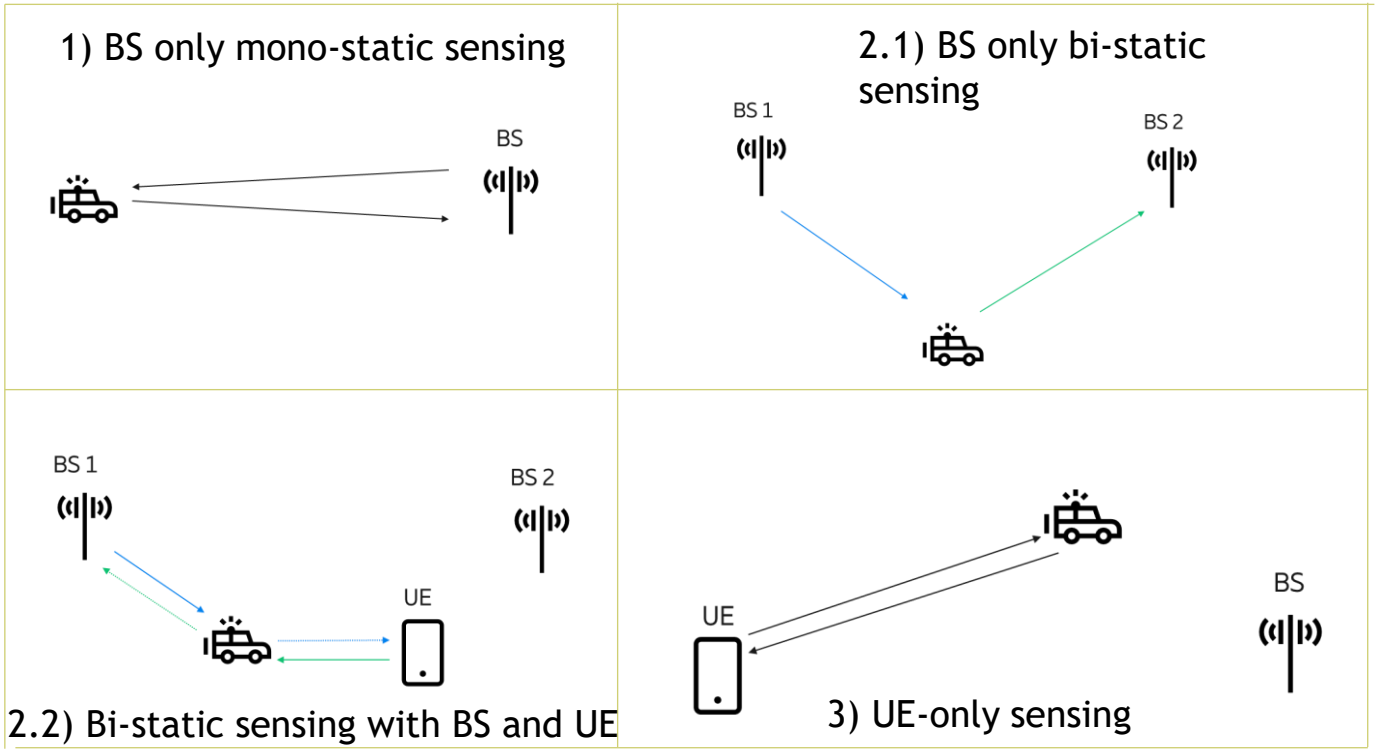
Energy efficient radio design

- Radio design has focused on increasing the spectral efficiency and data rate by employing a single analogue front-end.
- The new energy efficient radio design will aim at maximizing the energy efficiency considering the spectrum availability while providing the required data rate.
- The main goal is to deliver the data rate needed at the highest possible energy efficiency.
- This concept will be realized through the definition and implementation of various operation modes, each one comprising a predetermined hardware configuration with adaptable software settings.

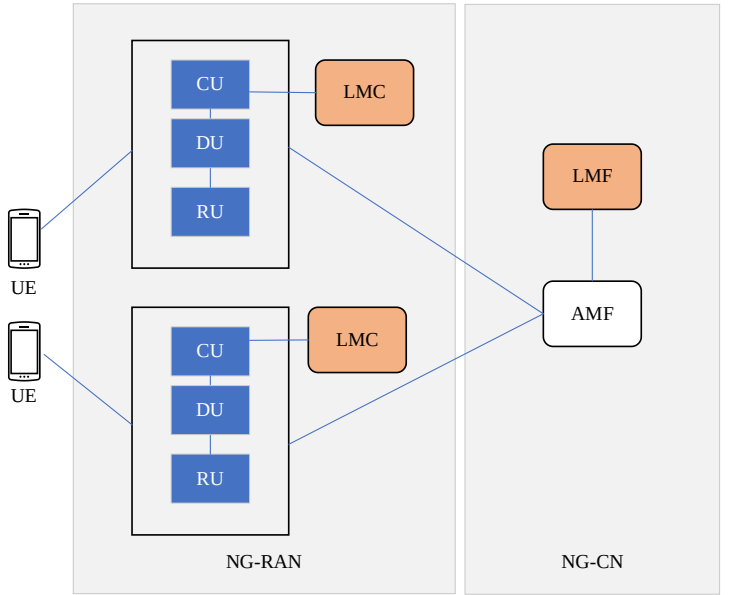


Radio protocol support for sensing and localization

- A unified approach between sensing and localization, due to similarities from the radio protocol interface/protocol point of view. Both positioning and sensing can be achieved by a node (either a device or a network node)
  - Three sensing scenarios are analyzed, from simplest for more complicated ones.



- New component is needed to improve localization latency and accuracy.



AMF: Access and Mobility Management Function, CU: Central Unit, DU: Distributed Unit, LMC: Location Management Component, LMF: Location Management Function, RU: Radio Unit, UE: User Equipment

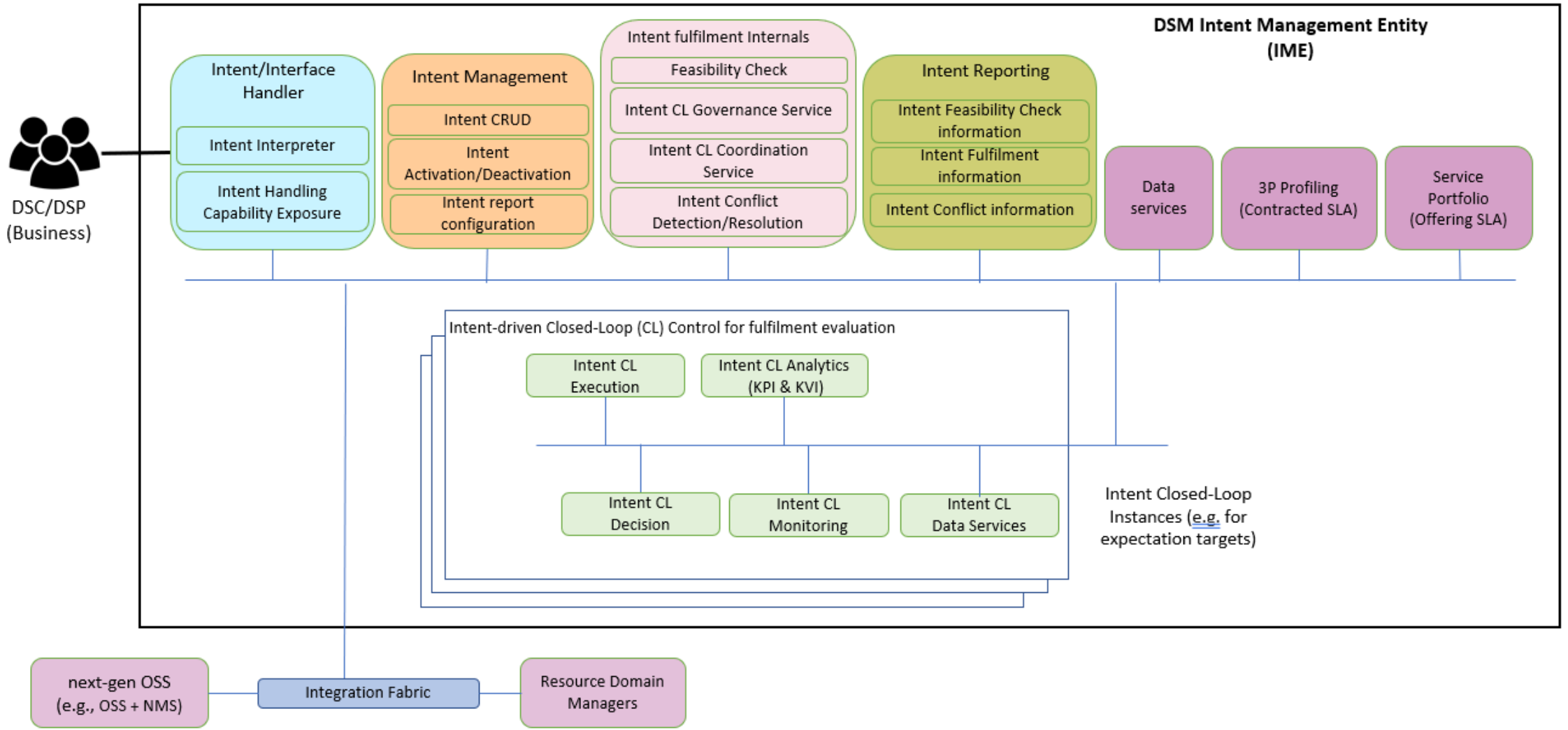
Positioning with new local management component (LMC)

Radio protocol support for other 6G enablers

- Compute offloading
  - Node discovery, computation offload, offload at RAN node
- AI
  - Protocol stack may be affected by:
    - Coordination and signalling of novel architectural components that enable for privacy aware data collection and learning.
    - Coordination mechanism for keeping the models and data up to date and synchronized among the cellular nodes.
- Subnetworks
  - Air interface and new procedures between the management node-BS and management node-UE
  - What spectrum the subnetwork operates on (i.e., licensed or unlicensed)
  - Role of the management node and whether the subnetwork is transparent or non-transparent to the NW.
- Distributed-MIMO
  - What is the difference from previous concepts on coordinated multi tx-rx point, multi-tx-rx points, the cell concept.
- Reflective intelligent surface
  - Can inherit 5G work on network-controlled repeater but unclear for UE-controlled repeater.
- Energy neutral device
  - The challenge on the radio protocol design is how to incorporate the aspects of energy neutral devices in the baseline. If not included in the baseline, how to ensure easy extensibility in the 6G time frame for those devices.

Chapter 4
Enablers related to E2E service management and automation

Intent-based digital service manager functional architecture



High-level description of the intent-based service manager

- **Intent/interface handler:** The gateway for the user to interact with the whole intent management solution and trigger those actions available for the user. It offers two main capabilities: the "Intent Interpreter" and "Intent Handling Capability Exposure".
- **Intent management:** It takes care of the intents data objects with the multiple actions to control the intent's life-cycle using CRUD (Create/Read/ Updated/Delete) operations, the activation/deactivation of an intent and intents reporting actions.
- **Intent fulfilment internals:** it has those capabilities that a user should never be able to access but that are key to those capabilities visible by the user such as the checking the intent feasibility, detecting & resolving conflicts or the governance and coordination of intent CLs.
- **Intent reporting:** It generates reports based on the different types of intent-related information: "Intent Feasibility Check Information", "Intent Fulfilment Information" and "Intent Conflict Information".
- **Intent-driven closed loop control for fulfilment evaluation:** This functional block offers the capabilities to manage the life cycle of the Intent CL instances and ensure they are fulfilled at any time.
- **Data services:** It is in charge to store the intent data objects and other possible information such as SLAs and policies.
- **3P profiling:** It allows to provide a full characterization of every Hexa-X-II tenant (i.e., a 3rd party) through a 3P profile.
- **Service portfolio:** It offers the available 6G services information to the tenants, so based on the available services and their information, tenants may request with more knowledge better intent-requests.

Enablers for intent-based management automation

- Intent translation and provisioning
- Data fusion mechanisms based on telemetry data
- Closed loop coordination for intent management
- Intent conflict administration
- Human-machine intent interface design
- Intent-driven placement
- Declatrative intent reconciliation
- Intent reporting
- 3rd party services

Intent translation and provisioning

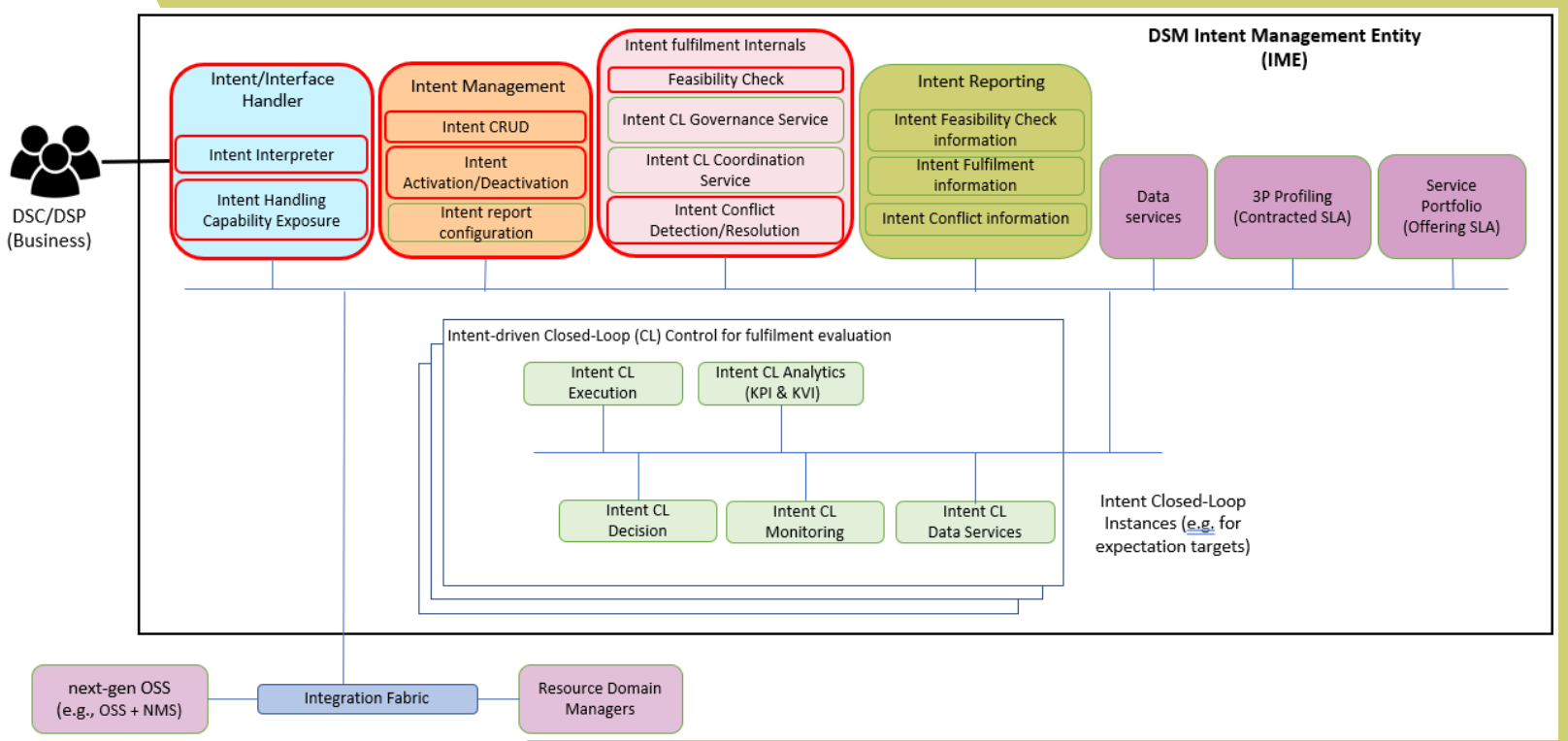
Objectives

To reach an agreement with the user and create the final intent data object that it can be translated (considering the service, security and trust levels and the constraints of the resources domains) into a set of machine-based requests depending on the different resource domain managers available behind the integration fabric.

High-level description

An intent-based solution to manage service resources located across multiple domains and to select the most suitable combination of them to deploy the E2E service and to achieve the expectations and targets defined by the service requester, while keeping under consideration the specific characteristics of each involved domain.

Enabler Figure



Data fusion mechanisms based on telemetry data

Objectives

Provide intent achieved values and support intent driven-orchestration

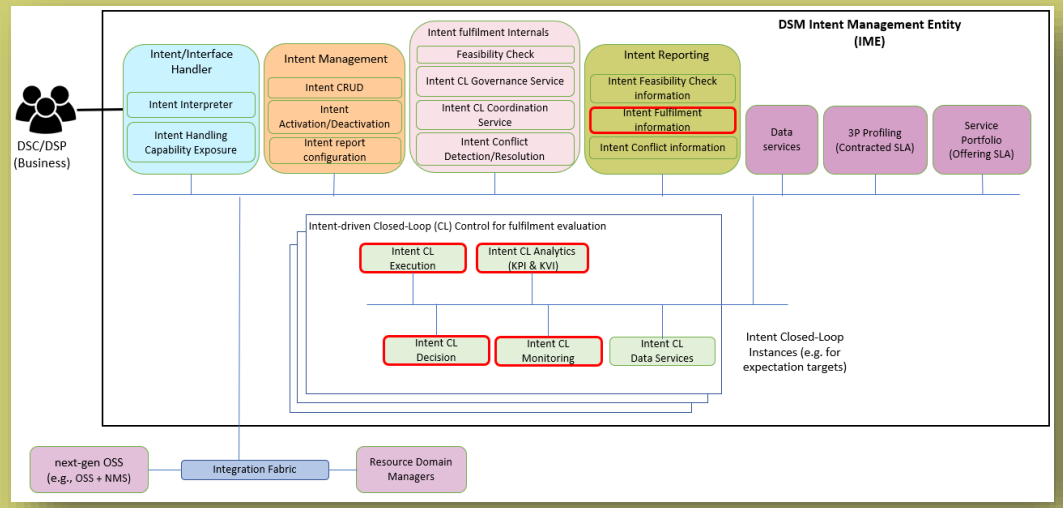
An end-to-end mechanism for intent monitoring, analysis, decision-making and execution

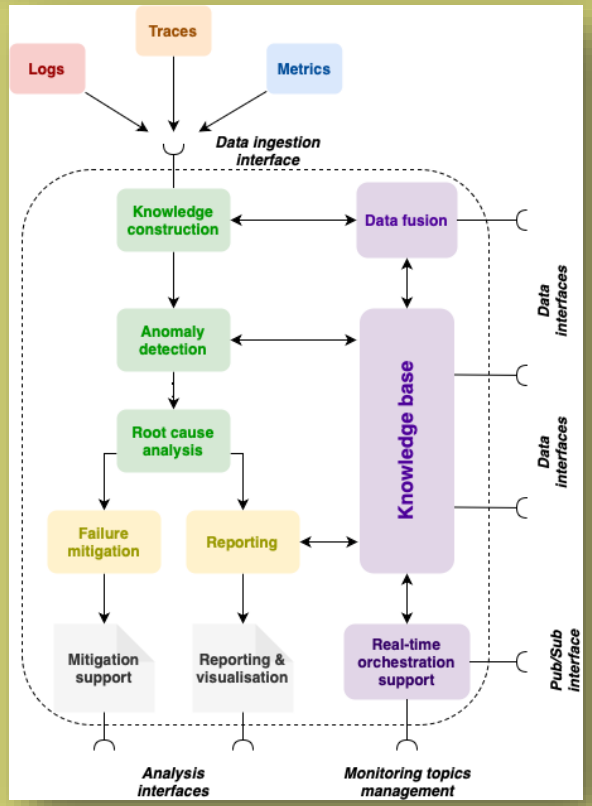
High-level description

Collection of heterogeneous observability signals based on OpenTelemetry standards for the early identification of anomalies and causality analysis.

Application, network and infrastructure failure identification and mitigation actions support.

Support for intent-based mechanisms at real-time and calculation of intent achieved values for intent fulfillment evaluation.





Closed loop coordination for intent management

Objectives

Aim at investigating and defining an IME integrated solution for the automatic coordination of multiple CL generated for the lifecycle management of the intents

Explore the possibility of interacting with other CL Coordination functions outside the IME scope

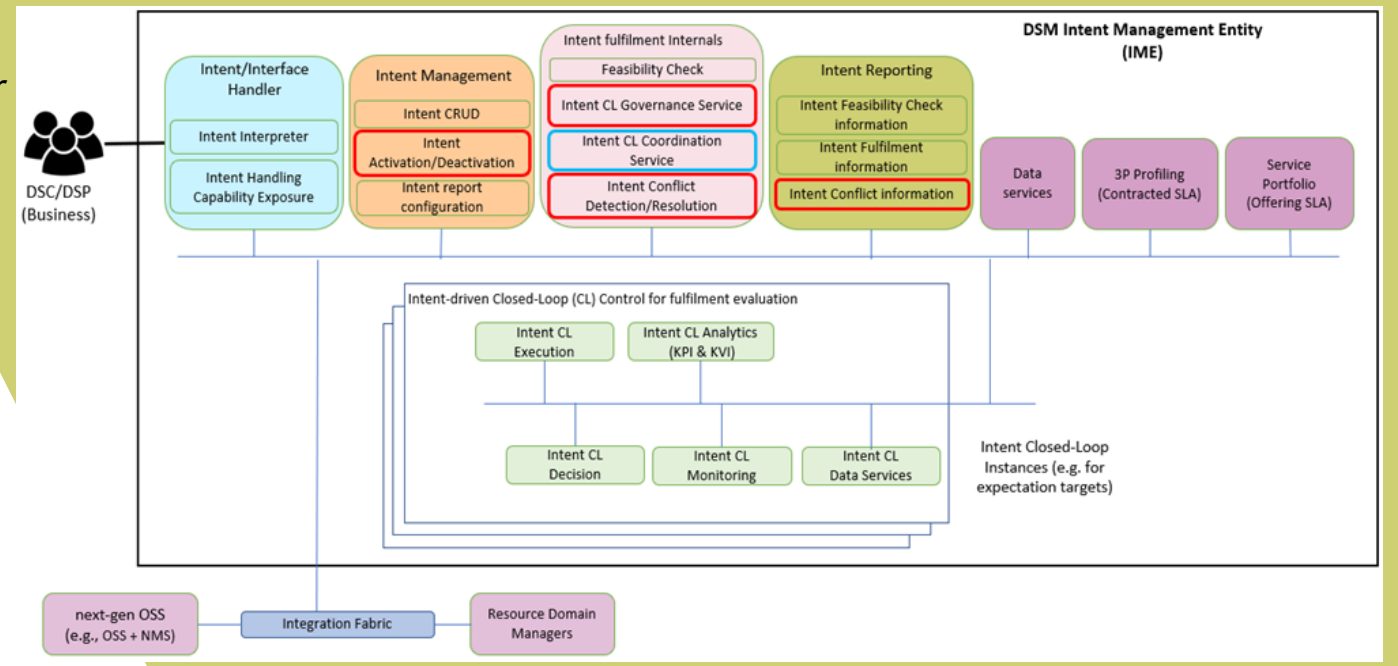
High-level description

Automatic management of multiple closed-loops at DSP Intent Management Entity, able to avoid/mitigate/resolve conflicts that may lead to system instability. Close cllaboration with Intent Conflict Administration (ICA) that detect potensital confilicts and provide instruction for their resoultion.

Conflicts can be detected at:

1. Intent creation
2. Intent Runtime

In 1) the Closed-Loop Coordination (CLC) executes specific actions (e.g., requets a new scheduling) to mitigate the conflict (if possible) or the basis of instruction received by ICA. In 2) CL concurrency issues may occur. In this case, the CLC needs to interact with the CL Governance(s) managing the potentially conflicting CLs, and tuning their execution (e.g., giving priority to a given CL by starting/stopping other CLs).



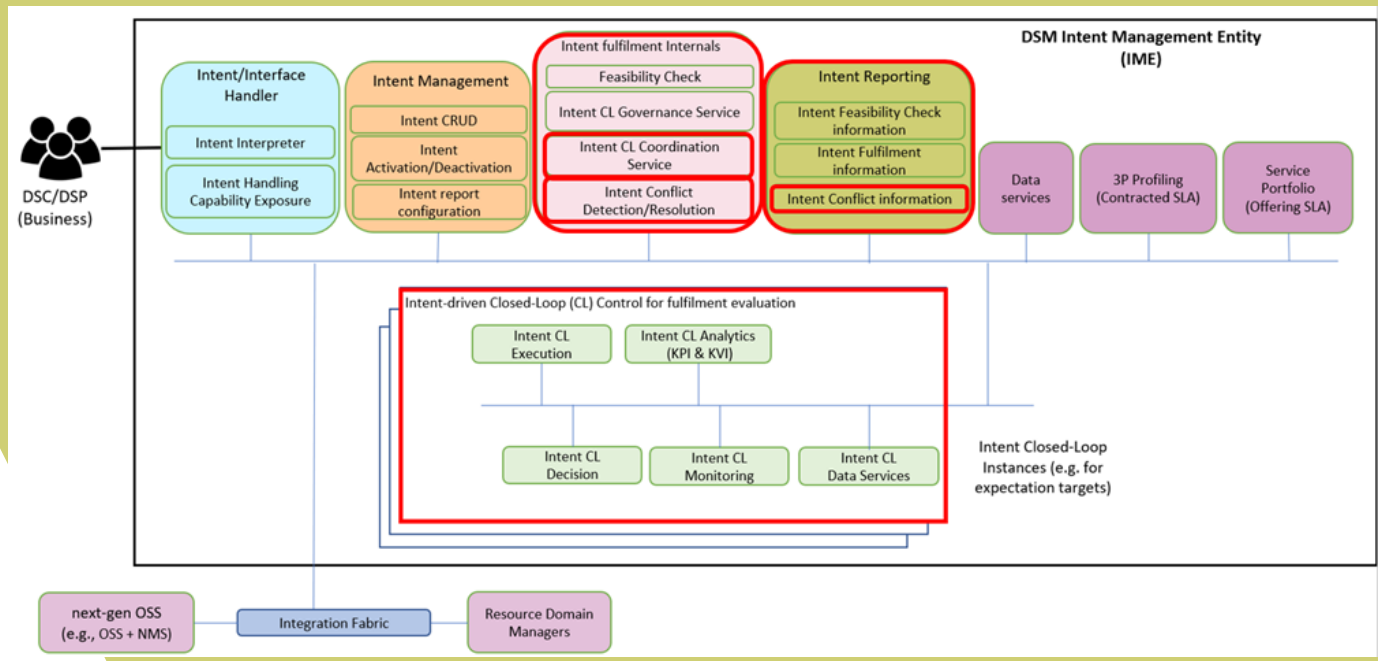
Intent conflict administration

Objectives

Detect conflicts between Intents and inform to the respective tenants. Provide solutions for Intent Conflict resolution.

High-level description

Different Intents that deployed in the network can have KPIs that affects negatively each other resulting in a conflict of Intents. Regarding the architecture mapping, as each Intent triggers a Closed-Loop, the Intent-driven CL is used such as the Intent CL Coordination service and Intent Conflict Detection / Resolution to detect and solve the conflict between Intents. The Intent Conflict Information is used to inform about the conflict of the Intents.



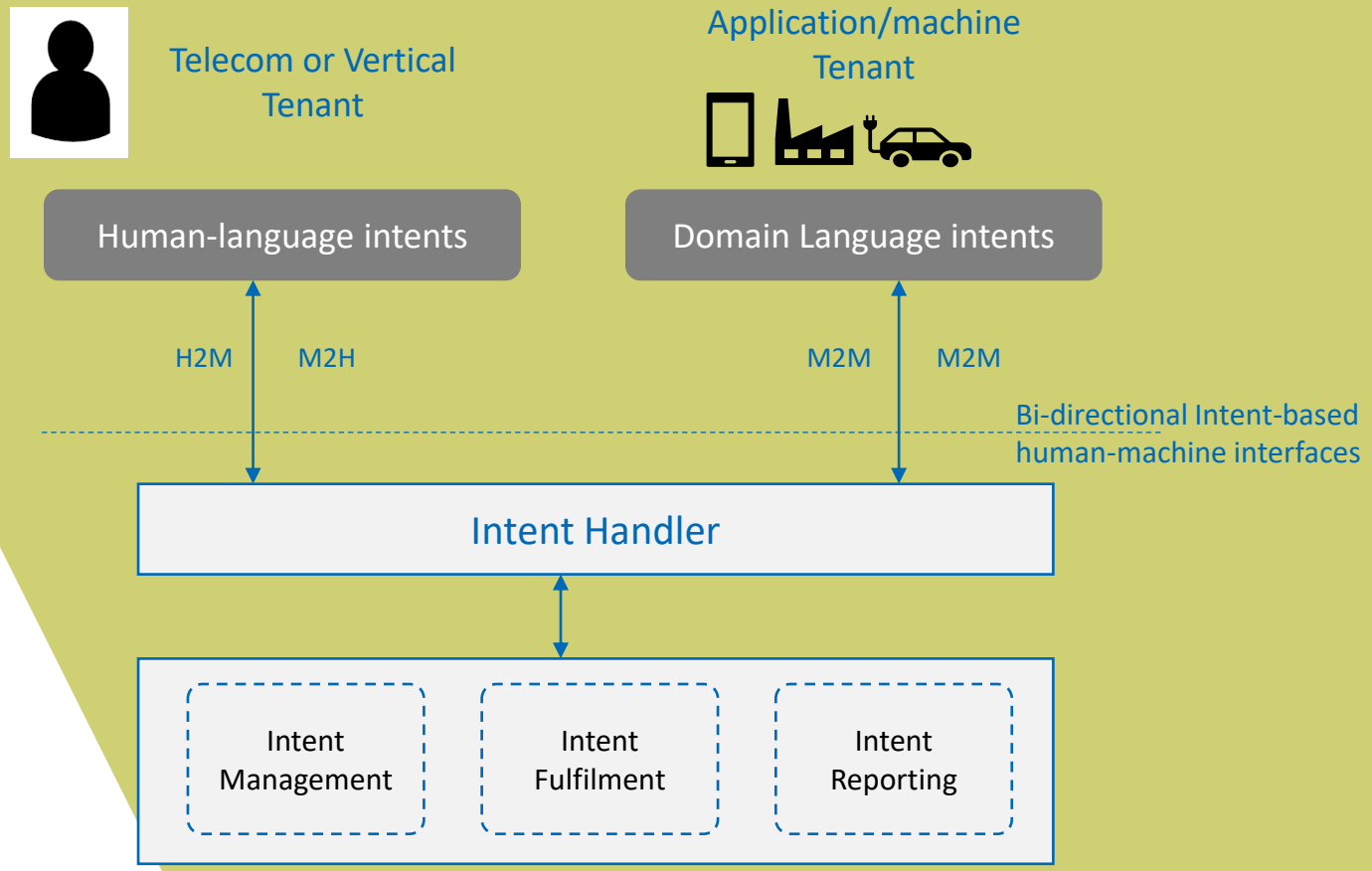
Human-machine intent interface design

Objectives

Fulfil the need for intent-based interfaces that allow expression of application's needs and requirements to networks, as well as system insights, feedback and actionable items back to applications.

High-level description

Enablement of dynamic interactions between applications and networks where application's needs are expressed efficiently, not necessarily in a native network language, whereas networks can adapt to human and application inputs and provide timely and meaningful feedback



Intent-driven placement

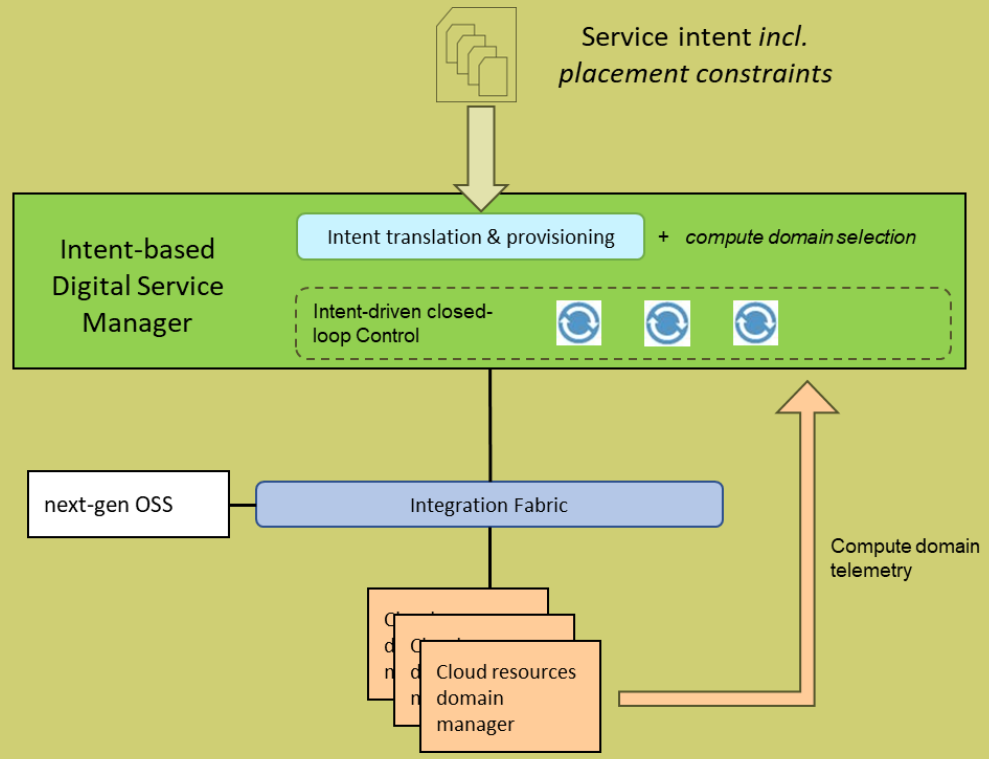
Objectives

Propose intent description extensions and associated analysis and decision mechanisms to steer high level (intra-DSP/cross-DSP) compute placement across the compute continuum

High-level description

Intent-based extensions to microservice descriptors to include target features of the infrastructure components on which these microservices are required to be deployed (or even explicit references to target execution domains)

Intent translation mechanisms for deriving the execution domain to contact and request orchestration from, while maintaining a closed-loop in charge of reacting to changes to adjust placement according to the intent expression



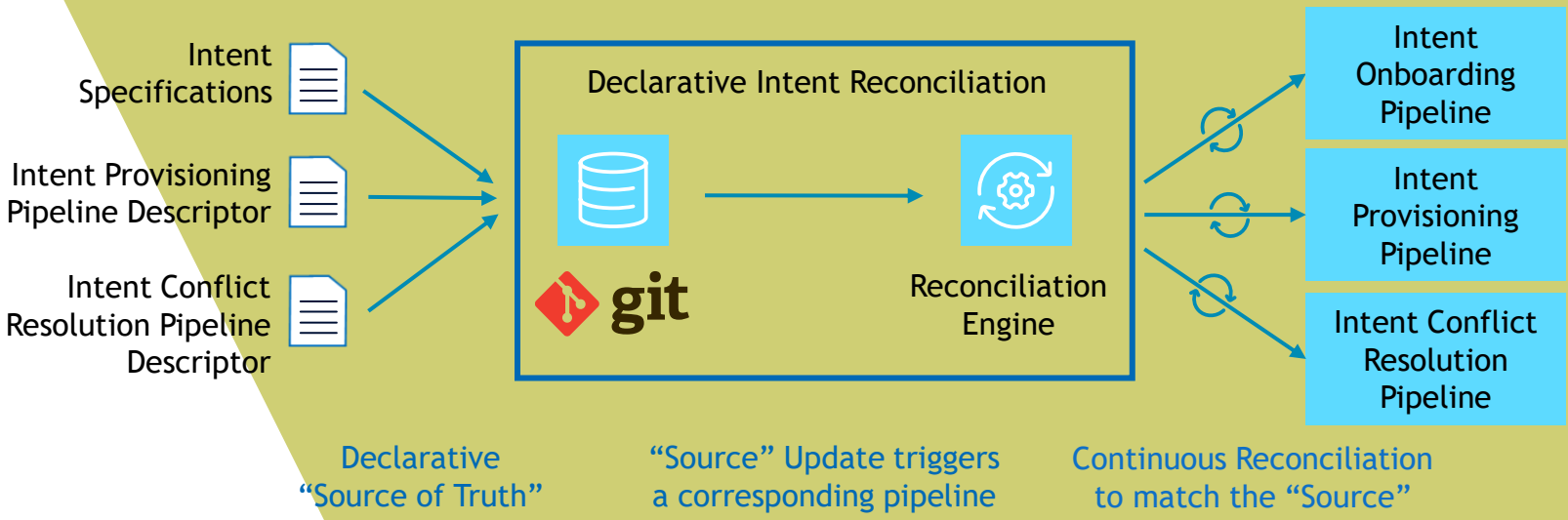
Declarative intent reconciliation

Objectives

- Manage intent parameters and intent life cycle across multiple management domains operated by different stakeholders.

High-level description

- Intent specifications and intent reconciliation pipelines are described, configured and version-controlled in a single source of truth.
- An intent update triggers corresponding pipelines to continuously reconcile the current intent deployment (actual state) to any changes declared in the source (desired state)
- Role-based Access Control for Intent Modification/Notification/View



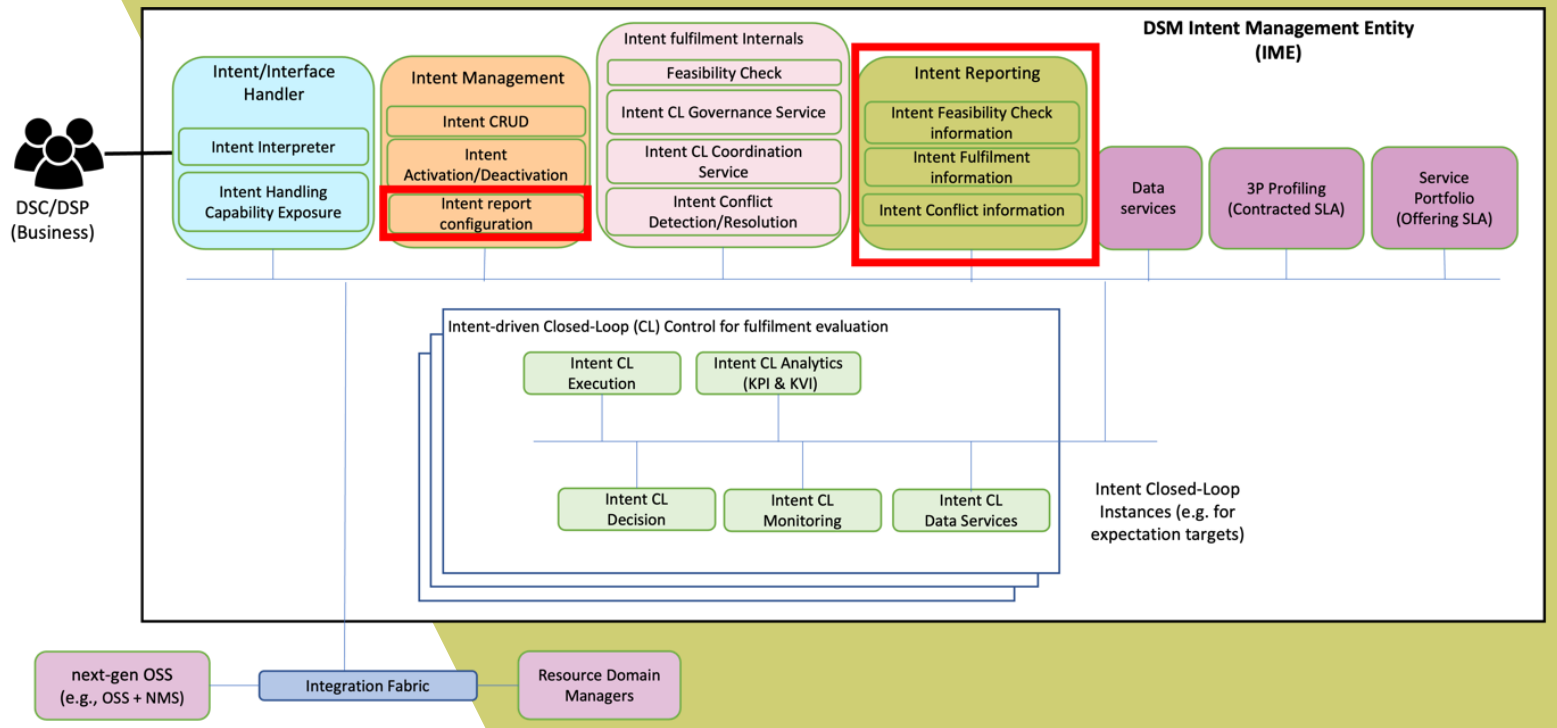
Intent reporting

Objectives

Provide means for the tenant (intent owner) to verify and audit that the intent gets fulfilled across the entire lifecycle. The DSP (intent handler) informs according to the reporting conditions that the tenant has defined for that intent.

High-level description

- Define an information model for the intent report. This model will allocate report information (fulfilment information, conflict information, feasibility check information) into well-defined constructions connected through class relationships.
- Solution design of advanced reporting features, to cope with the specific needs of Hexa-X-II tenants with regards to:
  - Consumption patterns (query vs subscribe-notify)
  - Intent report content and triggers
  - Intent report observation period



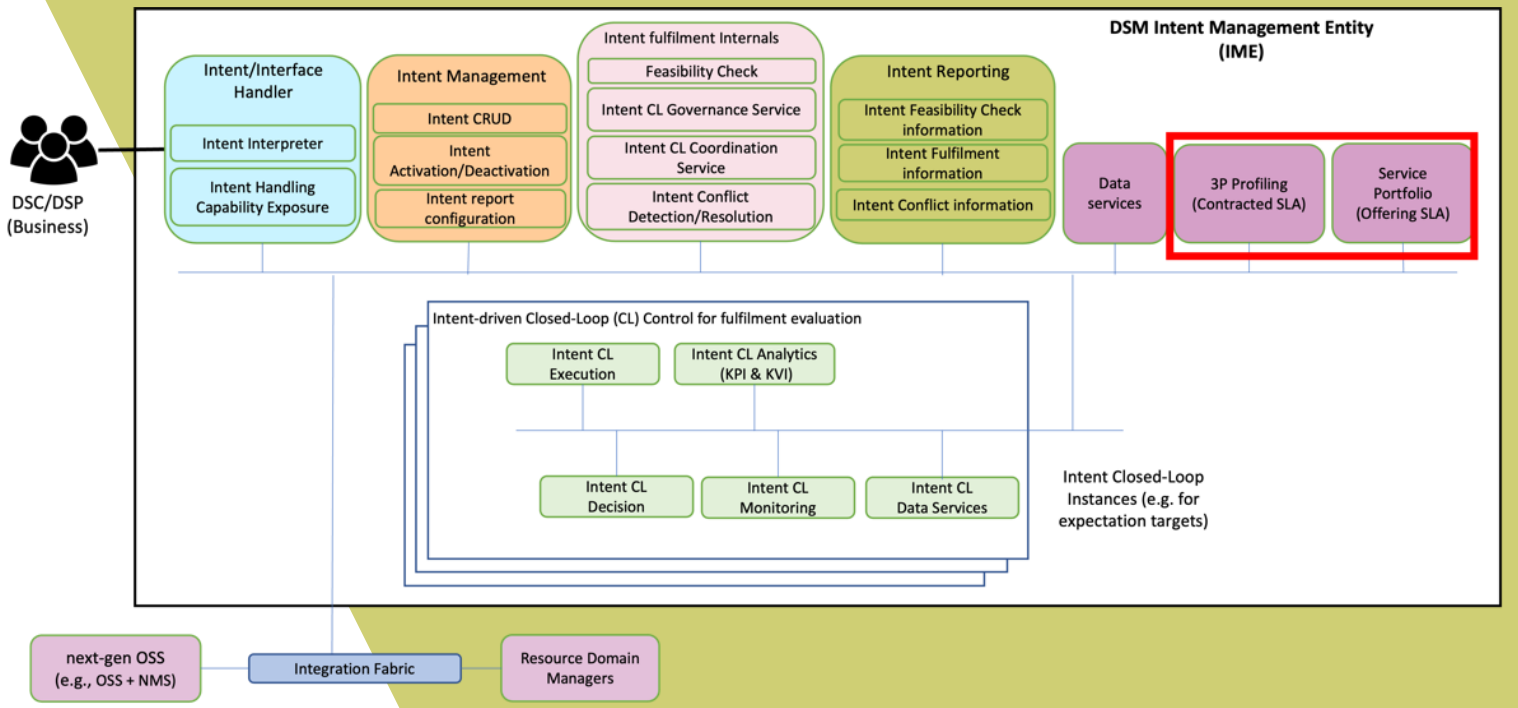
3rd party facing services

Objectives

Provide solutions that allows profiling tenants and service offerings under the DSP realm

High-level description

- Characterisation of individual tenants accessing the Hexa-X-II system, capturing this information in the form of 3rd party (3P) profile. This profile specifies i) tenant type, ii) 3P supported credentials and access control, iii) 3P trust level, iv) contracted services, v) information on 3P subscribers.
- Characterisation of DSP service offerings (service name, service status, service owner, flavors, costs & pricing, dependencias w/ other services). These offerings Will be later linked to tenants according to well-defined SLAs.



Chapter 5
Enablers related to security, privacy and sytem level resilience

Mechanisms related to security, privacy and system level resilience

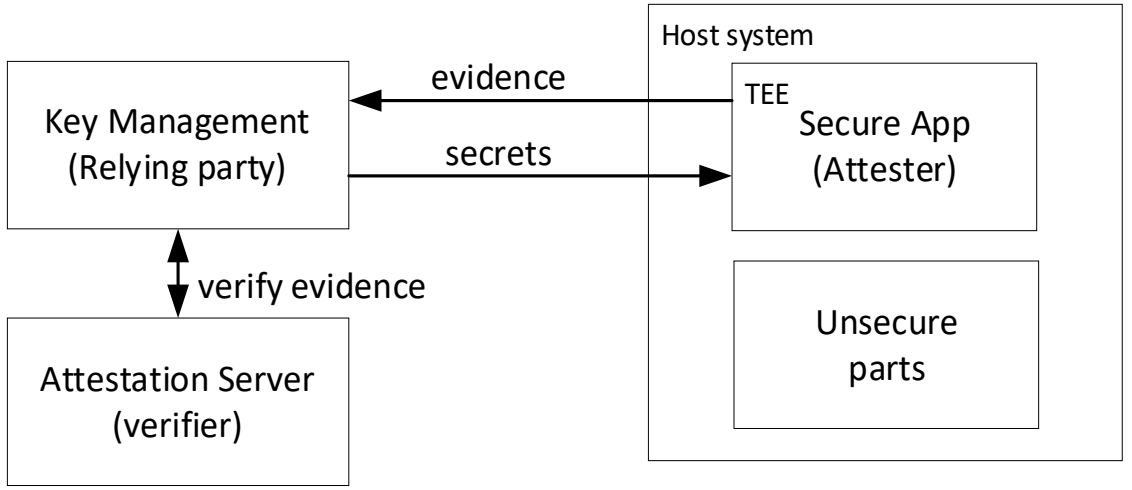
- On the Nature of Security/Privacy/Resilience Enablers
- Architectural Enablers
- Enablers for Trustworthy AI
- Enablers for Trust Infrastructures
- Physical Layer Security Enablers
- Validation Methods. Simulation
- Validation Methods. Network Digital Twin

On the Nature of Security/Privacy/Resilience Enablers

- Not necessarily intended to provide a new, differential functionality
  - But to address specific threats
  - Providing mechanisms to detect them and to mitigate their impact
  - Enabler analysis requires identifying and describing the potential threats
- Structured along the *threat families* they intend to address
  - Foreseen architectural trends
  - Pervasive use of AI
  - Mechanisms to evaluate trustworthiness and establish trust
  - Physical layer evolution and new paradigms
- Concluding by an analysis of the proposed mechanisms to validate these enablers
  - Simulation
  - Emulation by means of synthetic environments (*Network Digital Twins*)
  - And their combination for enhanced validation

Architectural Enablers

- Key trends with high security impact
  - The NoN (*Network of Networks*) concept
    - Integration of different NSPs, with limited information exchange
  - The Cloud Continuum
    - Isolation, observability, transitivity…
  - Disaggregation, especially in RAN
    - Expansion of the attack surfaces
- Addressing these issues by
  - Formal Specifications and Formal Security Proofs
    - Supporting (automated) formal reasoning to evaluate trustworthiness
    - While keeping understandability
  - Confidential deployments
    - Confidential computing and measured boot
    - Identity provisioning and key management
    - Confidential container and workload provisioning
    - Topology attestation and path validation
    - Supply chain integrity



Enablers for Trustworthy AI

- AI security implications
  - Attack surface on models and (especially) data
  - Pervasiveness increases impact and complicates detection
  - Go beyond black-box AI, and move towards explainable AI (XAI)
    - Better understand attack surfaces and detection mechanisms
    - Enhance transparency and auditability
    - Improve trustworthiness, *demystifying* AI decisions
- AI privacy implications
  - Avoid exposure of sensitive data of any nature
    - At any stage: training data, inference query, inference result, AI/ML model…
  - Advance in data protection mechanisms: multi-party computation, homomorphic encryption, and differential privacy
  - Generalize federated learning approaches
  - Extend confidential computing to AI
- Be aware of the required balances
  - Privacy and security
  - Security and performance

Enablers for Trust Infrastructures

- Consider issues regarding how trust on network services is established
  - Not strictly 6G issues, but to be addressed in the 6G development timeframe
  - Going beyond traditional assurance
    - Including trustworthiness as a *measurable* KVI
    - Make it part of service levels, aligned with intent
    - Support users in assessing their trust on a particular service
- Address the transition in cryptography
  - As base methods evolve
  - *Agility*, allowing a seamless evolution
  - *Pliability*, adapting to management best practices
- Distributed ledgers
  - As a source of evidence and reputation for Level of Trust assessment
  - As support for *smart contracts*, enforcing agreements
  - As enabler for decentralized identity management

Physical Layer Security Enablers

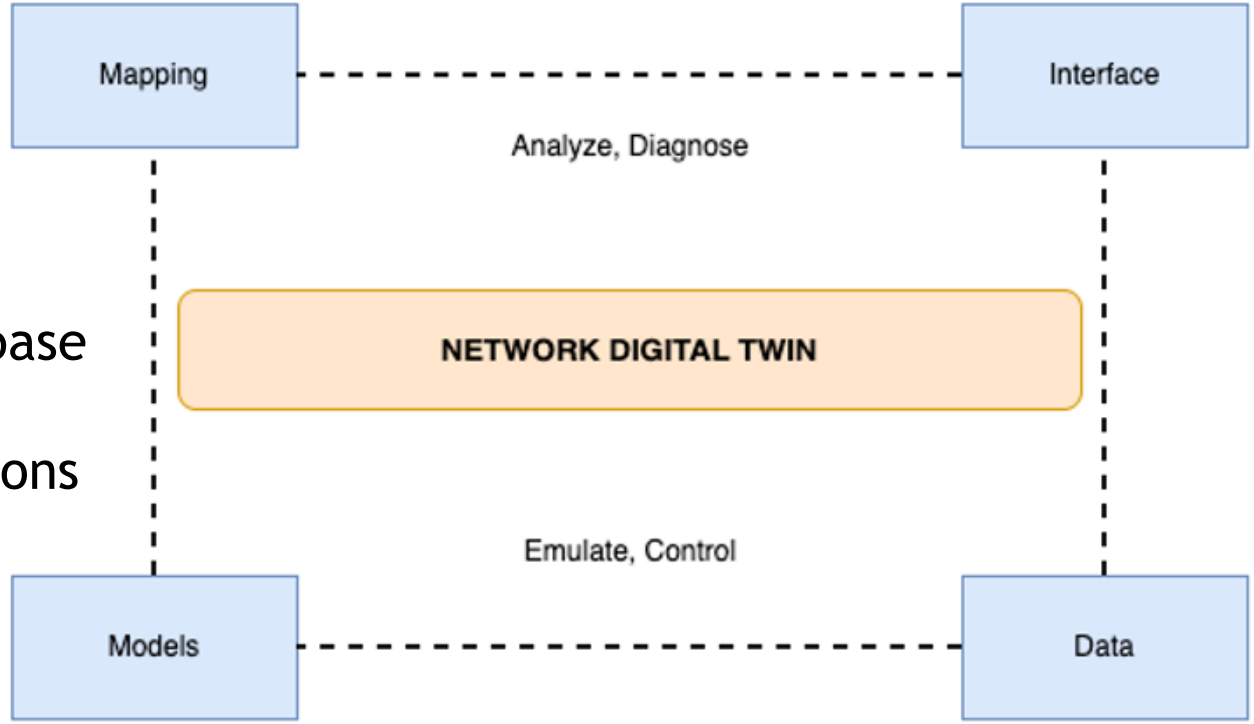
- Extending the threat analysis and mitigation mechanisms to the physical layer
- AI vulnerabilities plus the use of malicious AI
  - Applying general AI protection measures
- Context awareness
  - Adapt secret key generation rate according to current and past channel measurements
- Security and privacy issues in JCAS
  - Focus on securing the sensing process, rather on applying JCAS to security goals
  - CIA (Confidentiality, Integrity, and Availability) of the sensing data flows
  - Applicability and scope of consent mechanisms for JCAS privacy preservation
- Sources of physical anomalies
  - Understanding, detection, classification, and localization of jammers, beyond SoA
  - Time-frequency analysis and machine learning for analysis/classification of jamming types
  - Using DT emulation, where differences in digital and physical twin would indicate anomalies

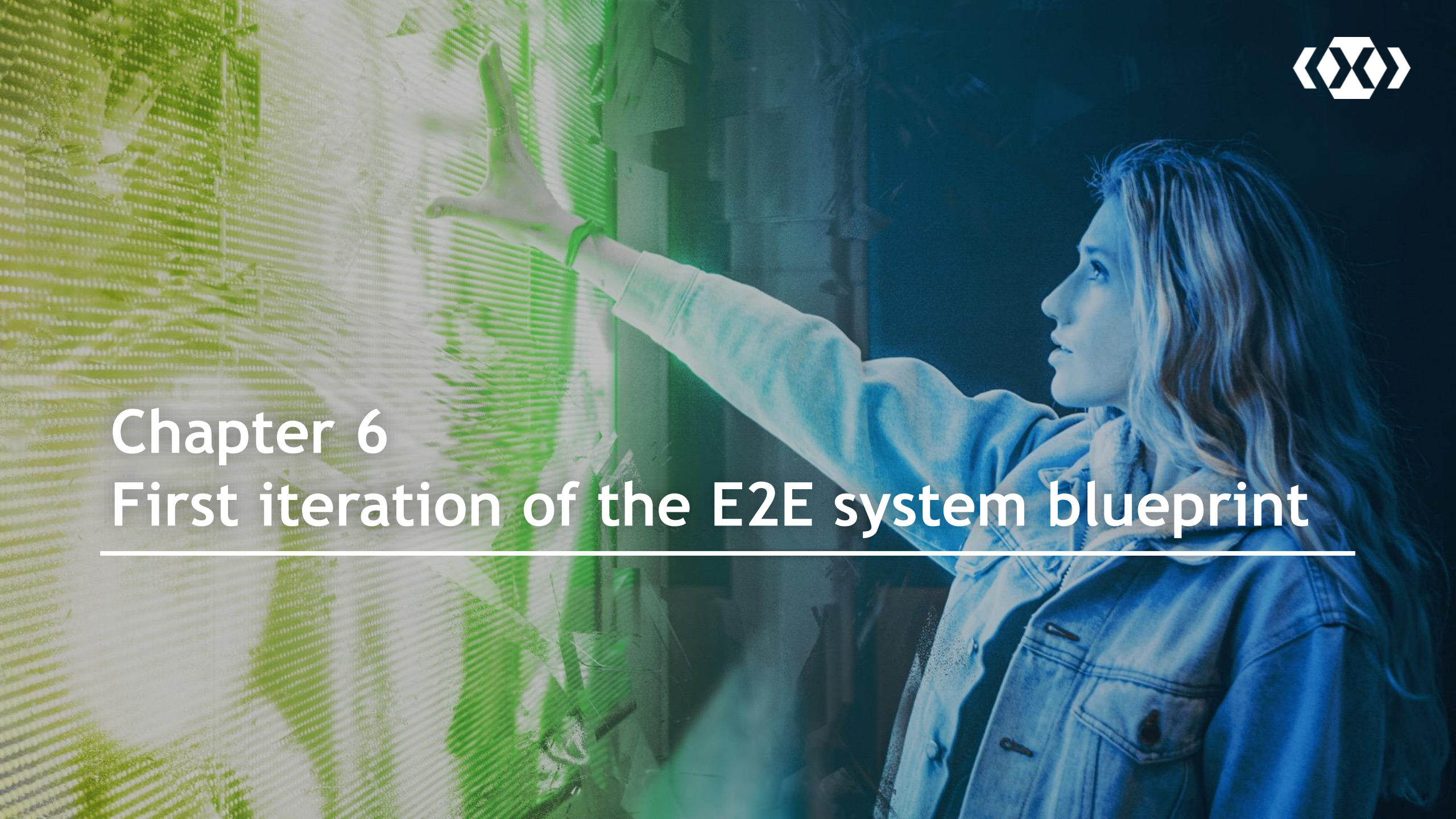
Validation Methods. Simulation

- Simulation-based resilience assessment environment
  - Based on discrete-event simulation
  - Using a model of the communication service connecting the modules
  - Threats are injected either as events or as irregular behaviors of the events
  - Internal failure of the network, represented by a network failure module
  - External threats of traffic variation (peaks)
  - The environment can be extended to adapt to other threats
  - The goal of the environment is to obtain KPIs and KVIs from simulation
  - A large number of simulations is envisaged to generate more variant risk scenarios
- Validation mechanisms for sources of physical anomalies
  - Exercise both phases on a simulated environment
  - Localization of the jamming sources
  - Classification of the jamming signal

Validation Methods. Network Digital Twin

- A general environment for security experimentation on a synthetic, emulated environment
  - Based on the IETF reference architecture for NDT
  - Focused on the first phase of the NDT methodology
    - No real 6G networks or threats available yet
  - Synthetic data modeling
    - Using current network deployments as base
  - Descriptors for experiments to guarantee
    - Reproducibility, to allow similar executions by other parties
    - Repeatability, to allow successive executions with controlled variations
- The specific case of DT-based physical anomaly detection
  - A first step towards NDT-simulation integration





Chapter 6
First iteration of the E2E system blueprint

Identification of key criteria for enabler integration in E2E system

- Relevance and significance of enabler towards E2E system design
- Impact of the enabler on the E2E system design
- How the enabler fits with the system design principles
- Feasibility (estimation) of enabler vs migration options
- Dependency with other enablers
- Any proposed updates to E2E system design and architecture design principles
- Network performance, security/privacy, flexibility, resilience/robustness, and sustainability/energy efficiency

Analysis of enablers for integration in E2E system

Intent-based management automation

1. Intent translation and provisioning
2. Data fusion mechanisms based on telemetry data
3. Closed loop coordination for intent management
4. Intent conflict administration
5. Human-machine intent interface design
6. Intent-driven placement
7. Declarative intent reconciliation
8. Intent reporting
9. 3rd party facing services

Smart network management and automation

1. Programmable and flexible network configuration
2. Programmable network monitoring and telemetry
3. Integration fabric
4. Trustworthy 3rd party management
5. Multi-cloud management mechanisms
6. Orchestration mechanisms for the computing continuum
7. Sustainable AI/ML-based control
8. Trustworthy AI/ML-based control
9. Network Digital Twins
10. Zero-touch closed loop governance
11. Zero-touch control loop coordination

Architectural enablers for cloud transformation

1. Integration and orchestration of computing continuum resources into the 6G architecture
2. Multi-domain/multi-cloud federation
3. Network modules placements in the resource continuum
4. Cloud transformation in 6G-quantum architecture

Architectural enablers for network function modularization

1. Optimized network function composition
2. Streamlined network function interfaces and interaction
3. Flexible feature development and run-time scalability
4. Network autonomy and multi-X orchestration

A preliminary set of Hexa-X-II enablers that have been identified as important technology innovations for the use case of cobot cooperating in the context of an industrial environment that is under study in the system-PoC A and B.

Recommendations for enabler integration in 6G E2E system

Recommendations related to enabler integration in 6G E2E system

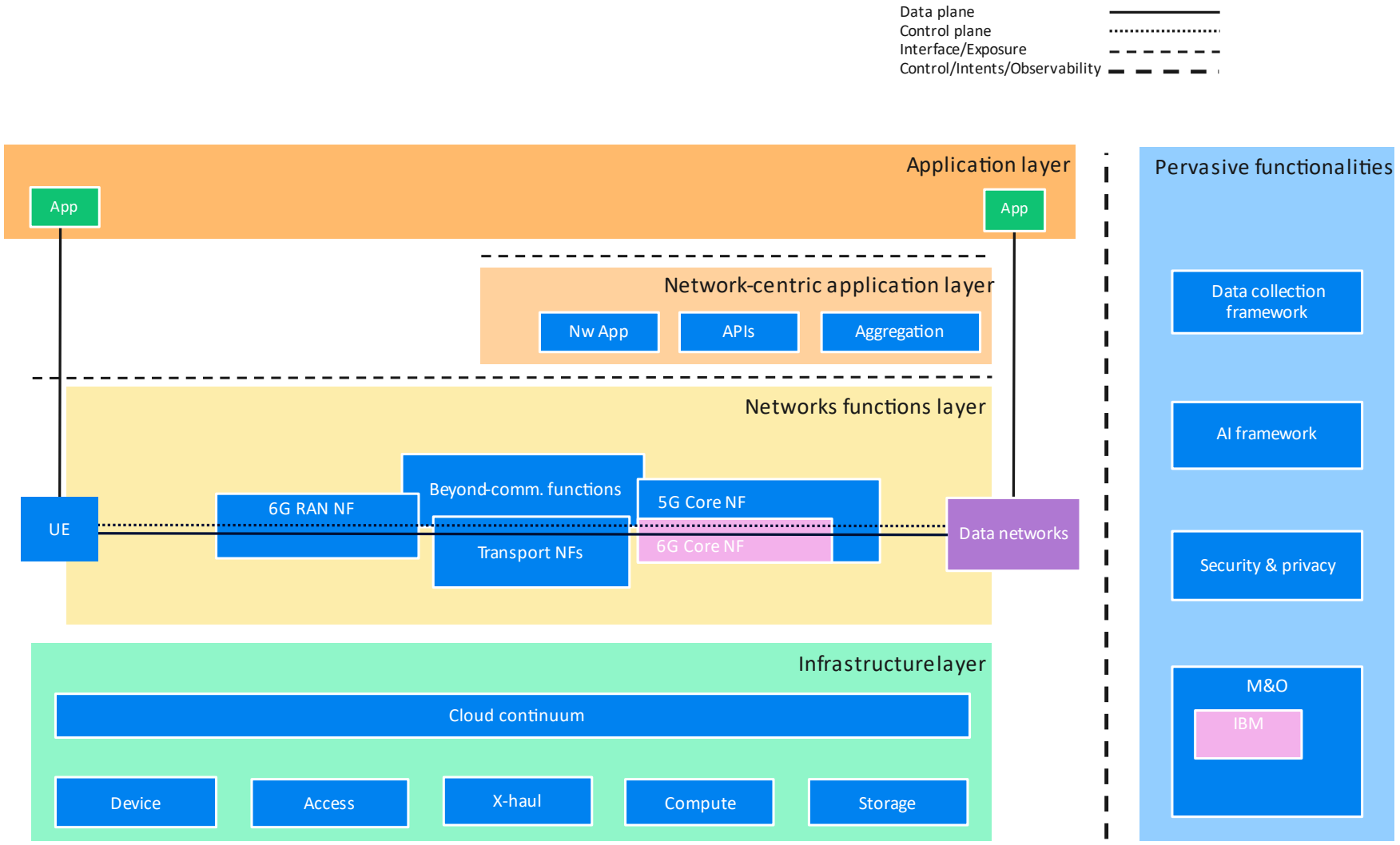
- Investigate potential synergies between different enablers addressing similar aspects and functionalities
- Refine the architecture enablers with well-defined new functionalities and interfaces for all the different options envisaged, and the implementation solutions of components, processes, or algorithms enablers.
- For the integration in the 6G system blueprint, select only enablers that fit with the migration path from 5G to 6G are selected.
- Identify further criteria to analyze enablers in the next iteration
- Incorporate any implications on the security, privacy or general resilience impact the enabler may have, any correction measure that can be applied to address these impacts (using guidelines from chapter 5 enablers)

Recommendations related to enabler integration in E2E system-PoC

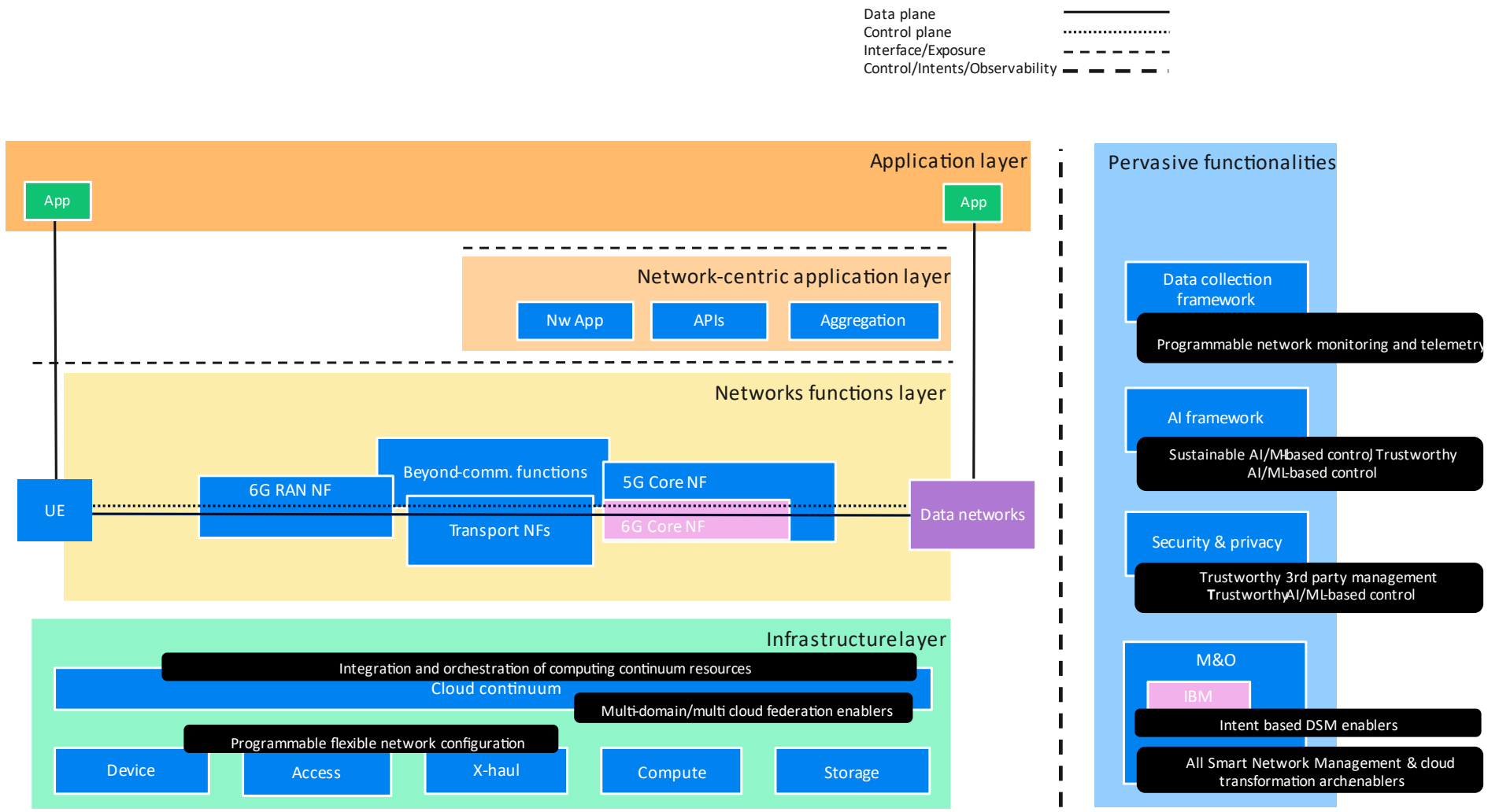
- Not all enablers will be integrated into the system PoC (insufficient technology maturity)
- Even if not integrated, provide a mapping of each enabler to the system-PoC's implementation architecture.
- Narrow-down multiple development options while evolving the enablers, and consider the ones that best serve the E2E functionalities from an architectural perspective
- Adopt a common data schema for all the involved systems, infrastructure, nodes, application components, etc
- For trustworthy AI/ML-based control it is recommended to harden the AI model to be robust against adversarial attacks.
- It is important to ensure the privacy of user in AI-based systems to enhance user trust and adoption to such systems.

Update on overall 6G E2E system blueprint

- RAN NF is re-named as 6G RAN NF.
- New core NFs specific to 6G are represented as 6G Core NFs.
- Infrastructure and Compute layer has been replaced to the infrastructure layer.
- Introduce the IBM block within the M&O block to represent intent-based management (IBM) enablers which are analyzed in detail.
- Removal of sub-network feature, as its presence depends on deployment scenarios



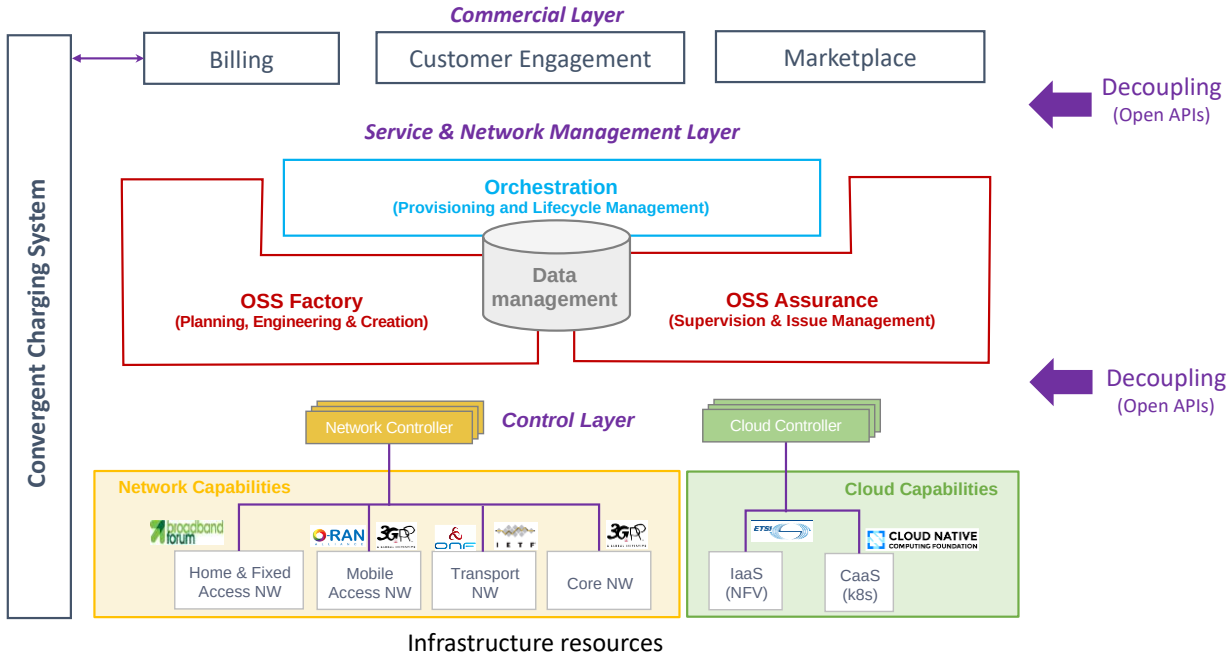
Mapping of management and orchestration enablers in E2E system blueprint



Representations the set of enablers analyzed in the first iteration that are part of the M&O view of the 6G E2E system blueprint.

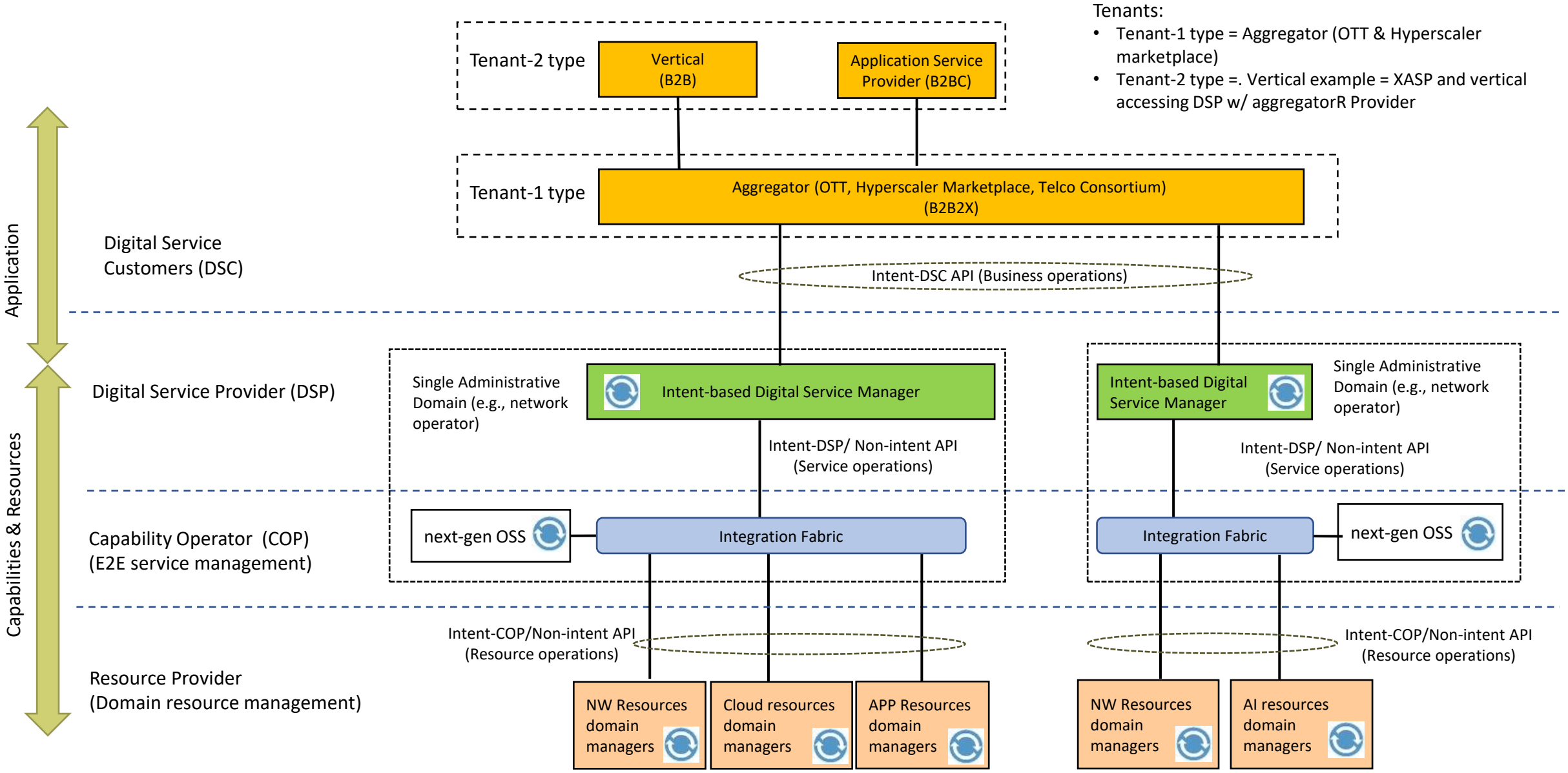
E2E intent-based service management automation framework

- Tier-1 telcos (i.e., large mobile network operators worldwide) typically structure their OAM systems as shown in figure.
- Telco federation approaches are required when there exist multiple network administrative domains and need to maintain consistent E2E path betwenn service endpoints.
- In the 6G ecosystem, it is expected for Tier-1 telcos to become TechCos, with a wider scope on service offerings, and further flexibility on the composition and operation of managed resources.
- TechCos service offering contains both communication and digital services.
- TechCos break functions into microservices each representing stand-alone capabilities
  - Allow offloading models in telco industry
  - Motivate the decomposition of the NOP role into capability operator (COP) and resource provider roles.



Baseline telco Operation and Maintenance (OAM) system architecture.

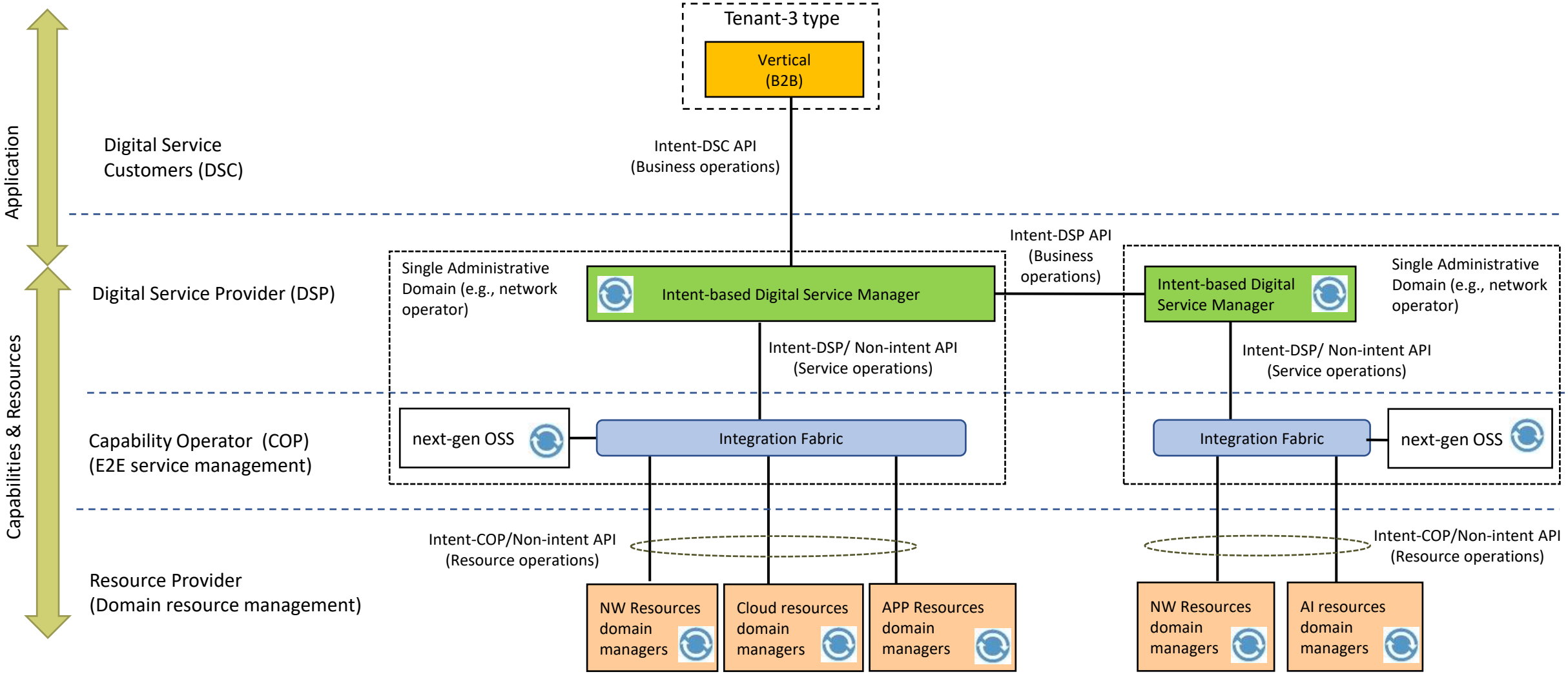
E2E intent-based service management automation framework (Option A: DSP aggregation)

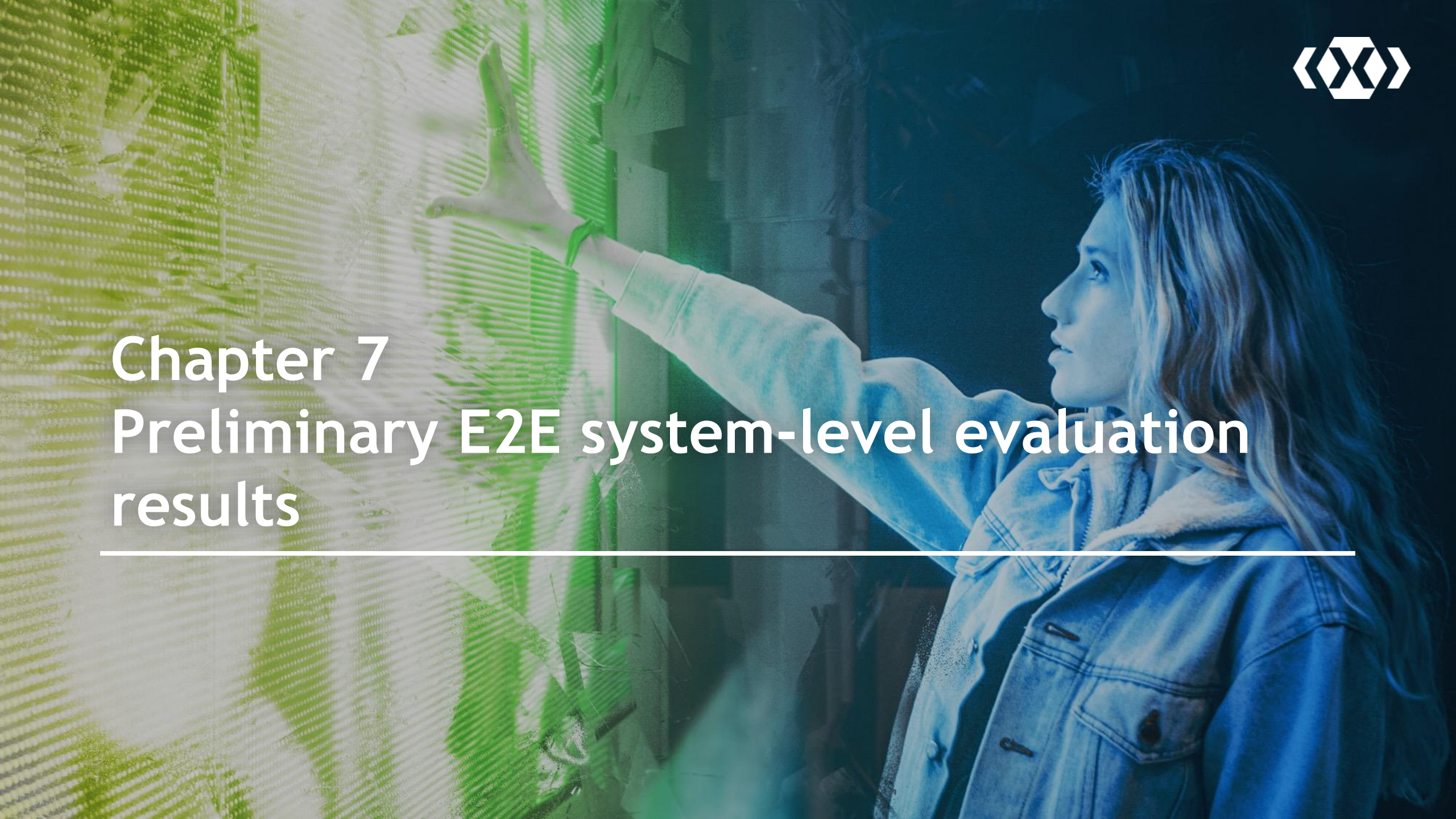


E2E intent-based service management automation framework (Option B: DSP federation)

Tenants:

- Tenant-3 type = vertical accessing DSP w/o aggregator. Vertical example = banking.





Chapter 7
Preliminary E2E system-level evaluation results

System-PoCs evolution

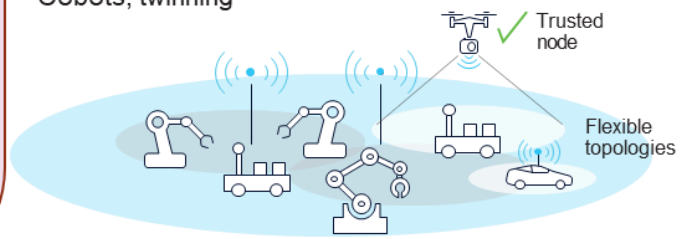
Key enablers

KVI: **Sustainability, trustworthiness (resilience)**	
Management and orchestration	Diagnostics intent
Network architecture and transformation Trustworthy flexible topologies, Beyond communications	
6G device components	6G radio aspects

Cobots

KVI: Sustainability, trustworthiness (resilience) and **inclusion**	
Management and orchestration	Diagnostics intent
Network architecture and transformation Trustworthy flexible topologies, Beyond communications	
6G device components	6G radio aspects

Cobots, twinning



KVI: Sustainability, trustworthiness (resilience) and inclusion	
Management and orchestration	Diagnostics intent
Network architecture and transformation Trustworthy flexible topologies, Beyond communications	
6G device components	6G radio aspects

Cobots, twinning, XR, IoSenses

6G

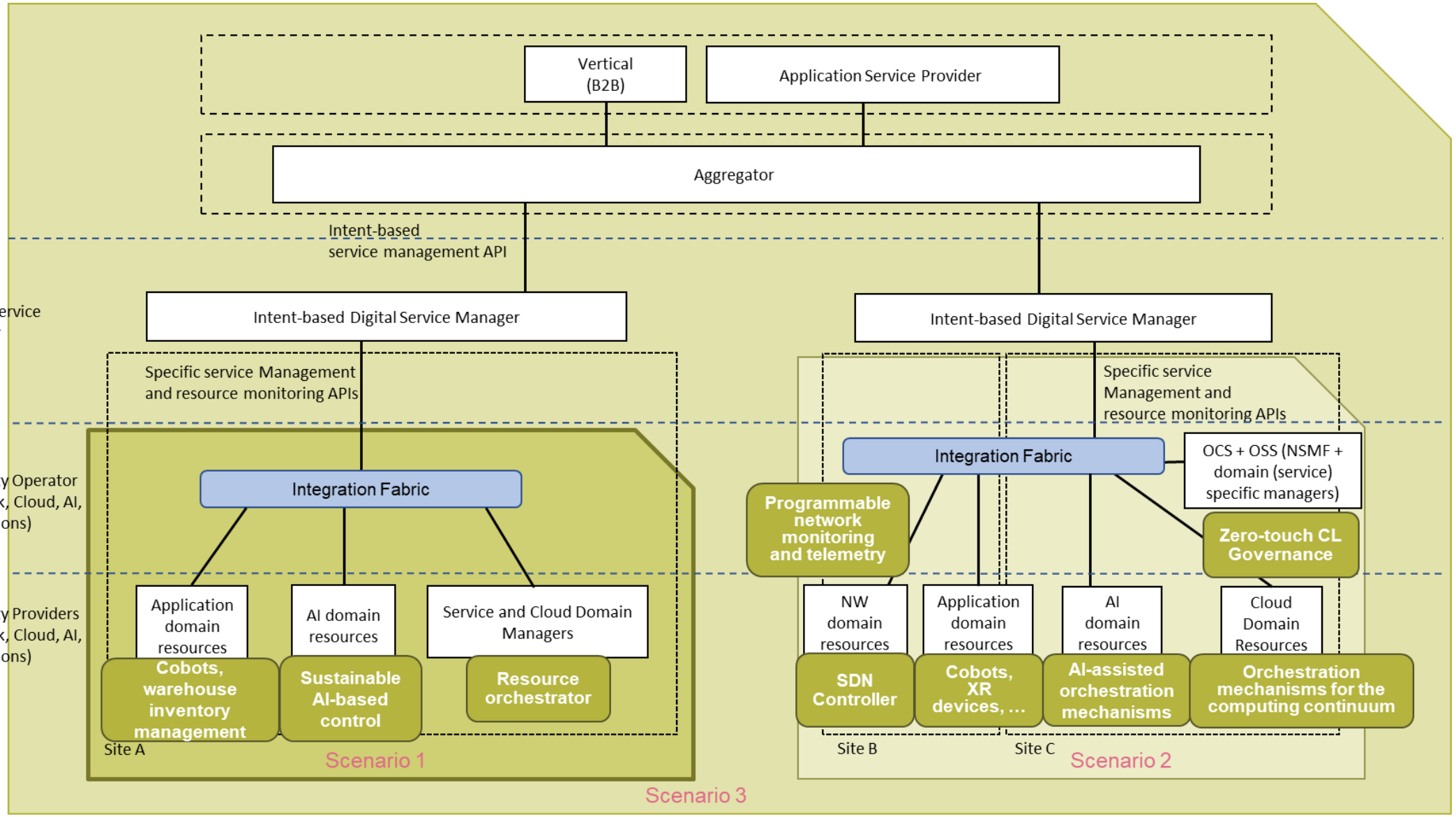
Gradual addition

System-PoC A focuses on aspects for demonstrating management mechanisms.

System PoC-B focuses on network architecture elements and refinements of management.

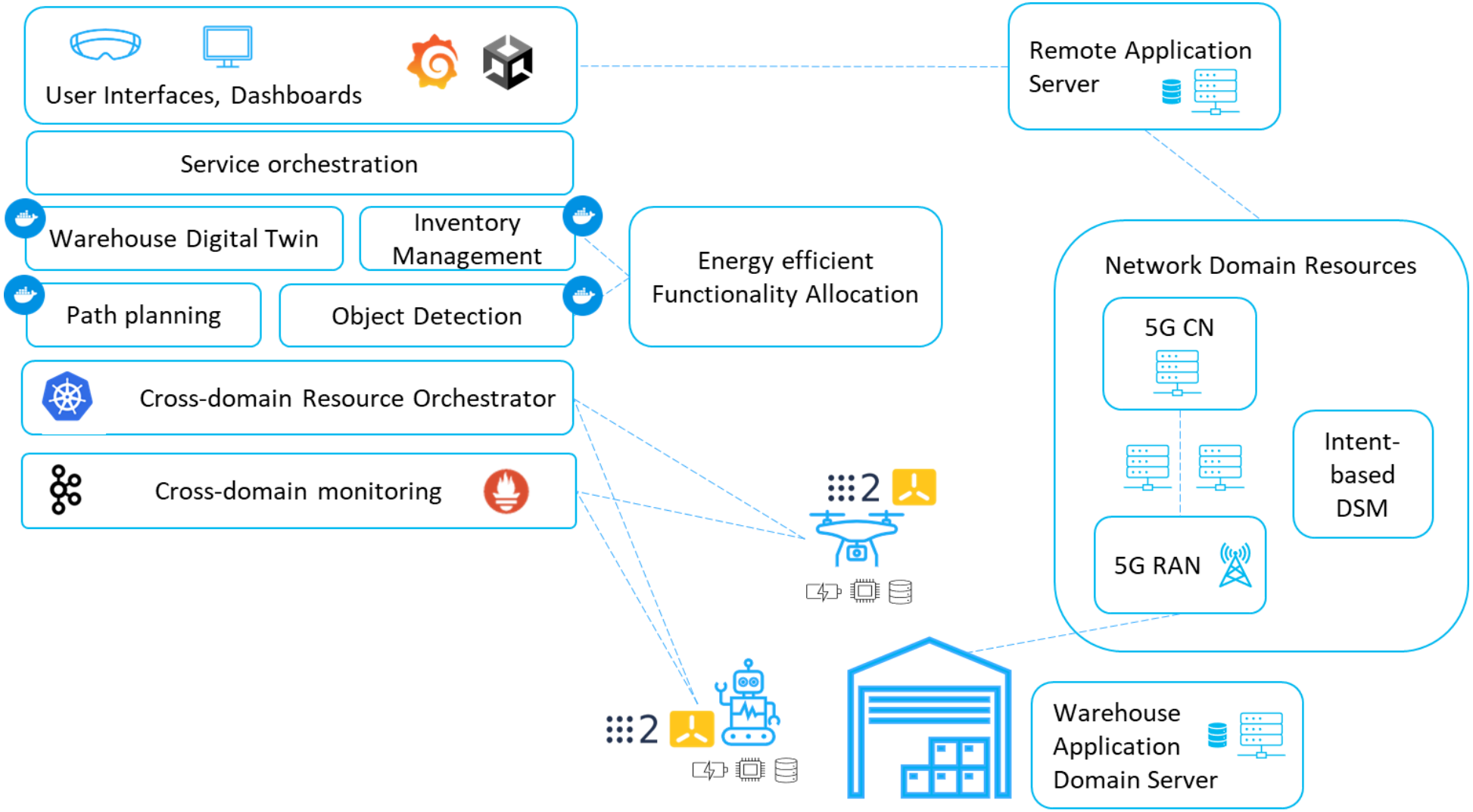
System-PoC C focuses on radio and devices aspects.

Scenarios for E2E system evaluation and validation



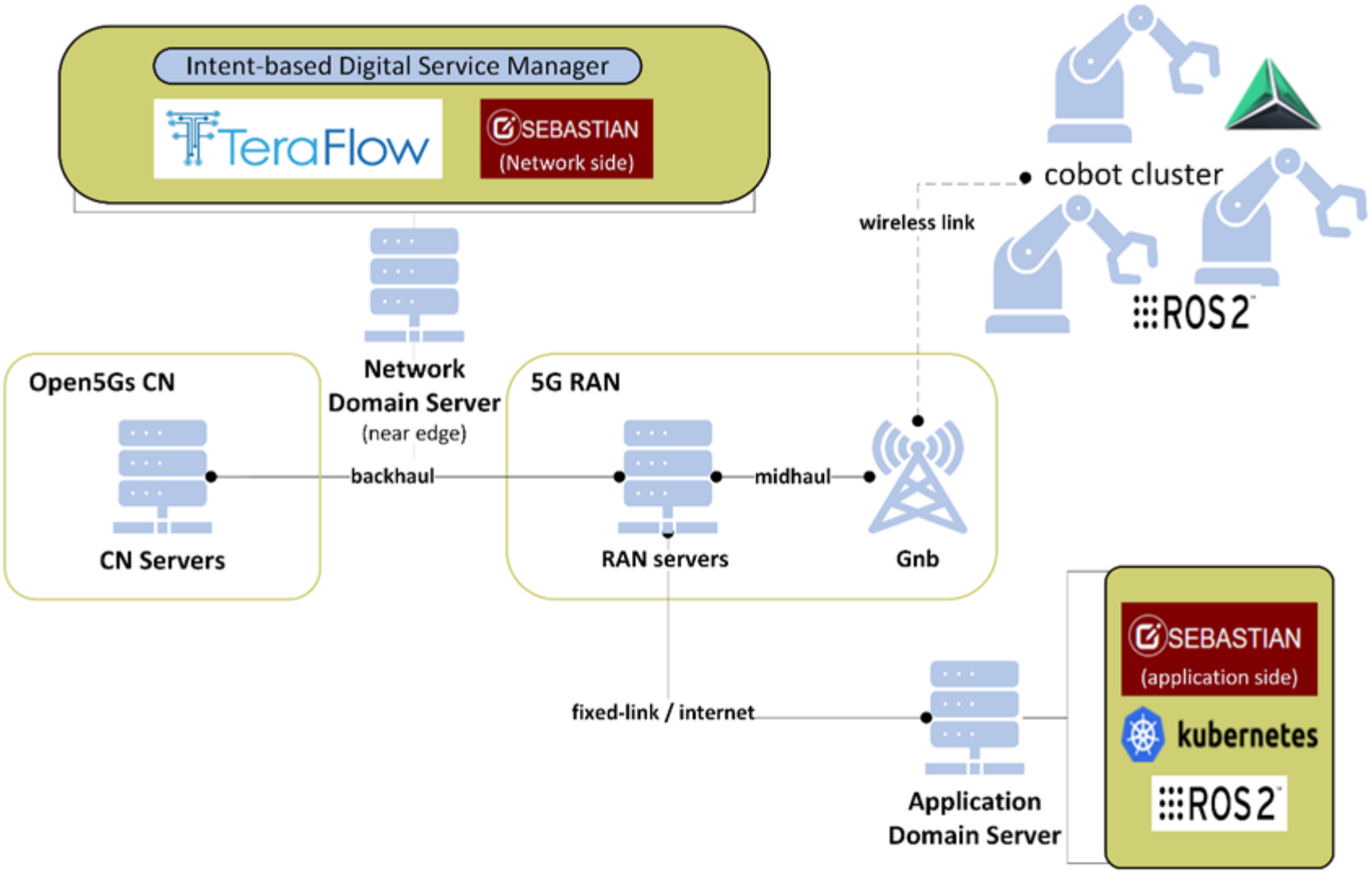
System-PoC A: E2E architecture (1st configuration)

1st configuration of system-PoC A architecture for the warehouse inventory management.



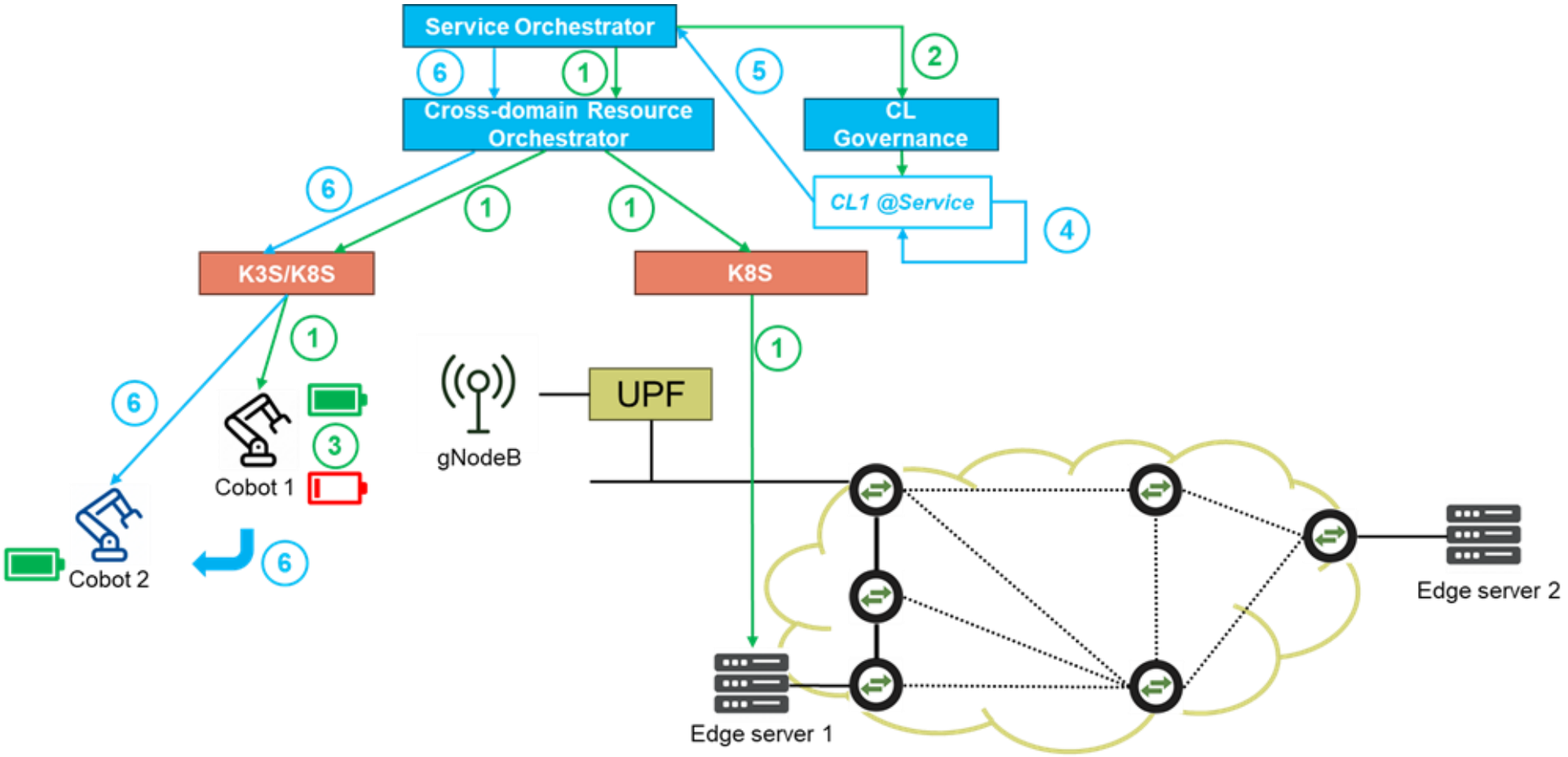
System-PoC A: E2E architecture (2nd configuration)

2nd configuration of system-PoC A architecture for task continuity and remote repairing scenarios.



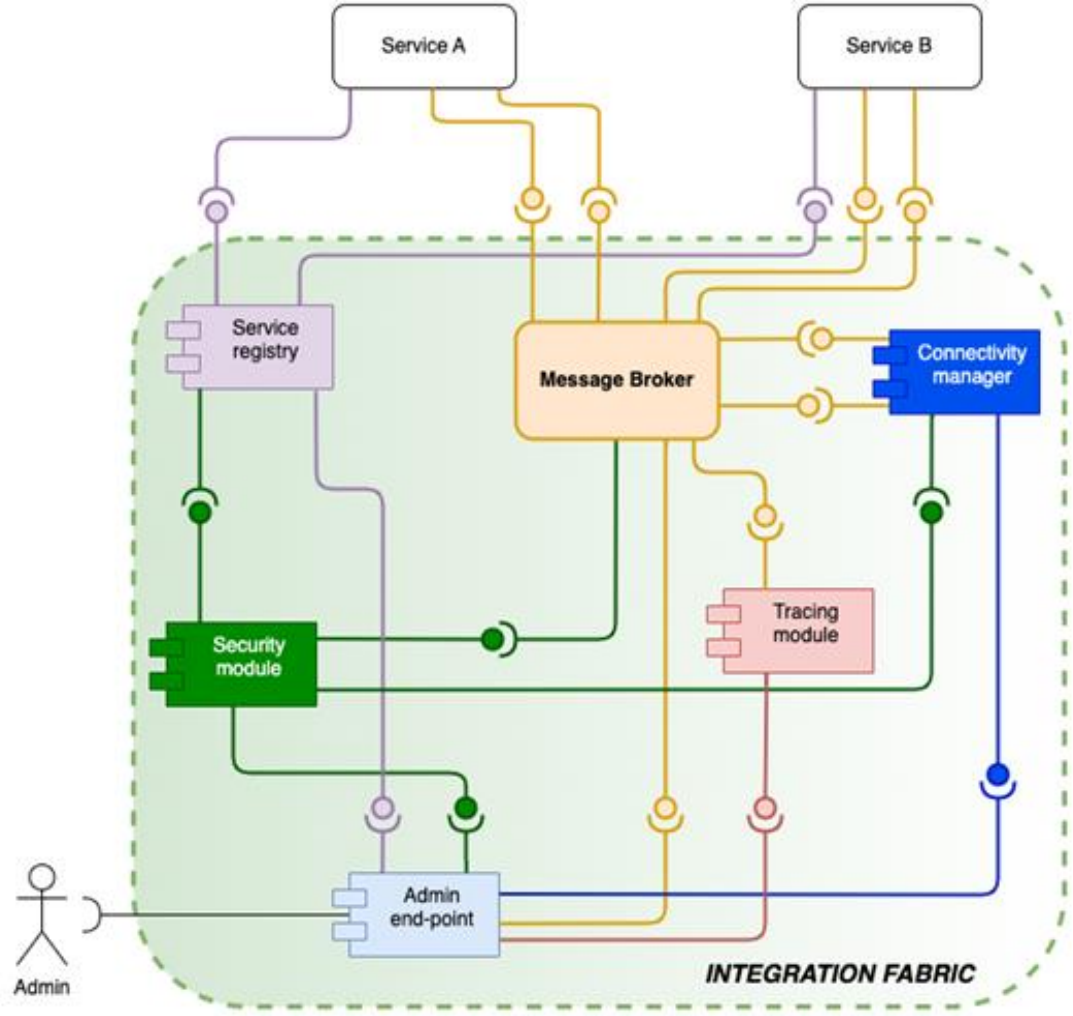
Components of system-PoC A – Closed-loop automation

Reactive CL based on real-time measurement of cobots' battery level



Components of system-PoC A - Integration fabric

Integration fabric message broker architecture



System-PoC KPIs

Title	Description
1. **Reliability**	Network reliability refers to the percentage of time that the network is available and functioning correctly. High network reliability is required to minimize disruptions to service and prevent lost revenue. Application/Service reliability refers to the percentage of time that the application or the service is fully functional and responsive to the posed requests/workload in accordance with the defined SLA.
2. **Latency**	Network/Link latency measures the time it takes for data to travel between two points in the network. It is typically expressed in milliseconds (ms) or microseconds (µs). In the context of 6G, low latency is crucial for applications that require real-time interactions, such as virtual reality, telemedicine, and autonomous vehicles. Software latency (distributed traces) measures the time required for the interaction between software components. Having information for both type of latencies is helpful to identify whether a misperformance or a bottleneck is due to network or application performance aspects.
3. **Provisioning Time**	This KPI measures the time taken to enforce a provisioning request of a managed entity (CNF, Network Service, Network Slice, Application etc.) to the underlying infrastructure, measured from when the request reaches the provisioning interface up to the time that the managed entity provisioning is fulfilled
4. **Termination Time**	Time to terminate a managed entity (CNF, Network Service, Network Slice, Application etc.), from the termination request up to the release of its assigned resources. This provides a measure of the promptness in re-availability of the resources after released by a service.

System-PoC KPIs

Title	Description
5. **Recovery Time**	This KPI measures the time to recovery of a managed entity (CNF, Network Service, Network Slice, Application etc.) after an outage, providing a measure of the reactiveness of the network in minimizing service downtime.
6. **Intent Deployment Latency**	Time to have the complete E2E intent-based service request properly deployed and available to be used by for the final user. This latency will start when the service user intent-based requests reach the IBN solution until the confirmation of the intent-based service is available for the user.
7. **Intent Conflict Resolution Latency**	Time to achieve the complete resolution (i.e., service completely working in normal status) since an intent-based conflict is detected, up until it is solved.
8. **Scaling Time**	Time to apply horizontal or vertical scaling actions. It is measured from the time that a scaling request is triggered till the time the new or updated instances of a service or application component are operational.
9. **APIs Performance**	A set of indicators can be considered for measuring the performance of the provided APIs (e.g., the Northbound APIs provided by the DSP). These indicators include the average and maximum latency for serving a request, requests served per minute, errors per minute, number of concurrent tenants.

Preliminary list of KPIs/KVIs specific to the presented applications

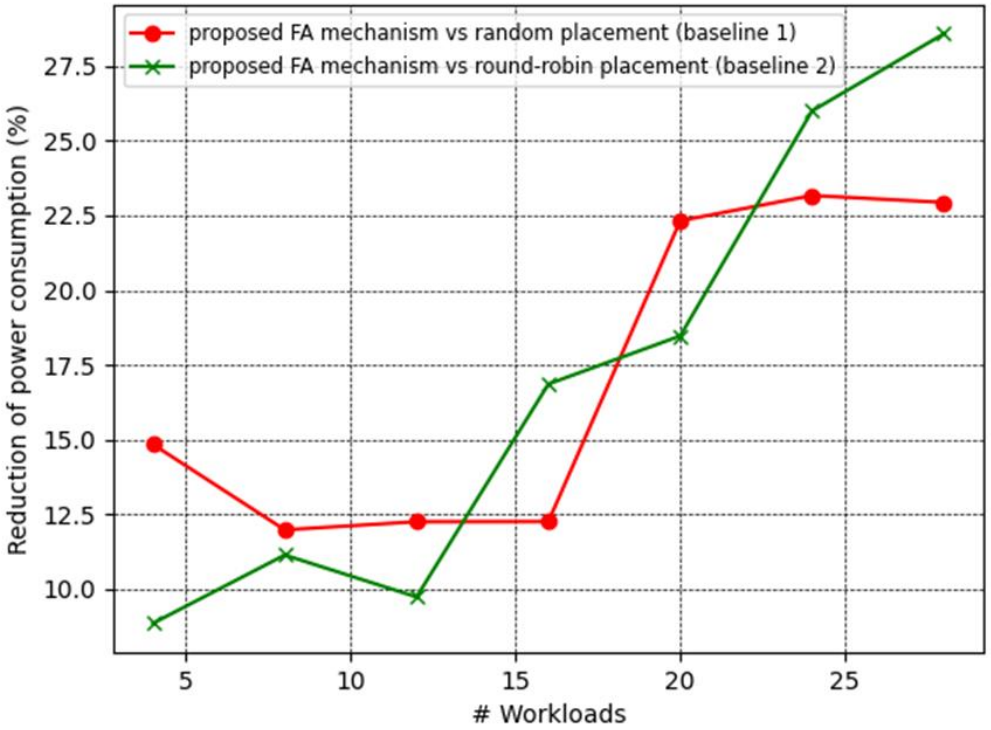
Title	Description
10. **Power Consumption per AMR/UAV**	This KPI measures the power consumption of the robot for a pre-defined set of configured roles/actions, per unit of time.
11. **Overall System Power Consumption**	The power consumption measured for all involved system components, for the E2E service execution, per unit of time.
12. **Overall System Trust**	A set of indicators for measuring the trust of all the entities/nodes, allocated in the E2E service, including end-devices (e.g., cobots), as well edge/cloud compute nodes.
13. **Path Planning Efficiency**	The time required to calculate optimal paths per robot.
14. **Object Detection Accuracy/Performance**	Performance metrics related to the object detection service, such as accuracy, precision, recall.
15. **Warehouse Digital Twin positioning accuracy**	The metric which assesses the error introduced in the digital representation of the physical objects, in real-time comparing to the actual one.
16. **High-Resolution, Real-Time Cobot Camera Feed Latency**	The amount of time that it takes for a single frame of video to transfer from the robot's camera to the Digital Twin's display.
17. **Cobot Tele-Operation Command Latency**	The time required for teleoperation command packets, from the tele-operation user interface (edge/cloud server) to reach the cobot tele-operation service.

Business KPIs:

- Warehouse task operational time.
- Number of accomplished tasks per time window.
- Percentage of workload covered with the use of the AMRs/UAVs.

Preliminary technical results of 1st configuration (1/2)

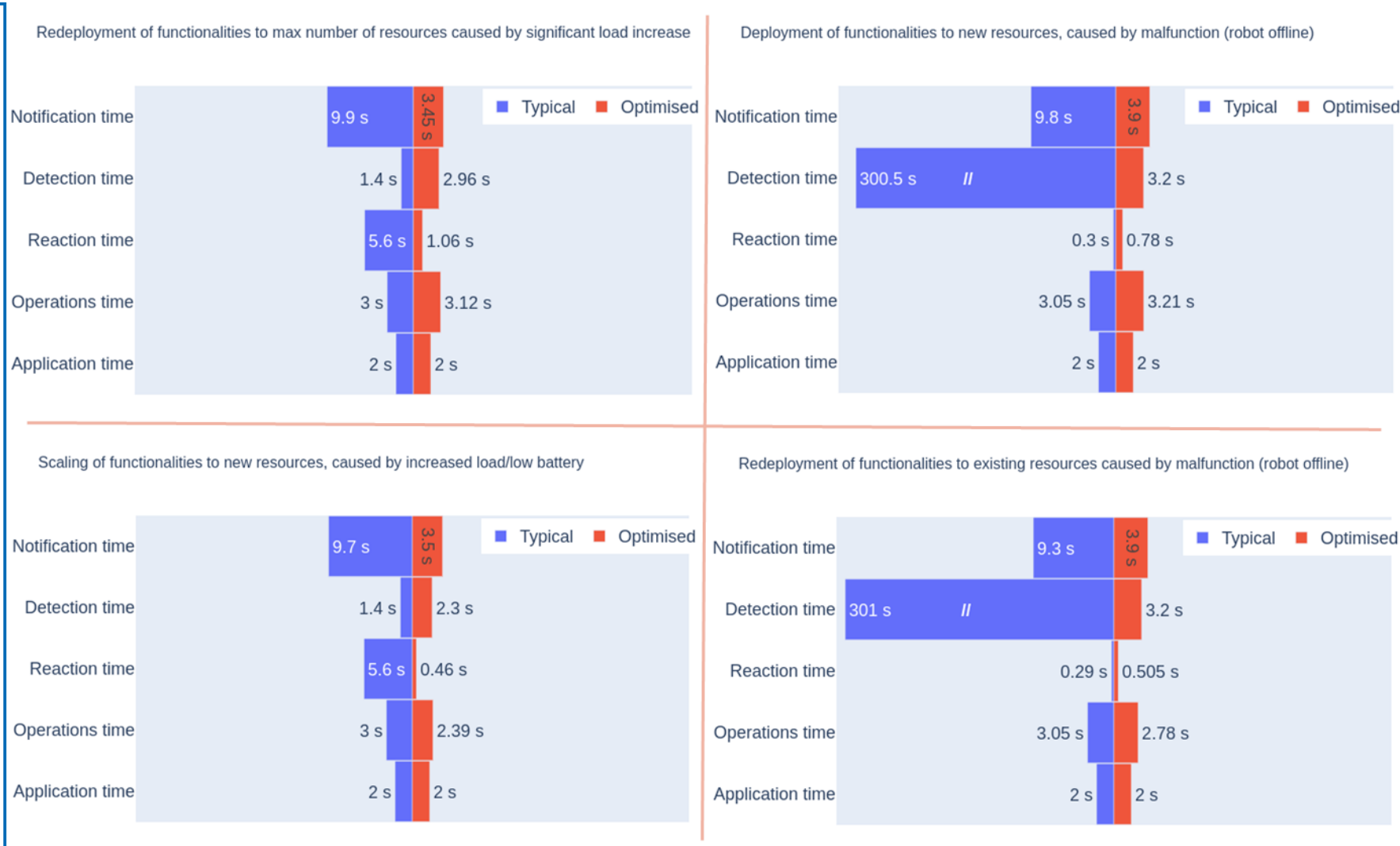
- Functionality Allocation (FA) mechanism was developed for optimally placing functionality to the various compute nodes of the system.
- As power consumption is considered the power consumption for processing and the transmission power consumption.
- A metaheuristic algorithm is developed based on a Genetic Algorithm paradigm.
- The results are compared with two baseline algorithms, the feasible random placement and the SoTA round-robin placement.
  - The validation scenario comprised 7 compute nodes (3 robotic units, 2 edge servers, 2 cloud servers) and increasing number of compute workloads/ tasks
- The FA algorithm compared to the baselines can gain 8.8-28.6% reduction of power consumption
- Working on:
  - integrating the trust manager component to succeed maximum trustworthiness.
  - Develop an ML algorithm to possibly obtain better performance.



Reduction of power consumption with increasing number of workloads of our FA mechanism compared with two baseline algorithms.

Preliminary technical results of 1st configuration (2/2)

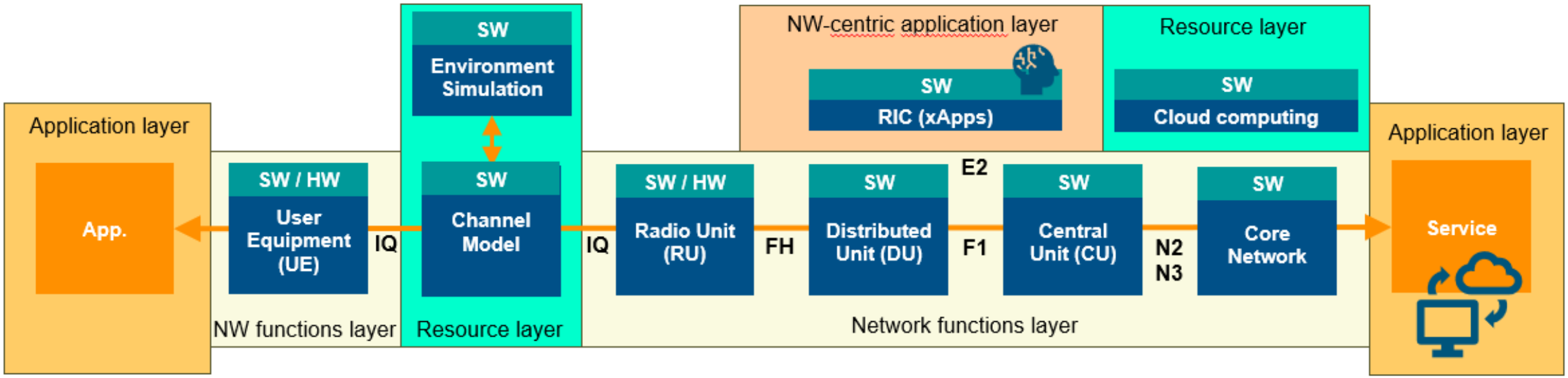
- Functionality Allocation mechanism along with performance diagnosis workflow was developed for enhancing the M&O operations.
- The results are compared with the typical M&O workflow (notification, action).
- Both workflows are used for handling 4 types of events that can happen in an industrial context.
  - For each of these types, 10 instances of events are manually triggered following the typical patterns of the industrial automation service. The average of them is presented in the table.
- The FA mechanism shows significantly better recovery time with range **10.65s - 13.09s** compared to the typical M&O with range **21.7s - 315.65s.**
- Working on:
  - integrating the trust manager component to succeed maximum trustworthiness.
  - Develop an ML algorithm to possibly obtain better performance.



Collected time measurements during unexpected events.

E2E simulation framework for connectivity

- E2E simulation framework is planned to be developed and used for selected 6G connectivity enablers performance evaluation
- High-level architecture of E2E simulation framework and its' mapping to the system blueprint is illustrated in below figure



HEXA-X-II.EU //

Co-funded by the European Union

6GSNS

Hexa-X-II project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101095759.