Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier XX.XXXX/ACCESS.XXXX.XXXXXXX

Future Open Networks Cross-Domain Cognitive Orchestration: A Novel Design Paradigm

SAPTARSHI GHOSH[1], HAMID ASGARI[2], DARRYL HOND[2], KONSTANTINOS ANTONAKOGLOU[1], IOANNIS MAVROMATIS[1], NOEL BUTLER[2], RASHEED HUSSAIN[3], SHAH ZEB[3], KOSTAS KATSAROS[1], SHADI MOAZZENI[3], DAVID TEE[2], GABRIELE INCORVAIA[2], and DIMITRA SIMEONIDOU[3]

[1]Digital Catapult, London, UK, NW1 2RA
[2]Thales Research, Technology, Solution and Innovation (RTSI), 350 Longwater Avenue, Reading, Berkshire RG2 6GF, UK
[3]University of Bristol, Faculty of Engineering, Woodland Road, Clifton, Bristol, BS8 1UB, UK

Corresponding author: Saptarshi Ghosh (e-mail: saptarshi.ghosh@digicatapult.org.uk).

This work is undertaken in the REASON project, a UK Government funded project under the Future Open Networks Research Challenge (FONRC) sponsored by the Department of Science Innovation and Technology (DSIT).

ABSTRACT Future Open Networks (FONs) are envisioned as large-scale, decentralised, and data-driven systems designed with open interfaces and interoperable standards to deliver diverse services and applications. The management and orchestration of these networks will utilise intelligent processing. This paper introduces a novel Cognitive Cross-Domain Orchestration (CDO) architectural framework for FONs, structured as a quad-view architecture. A background setting for the architecture is provided by a survey of relevant projects, followed by a requirements analysis for FON orchestration and management. The proposed CDO architectural framework consists of four distinct views: the Organizational View identifies stakeholders and business entities; the Functional View outlines the logical design; the Cognitive & AI/ML View connects logical functions with supportive cognitive functions for network optimization; and the System-level View links these functions to the necessary physical and intangible assets. This segregation enables each view to provide a focused analysis of the roles, interactions, and properties, thereby promoting a coherent design. The paper also describes a plausible partial proof-of-concept implementation of the CDO System-level architecture. Within the context of this CDO implementation, stakeholder participation in the provision of an end-to-end service delivery orchestrated across multiple network domains is described.

INDEX TERMS Future Open Networks, Cross-Domain Orchestration, Cognition-Enabled Networking, 6G, System-Level Architecture, Cognitive & AI/ML.

I. INTRODUCTION

THE Future Open Network (FON) is a novel architectural paradigm that is evolving from current communication system standards and practice to promote telecoms diversification, with a focus on the openness and interoperability of various networking architectures [1]. FON envisions a seamless blend of openness within 5G and beyond-5G (B5G) use cases across industry verticals, scoped, but not limited by, the European Industrial Strategy framework. This framework identifies three key application areas: Transportation, Automotive, and Public Safety [2]. Moreover, the challenges and opportunities posed by the social, economic, technological and regulatory trends in telecoms heading towards 2030 provide a basis for FON requirements [3]. This will result in the creation of 22.3 million jobs by 2035, new government policies emphasising the use of verifiable and explainable AI in telecoms, and the promotion of both Network Intelligence and Cross-Domain service delivery [4]. FONs must be flexible enough to cater to the diverse requirements of different ecosystems, ranging from Radio Access Networks (RANs) to dynamic network edges and the core. Therefore, they will require a top-down orchestrator that harmonises the collaboration between multiple downstream heterogeneous network domains to provide customer-facing services. At the same time, there must be compliance with the expectations placed on FONs, for example, open-architecture [5]; data-driven telecommunication network design [6]; AI/ML-based network optimisation [7]; and multi-domain service provisioning and orchestration [8]. This paper refers to customer service as a "**Task**" and the enabling orchestration as "**Cross-Domain Orchestration** (CDO)".

It is essential at this point to formally define a Task and differentiate between Intent-Based Networking (IBN) and Task-Oriented Networking (TON). An Intent is an expected state of a network translatable into network device configurations. Application-aware networking enhances IBN capability by considering the application-specific requirements and translating them into the required network-level configuration [9]. A Task is a customer service or flow of processes performed by several participating entities in collaboration. Task-oriented cross-domain orchestration requires proactive service provisioning, resource allocations and optimal domain selection while establishing secure inter-domain connectivity at scale. Such capabilities form the basis of the CDO proposed in this context.

Cross-domain network orchestration stands on four pillars of networking, i.e. intelligence, flexibility, sustainability and security [10]. Intelligence should ultimately enable autonomous network operation, with minimal human intervention, and network adaptability, using cognitive functions [11] for dynamic function placement [12] and service delivery (including AI-as-a-Service [12]). The security aspect of FONs is a vast domain which could be discussed at length; in summary, there is a prominent trend towards zero-trust and distributed policy management.

FONs will also use Intra-Domain Orchestrators (IDOs), where an IDO will orchestrate services and resources in each independent administrative network domain. These IDOs will collaborate with the CDO to provide end-to-end services that extend beyond their geographical scope.

This paper surveys relevant state-of-the-art projects and initiatives beyond 5G and 6G and then conducts a comprehensive requirement analysis. It then presents the architecture of a proposed cross-domain orchestrator from a novel multi-view perspective. Each of the four views depicts an exclusive architectural representation. In combination, the related but complementary views capture the principles of the proposed architecture.

The **Organisational View** specifies the ecosystem formed by the stakeholders who define the CDO requirements and who will benefit from the CDO operation. The **Functional View** illustrates the logical architecture from a design perspective, breaking it down into functional blocks. The **Cognitive & AI/ML View** relates how AI/ML supports the functional blocks from an optimisation and automation perspective. The **System-level View** lays out the physical architecture from an implementation and operational perspective, which includes workflows for progressing towards Proof-of-Concept. The architectural views comprise several sub-views, including Service Management and Network Management, as described in Section VI. Table 1 summarises the list of contributions made within this article.

The remainder of the paper is organised as follows. Sec. II presents a background study of recent telecoms research projects, primarily in the EU and UK, focusing on multi-domain orchestration. Sec. III reviews current trends in intelligent network orchestration before listing the requirements for 6G cross-domain orchestration. Sec. IV depicts the high-level architectural view encompassing the four underlying views (Organisational, Functional, Cognitive & AI/ML, and System-Level), which the following four sections (Sec. V to IX) discuss in detail. Finally, the paper concludes with a summary and future directions.

TABLE 1. List of Novel Contributions Introduced in this Paper

Contrib. ID	Description
CON-1	Proposes a multi-view architectural paradigm in the form of a quad-view CDO architecture
CON-2	Provides details of the systematic use of AI/ML models to support the cognitive processing required by the CDO
CON-3	Provides a series of CDO workflows for end-to-end service delivery, and in this context, describes how Stakeholder participation and interaction results in the offer of end-to-end complex services across multiple domains

II. 3GPP & ETSI STANDARD ATTRIBUTES AND OVERVIEW OF RELEVANT EC PROJECTS

The proposed CDO architecture reflects how cross-domain orchestration is conceived within the scope of the REASON project. This section takes a broader view, first providing key standard attributes for cross-domain orchestration. Then, we provide an overview of recent EC projects and their main features relating to multi-domain orchestration in Beyond 5G and 6G. In addition, the section compares the projects (including REASON) with the key attributes (Table 3).

This background study is explicitly limited to cross-domain orchestration. However, we encourage the reader to refer to our previous paper [13] for a more complete comparison.

A. CROSS-DOMAIN ATTRIBUTES

Here, we define the six key attributes that we will use to compare relevant state-of-the-art projects regarding the 6G architectural principles proposed by the 5G PPP reference architecture [4], which can be cross-referenced with 3GPP and ETSI standards.

Service management refers to the lifecycle handling of network services, including creation, monitoring, and termination across domains. 3GPP TS 28.531 [14] defines procedures for managing network slice instances, acting as containers for services, while TS 28.533 [15] provides a service-based management architecture with role-based interactions. ETSI GS ZSM 008 [16] expands the scope to zero-touch, end-to-end service orchestration across heterogeneous domains. Unlike 3GPP, which focuses on 5G-specific mechanisms, ZSM 008 supports domain-agnostic coordination and flexible service chaining. ETSI's approach is broader and designed for automation beyond 5G, offering abstraction layers that enable interoperable service management across multi-vendor and multi-technology environments.

Network management involves monitoring, configuration, and fault handling across infrastructure domains. 3GPP

TABLE 2. List of Acronyms.

Acronym	Description
5G	Fifth Generation Telecommunication Systems
6G	Sixth Generation Telecommunication Systems
AIO	AI/ML Orchestrator
c/pSLA	Customer/Provider Service Level Agreement
CAA	CDO AI/ML Agent
CAD-FB	Capability Advertisement Discovery FB
CAM	CDO AI/ML Manager
CD-SP	Cross-Domain Service Provider
CDO	Cross-Domain Orchestrator
CF	Cognitive Functions
CFC-FB	Common Function Catalogue FB
CHN-FB	Service Planning and Chaining FB
CRF-FB	CDO Customer Resource Forecast FB
CT	Complex Task
DLT	Distributed Ledger Technology
E2E	End-to-End
EC	European Commission
ET	Elementary Task
FA-SV	Functional Architecture Sub-View
FB	Functional Block
FON	Future Open Networks
FPC-FB	CDO Resource & Function Prediction & Chaining FB
IDO	Intra Domain Orchestrator
KPI	Key Performance Indicator
NAK	Negative Acknowledgement
NFV	Network Function Virtualisation
NM-SV	Cross-Domain Network Management Sub-View
NMg-FB	CDO Network Management FB
NMg-FB	Network Management Sub-View
NPR-FB	CDO Network Planning and Route Management FB
NSI	Network Slice Instance
PCS-FB	E2E Policy Catalogue Service
PEC-FB	Policy Enforcement and Compliance FB
PIC-FB	Policy Issuance and Consumption FB
PM-SV	Cross-Domain Policy Management Sub-View
PRp-FB	Policy Repository FB
QoS	Quality of Service
RAN	Radio Access Networks
REASON	Realising Enabling Architectures and Solutions for Open Networks Project
SA	Service Level Architecture
SAr-FB	Service Assurance FB
SAs-FB	Service Assurance FB
SBr-FB	Service Brokering FB
SCA-FB	Service Capability Advertisement FB
SFC	Service Function Chain
SFP-FB	Service Forecast and Prediction FB
SHS-FB	Service Handling and Subscription FB
SM-SV	Cross-Domain Service Management Sub-View
SMg-FB	Service Migration FB
SMon-SV	Cross-Domain Service Monitoring Sub-View
SOI-FB	Service Ordering and Innovation FB
SPC	Service Provisioning Cycle
SV	Sub-View
T&SM-SV	Cross-Domain Trust & Security Management Sub-View
UE	User Equipment
VNF	Virtual Network Function

TS 28.531 [14] provides a Network Resource Model (NRM) for managing slice components, while TS 28.541 [17] extends the NRM to broader 5G network functions, supporting configuration and performance management. ETSI GS ZSM 003 [18] addresses end-to-end slice orchestration, offering high-level coordination mechanisms across domains. Unlike 3GPP's detailed object-level models, ETSI focuses on domain orchestration logic and the abstraction needed for cross-domain interaction. While 3GPP ensures standardisation at the resource level, ETSI enables broader integration for multi-domain, zero-touch network management and interoperability between different administrative environments.

Cognition refers to the use of AI/ML to enable networks to learn, adapt, and optimise operations. ETSI GS ZSM 012 [19] defines architectural enablers for AI-driven automation, including model training, inference, and data collection. ETSI GS ENI 005 [20] introduces a cognitive management system to make context-aware decisions across services. While 3GPP is still developing general cognitive frameworks, it supports foundational mechanisms, such as data collection for machine learning (e.g., TR 32.866 [21]). ETSI's work offers comprehensive, system-level AI integration for autonomous orchestration, whereas 3GPP remains focused on data interfaces and operational telemetry within the 5G network management architecture.

Trust and Security Management ensures secure interactions across domains, safeguarding configuration, access, and automation. 3GPP TS 33.501 [22] defines the security architecture for 5G, covering authentication, authorisation, and trusted communication. TS 28.554 [23] adds security assurance for management functions. ETSI GR ZSM 010 [24] addresses automation-specific concerns like trust negotiation and secure cross-domain orchestration. While 3GPP enforces protocol-level integrity and confidentiality in telecom systems, ETSI emphasizes trust models, secure interfaces, and policy exchange in zero-touch automation. The ETSI model is particularly important for multi-domain and multi-vendor environments where trust boundaries extend beyond a single operator's infrastructure.

Policy management governs the rules for network behaviour, resource use, and service orchestration. 3GPP TS 23.503 [25] defines policy control functions in the 5G Core, including QoS and slice enforcement. TS 28.541 [17] supports policy-driven resource and performance management. ETSI GR ZSM 010 [24] addresses lifecycle handling of policies across domains, including conflict detection and distributed enforcement in autonomous systems. Unlike 3GPP's runtime enforcement mechanisms tailored to mobile core networks, ETSI focuses on orchestrated policy automation across heterogeneous domains. This enables more flexible and scalable management for cross-domain services involving multiple vendors or administrative boundaries.

Finally, **cross-domain connectivity** involves coordinating services and resources across multiple network domains, such as RAN, core, and transport networks. 3GPP TS 28.501 [22] offers foundational concepts and requirements for management and orchestration, facilitating interoperability across diverse network segments. TS 28.533 [15] details the management of services and network slices spanning various domains, while TS 28.531 [14] focuses on provisioning network slice subnets for end-to-end service delivery. ETSI GS ZSM 008 [16] emphasises cross-domain service orchestration, providing integration frameworks for seamless automation. While 3GPP standards ensure coordination within 5G systems, ETSI's approach supports broader service federation and automation beyond traditional telecom boundaries, enabling collaboration in complex, multi-operator environments.

Next, we map the key attributes to several surveyed projects, including REASON.

B. OVERVIEW OF RECENT EC PROJECTS FEATURING CROSS-DOMAIN ORCHESTRATION

In this section, we cover an overview of recent EU projects commenced within the last five years from the time of composing this paper (2019-2024) and emphasise the size and cross-domain attributes identified in the previous section. We present a summary of the projects referring to respective attributes, citing corresponding publicly available deliverables in Table 3.

5GROWTH [49] addresses the deployment of network slices for Industry 4.0, transportation, and energy sectors. Comprising the Vertical Slicer (5Gr-VS), the Service Orchestrator (5Gr-SO), and the Resource Layer (5Gr-RL), 5GROWTH provides a platform for life-cycle management and orchestration of network slices, with resource forecasting enabled by monitoring capabilities. The 5Gr-VS component provides a user interface for service deployment and the creation of network slice instances. Furthermore, the 5Gr-SO component is responsible for network service orchestration and lifecycle management, while the 5Gr-RL component enables resource management through the abstraction of physical, virtual, computing, and networking resources.

5GROWTH offers the following cross-domain orchestration capabilities: Network Management through Network Slicing and Slice Subnet Management, a monitoring platform and Monitoring Manager for managing VM agents, a Distributed Ledger Technology (DLT) based Federation for Trust & Security Management, Arbitration Policy Management [26], and Inter-domain communication using East-West interfaces [27]. However, support for cognitive capabilities in 5GROWTH is limited.

5GVICTORI [50] is aimed at connecting European 5G testbeds and the 5GUK test network to deploy and test use cases in sectors such as transportation, energy, media, and future factories with cross-vertical applications. Each testbed within its administrative domain has 5G and WiFi, service monitoring, and network slicing and orchestration capabilities. Furthermore, 5G-VICTORI has introduced a cross-domain orchestrator known as 5G-VICTORI Operating System (5G-VIOS) [51] to manage network services across different edges. An intelligent profiling agent has also been integrated into each domain and the 5G-VIOS platform to anticipate and allocate the required network resources to meet the KPI thresholds.

5GVICTORI offers the following cross-domain orchestration capabilities: A Mobility Manager and Inter-Domain Communication Manager for Network Management [28], Edge and E2E Service Monitoring [29], and inter-domain communication using Dynamic Multipoint VPN (DMVPN) [28]. However, the support of Cognitive Capabilities, Trust & Security Management and Policy Management in 5GVICTORI is limited.

5GZORRO [52] is aimed at developing a secure and trusted cross-domain architecture and framework for service and network management within multi-stakeholder environments [53]. Key technologies used for this purpose have included: Smart Contracts based on Distributed Ledger Technologies aiming to enhance business agility, a 5G Operational Data Lake with APIs that enable AI Operations for ML model management and optimisation, as well as a Smart Contract solution for SLA management [54]. Additionally, the project focused on implementing cross-domain security and trust mechanisms, as well as creating a secure, shared spectrum market for the real-time trading of spectrum allocations.

5GZORRO offers the following cross-domain orchestration capabilities: Network Management using Any Resource Manager (xRM) that offers Intelligent and Automated Slice and Service Management, which includes Workflow and MEC Manager; Service Monitoring using Data Lake, Monitoring Data Aggregation and SLA Monitoring; Trust & Security Management through Security Analysis Service, VPN-as-a-service, DLT and Smart Contracts based Trust Management, e-Licensing Manager and Trust level monitoring [30]; and VPN for secure Inter-Domain connectivity. However, the support of cognitive capabilities and policy management in 5GZORRO is limited.

INSPIRE-5GPLUS [55] has proposed to advance the security of 5G and Beyond networks. Its goal is to achieve intelligent and trusted multi-tenancy in a cross-domain infrastructure, focusing on intelligent security and security management of the automated end-to-end (E2E) service and network orchestration platform. This platform is based on the ETSI ZSM reference architecture and incorporates trust, resulting in an improved closed-loop model.

INSPIRE-5GPLUS offers the following cross-domain orchestration capabilities: a Network Slice Manager [31], a trustable data collection and monitoring subsystem, a Smart Security Management Framework, and a Moving Target Defence Controller for security orchestration and trust management accompanied by a Hyperledger Fabric and Smart Contracts, SLA-based policy management [32], and a Cross-Domain Integration Fabric [33]. However, the project has limited support for cognitive capabilities.

5GCLARITY [56] introduced a Beyond 5G O-RAN-based architecture for private networks with SDN capabilities. This architecture integrates 5G, Wi-Fi, LiFi technologies, and other components to offer Wireless Access Technologies as a Service, NFV Infrastructure as a Service, and Slicing as a Service [57]. Key features of this architecture include the Intent Engine and the AI Engine [58], which is responsible for acquiring and translating a user's intent into a policy to be applied to the underlying infrastructure. On the other hand, the AI Engine hosts and manages AI/ML models as a service, which can be selected based on the user's intent. 5GCLARITY is built upon 5GROWTH.

5GCLARITY offers the following cross-domain orchestration capabilities: network management through NFVI-as-a-Service, Slice-as-a-Service, and WAT-as-a-Service [34]; service monitoring using Data Semantic Fabric, a semantic model-driven data processing and management subsystem [59], and non-RT-RIC policy management regarding network slicing and private site gateway concerning data privacy and

TABLE 3. Comparison of the relevant 6G EC and UK projects with respect to the key 3GPP attributes for cross-domain orchestration

Projects	Duration	Network Management	Cognitive & AI/ML Capabilities	Service Management	Trust & Security Management	Policy Management	Cross-Domain Connectivity
5GROWTH	Jun 2019 - Feb 2022	[26]	-	[26]	[26]	[26]	[27]
5GVICTORI	Jun 2019 - Jun 2023	[28]	-	[29]	-	-	[28]
5GZORRO	Nov 2019 - Oct 2022	[30]	-	[30]	[30]	-	VPN
INSPIRE-5GPLUS	Nov 2019 - Oct 2022	[31]	-	[32]	[32]	[32]	[33]
5GCLARITY	Nov 2019 - Feb 2022	[34]	-	[34]	[34]	-	-
HEXA X: I & II	Jan 2021 - Jun 2025	[35]	[35]	[36]	[35]	[36], [37]	VPN
DAEMON	Jan 2019 - Mar 2024	[38]	[39]	[39]	-	[39]	-
HORSE	Jan 2023 - Dec 2025	[40]	-	[40]	[40]	[40]	-
ADROIT6G	Jan 2023 - Dec 2025	[41]	[41]	-	-	-	-
DESIRE6G	Jan 2023 - Dec 2025	[42]	-	[42]	[42]	[42]	-
RIGOROUS	Jan 2023 - Dec 2025	[43]	-	[44]	[43]	[43]	[43]
PREDICT6G	Jan 2023 - Jun 2025	[45]	-	[45]	[46]	-	[47]
ACROSS	Jan 2023 - Dec 2025	[48]	[48]	-	[48]	-	[48]
REASON	Jan 2023 - Feb 2025	Sec. VI-D	Sec. VII-A	Sec. VI-G	Sec. VI-E	Sec. VI-C	Sec. VI-F3

QoS [34]. However, the project has limited support for cognitive capabilities and cross-domain connectivity.

HEXA-X and HEXA-X II [12] aims to define, develop, and evaluate a blueprint for a 6G platform architecture and relevant technology enablers. The proposed platform encompasses a diverse range of 6G enablers, including AI-as-a-Service, intent-based management, ultra-low latency connectivity, and high-efficiency, energy-neutral devices for end-users and operators. Additionally, it considers observability and computing capabilities to support Key Value Indicators (KVIs) such as sustainability, inclusion and trustworthiness.

HEXA-X offers the following cross-domain orchestration capabilities: Multi-X (i.e., domain, technology, vendor, and tenant) Orchestration [35]; Intent-based cognitive closed-loop management using Explainable AI for QoE prediction and radio control, Federated Explainable AI framework [35]; Programmable network monitoring & telemetry with AI monitoring [36]; DLT, Trust level monitoring & management and Trustworthy third party management [35]; Policy enforcement in dynamic function placement [37] and Policy control is employed for cross-domain AI framework interactions [35]; Inter-domain secure connectivity (VPN). This project fulfils all cross-domain orchestration attributes and is closest to the REASON project.

The **DAEMON** [60] is focused on the limitations of AI-assisted network functions in eight categories and suggested alternative methods to the current plane-centric closed-loop control approach that integrates AI within E2E network architecture [61]. The project also explores native Network Intelligence within three time-scale levels: Orchestration, non-real-time controllers, and real-time controllers [62].

DAEMON offers the following cross-domain orchestration attributes: Network Intelligence Orchestrator for network management [38]; cognitive capabilities using Self-learning models with Explainability and Knowledge management; monitoring capability of both ML-related and non-ML-related (e.g. QoE, QoS) operations; policy management with interpretation and configuration capability [39]. However, the project has limited trust & security and inter-domain connectivity features.

HORSE [63] has developed a platform that enables intent-driven, AI-enhanced, security-focused, and trustworthy service and network orchestration. The project aims to demonstrate how applications can leverage the advanced capabilities of 6G mobile networks to address the challenge of intelligent connectivity and service management within a secure, privacy-preserving, and trustworthy infrastructure. The main architecture modules of HORSE are the Intent-based Interface, Platform Intelligence, and AI Secure and Trustable Orchestration [64].

HORSE offers the following cross-domain orchestration attributes: network management using a Single slice optimisation capability standardised as 3GPP TR 23.700-80; intelligent monitoring using Event Calculus; AI-based Secure and Trustworthy Orchestration; and Policy Configurator [40]. However, this project's support of cognitive capability and inter-domain connectivity is limited.

ADROIT6G [65] presents a 6G mobile network architecture that uses ML to optimise control loops for zero-touch automation. This architecture is fully distributed, with its cloud-native functional components dynamically deployed to support various edge-cloud platforms. It comprises three cooperating inter-domain frameworks that enable distributed ML techniques and Federated Learning (crowd-sourcing AI). The architecture includes the Belief-Desire-Intention and AI-driven Unified and Open Control framework, which utilises AI-driven Management and Orchestration components to allocate resources based on current and context-aware predictions.

ADROIT6G offers the following cross-domain orchestration attributes: Slice Management Layer that includes a Zero-Touch Decision Engine sublayer for network management and Cognitive support using continuous AI model validation and model refinement capability [41]. However, the moni-

toring, trust & security, policy management and interdomain connectivity support are limited in this project.

DESIRE6G [66] is an ongoing project introducing a platform architecture incorporating intent-based control for E2E management, orchestration, and distributed intelligence deployments. At each DESIRE6G domain, the compute and network infrastructure are integrated under the Infrastructure Management Layer, controlled by the Multi-Agent System agents, enabling a Programmable Data Plane. Additionally, DESIRE6G utilises DLT and employs blockchain-based federation at the SMO level to facilitate the execution of services across different domains.

DESIRE6G offers the following cross-domain orchestration attributes: Service Management and Orchestration; multi-agent-based intelligent network monitoring with data aggregation; agent-based security-by-design and Security-as-a-Service and DLT-based SMO federation; and a Policy Framework that includes a policy engine that enables network operators to define and enforce policies for network services [42]. However, the project has limited support for cognitive functions and inter-domain communication.

RIGOROUS [67] is an ongoing project to ensure intelligent, secure, trusted, and privacy-preserving management and orchestration of 6G services across the IoT-Edge-Cloud continuum. The proposed framework leverages AI/ML mechanisms to achieve advanced AI-driven anomaly detection, apply intelligent mitigation strategies, and dynamically respond to threats across the different layers of the proposed architecture.

RIGOROUS offers the following cross-domain orchestration attributes: network management using E2E multi-domain multi-tenant slicing with AI-driven security Orchestrator and Security Slicing [43]; cognitive support using assisted autonomous identification of cyber threats in SMO control loop; Data monitoring and processing that provides input to the various data-driven services ensuring privacy preservation and Cyber threat information sharing [43]; Management Domain Security & Policy Enforcement using Moving Target Defence for Federated Learning, Trust Evaluation and Enabler Service Function Management and Zero-trust-based Identity management; Security & Policy Enforcement function in the management domain; and AI-driven cross-domain Security and Privacy orchestration in IoT-edge-cloud continuum [43]. This project possesses all cross-domain attributes.

PREDICT6G [68] introduces a platform and architecture powered by AI to orchestrate and manage 6G services across multi-stakeholder inter-domain deterministic networking infrastructures. The focus is on wired and wireless network infrastructure to improve cross-domain determinism. The project introduces a multi-technology, multi-domain data plane to accommodate the reliability and time-sensitivity capabilities of network standards implementations. In PREDICT6G, closed-loop operations are also supported by deploying network digital twins.

PREDICT6G offers the following cross-domain orchestration attributes: Network management, including resource management, path computation, topology exposure and time synchronisation; intra-domain measurement collection [45]; trust & security management is offered only in the case of inter-domain cooperative learning [46]; and AI-driven multi-stakeholder inter-domain control plane for offering inter-domain connectivity [47]. However, the support of cognitive capability and policy management in this project is limited.

ACROSS [69] is another ongoing project that develops a distributed, AI-driven orchestration platform for next-gen networks, enhancing automation, scalability, energy efficiency, and security. It uses domain-level and cloud-managed orchestrators, standardised interfaces, deep telemetry, and AI to enable zero-touch provisioning. Validated through federated test environments, ACROSS supports secure orchestration across heterogeneous cloud-edge setups and contributes proof-of-concept cases to standardisation bodies like ETSI ZSM, NFV-OSM, TMF, and ONF.

ACROSS offers the following cross-domain orchestration attributes: Cognitive capabilities, including Network Management using Zero Touch connectivity client with support of topic-based message queueing protocol, telemetry of compute and communication resources, and traffic-engineering specific network functions; cognitive capabilities including data analysis, model repository, and automation services; trust and Security Management targeting DDoS mitigation; and cross-domain connectivity Zero Touch Connectivity (ZTC) fabric. Given that the project is ongoing with limited deliverables available, we found limited information on Service and Policy Management [48].

Finally, Table 3 summarises various cross-domain capabilities the projects offer, mapping their publicly available deliverables to the key attributes and highlighting gaps in the range of attributes covered by each project. The table also includes the REASON project for comparison, referencing its CDO capabilities in the sections of this paper.

III. 6G CROSS-DOMAIN ORCHESTRATION CONTEXT AND REQUIREMENTS

This section provides a brief overview of some trends in network orchestration, with a focus on the growing role of cognition and network intelligence. It also discusses how these advancements will enable cross-domain orchestration for FONs. It then provides a concise summary of a range of cross-domain orchestration requirements, whose specification is partly drawn from the state-of-the-art survey in Sec. II.

A. COGNITION AND NETWORK INTELLIGENCE IN 6G ORCHESTRATION

The landscape of relevant research on orchestration is extensive, encompassing three primary strands. Each strand illuminates aspects crucial for advancing orchestration, particularly within 6G networks.

1) Less Recent Orchestration Research (4G, 5G)

Past research has mainly focused on coordinating resource allocation within Cloud and Edge environments and managing connectivity across the Edge-Cloud continuum under a single administrative boundary, referred to as intra-domain orchestration. Notable studies within this research area focus on Cloud and Edge orchestration [70], [71], [72], and [64].

2) Cognitive Dimensions of Network Orchestration (Recent Investigations in 5G)

There is a noticeable shift towards intelligent orchestration, emphasising the use of AI/ML-based intelligence for resource orchestration. This approach is crucial for adapting to the dynamic nature of software-defined 5G networks, particularly in supporting diverse and demanding services such as online multiplayer mobile gaming, holographic services, and Augmented Reality/Virtual Reality (AR/VR). Current and ongoing research efforts focus on utilising AI/ML for the proactive and predictive orchestration of individual service elements. For example, research is being conducted into Virtual Network Function (VNF) profiling for cognitive orchestration, as highlighted in [73], [74], [75], and [76]. Further reports in the literature addressing this area are discussed in [77], [78].

3) 6G Network Cognitive Orchestration

A vision of a comprehensive, cognitive, and all-inclusive service and resource orchestration landscape is setting the course for ongoing and future research. This approach combines advanced data analytics with traditional monitoring techniques to enhance the AI-driven orchestration of resources, services, security, and trust enablers. Additionally, 6G orchestration will require capturing extensive sensory data from all network devices and equipment and providing domain-level services such as connectivity and computing. Multiple cognitive and AI/ML elements will be needed to enable this orchestration and management functionality. Furthermore, the operation of these intelligent elements will need to be harmonised to support both cross-domain and intra-domain orchestration.

B. CROSS-DOMAIN ORCHESTRATION REQUIREMENTS

We present the requirements for cross-domain orchestration by dividing them into five categories: stakeholder, technical, monitoring and measurement, policy and cooperation, and non-technical requirements, as described below.

1) Stakeholder Requirements

Stakeholder requirements (labelled as *STK-n*) cover the general expectations of those with a stake in, and interest in, 6G from the business perspective. Stakeholders range from customer service providers, content providers, and network providers to government bodies, standardisation bodies, regulators, and others. For brevity, (Table 4) only states the requirements from an SLA perspective.

STK-1 relates to various forms of SLA Compliance. *STK-2* relates to the SLA Management.

TABLE 4. Stakeholder Requirements.

Req ID	Description
STK-1	Fulfil contracted SLA requirements in performance and offer service delivery choices
STK-2	Provide capacity management functions to handle SLA requests

2) Technical Requirements

General technical requirements (labelled as *TECH-type-n*), which include cognitive and security requirements (types *GEN*, *COG* and *SEC* respectively), cover the essential operational prerequisites for ensuring robust, secure and safe communication across administrative network domains (Table 5).

Starting with the general technical requirements and their satisfiability, *TECH-GEN-1* relates to the overall Service-Based Architecture & Interfacing between the architectural sub-views and Functional Blocks. *TECH-GEN-2 & 3* relate to CDO-IDO Communication and the corresponding scalability of the open interfaces between them. *TECH-GEN-4* relates to Cross-Domain Networking. *TECH-GEN-5* relates to the dynamic policy accommodation. *TECH-GEN-6* relates to collaborative route management and *TECH-GEN-7* mandates the CDO design follows standardised internal and external communication patterns.

Turning to the technical requirements concerning Cognition, the CDO needs to cooperate with the AI Orchestrator (Sec. VII-A) to source the Cognitive & AI/ML support functions. *TECH-COG-1* relates to Intelligent Traffic Engineering. *TECH-COG-2* relates to sourcing the MLOps pipelines, which assist various CDO functions. *TECH-COG-3 & 4* relate to The Lifecycle Management of the MLOps Pipeline and Autonomous Configuration (which depends on the level of autonomy expected). *TECH-COG-5* relates to CDO-AIO Interfacing.

Finally, about the security-related technical requirements, *TECH-SEC-1 & 2* relate to the API Security and Security by Design principles.

3) Measurement Requirements

The Measurement Requirements (labelled as *MSR-n*) concern the collection, storage, and analysis of telemetry data from various assets at different levels across the administrative network domains, while ensuring agreed-upon Service Level Agreements (SLAs) between parties. Table 6 lists the relevant requirements.

MSR-1,2 & 3 relate to the three aspects of **monitoring**, i.e., continuous monitoring, aggregation of monitoring data and monitoring cross-domain transactions, respectively.

4) Policy and Cooperation Requirements

The Policy and Cooperation Requirements (labelled as *POL-n*) cover the compliance of various policy frameworks (e.g., GDPR) when provisioning cross-domain services. Table 7 summarises the relevant requirements.

TABLE 5. Technical Requirements.

Req ID	Description
TECH-GEN-1	Need to provide Service-Based communication between CDO Functions
TECH-GEN-2	IDO must provide access to APIs for the CDO to establish hierarchical collaboration
TECH-GEN-3	Should support Open interfaces and network function disaggregation
TECH-GEN-4	Need to support interconnect of dynamic networks
TECH-GEN-5	Need to ensure policy compliance while provisioning service and networking required to fulfil application's needs
TECH-GEN-6	Need to establish collaboration and agreements between CDO and IDOs to provide collaborative management between CDO and IDO.
TECH-GEN-7	Need to comply with 3GPP and/or ETSI standardised internal and external communication
TECH-COG-1	Should provide optimal cross-domain connectivity with Cognitive Networking
TECH-COG-2	Should define Network Intelligence (where applicable) in CDO operations as MLOps pipeline
TECH-COG-3	Need to ensure request, deployment, monitor and retire AI/ML Models for CDO operations
TECH-COG-4	Should provide a gradual transition of the level of autonomy
TECH-COG-5	The cross-domain and AI Orchestrators should cooperate when supplying AI/ML models to support a task
TECH-SEC-1	Need to ensure the security of public, third-party and private APIs
TECH-SEC-2	Need to integrate standardised security measures at all stages.

TABLE 6. Measurement Requirements.

Req ID	Description
MSR-1	CDO needs to monitor SLA compliance from service and network operations
MSR-2	CDO needs to provide generalisation and aggregation of domain-level telemetry received from the IDOs
MSR-3	CDO needs to monitor any cross-domain transaction subject to a E2E service complying the privacy agreed

POL-1 relates to the overall policy management framework and *POL-2 & 3* relate to compliance with data-protection laws.

5) Non-Technical Requirements

The Non-Technical requirements (labelled NT-type-n) cover the essential requirements that do not fall under the above categories. These include environmental (*NT-ENV*) requirements, such as energy efficiency, and ethical (*NT-ETH*) requirements in the cross-domain orchestration context. Table 8 summarises the relevant non-technical requirements.

ENV-1 relates to environmental sustainability with a primary focus on energy efficiency and consumption side, while acknowledging other sustainability factors such as emissions of CO2, Chlorofluorocarbon (CFC) and greenhouse gases, including resource utilisation and lifecycle impact, as discussed in related literature.

TABLE 7. Policy and Cooperation Requirements.

Req ID	Description
POL-1	CDO needs to establish a policy framework to support cross-domain orchestration
POL-2	CDO Needs to adhere to data protection laws, such as the UK Data Protection Act
POL-3	CDO needs to act based on business intent, government regulation, and customer/provider requirements.

TABLE 8. Non-Technical Requirements.

Req ID	Description
NT-ENV-1	Should consider energy consumption as a constraint for global network optimisation
NT-ETH-1	Must comply with privacy and data protection norms of the country of operation
NT-ETH-2	Must ensure the autonomy given to AI follows the regulatory norms concerning ethics, verifiability and explainability.

ETH-1 relates to Privacy Protection, and *ETH-2* relates to Responsible AI, a status that must be ensured by the CDO AI/ML manager (CAM).

IV. HIGH-LEVEL ARCHITECTURAL VIEWS

In this section, we outline the design philosophy of the CDO and present a high-level architectural framework that integrates four architectural views, each of which will be elaborated upon in subsequent sections. It also presents several multi-domain networking scenarios where CDO orchestrates end-to-end service delivery. It should be stated that architectures are not random pictures. They must be structured views whose power lies in their specificity and how they are interlinked. This novel multi-view approach describes the high-level CDO architecture from four different but complementary perspectives.

The architectural framework comprises four distinct, well-defined views, each featuring elements of a particular type. These types are specific to each view and represent stakeholders, logical functions, AI/ML models, and physical assets. This enables each separate view to focus exclusively on the roles and properties of, as well as the interactions and connections between, elements of the same type. We avoid specifying a mixture of types, for example, logical functions and physical assets, within the same view. This clarifies, cleans, and simplifies analysis, promoting coherent design. We set forth an organisational view (Sec. V) from a business perspective, a Functional View (Sec. VI) from a logical perspective, a Cognitive & AI/ML View (Sec. VII) from the standpoint of intelligent and autonomous operation, and a System-level View (Sec. IX) from an implementation & deployment perspective. Figure 1 shows the four Architectural Views detailed in the following sections.

The interlinkages between the views and the correspondence between elements contained in different views are also

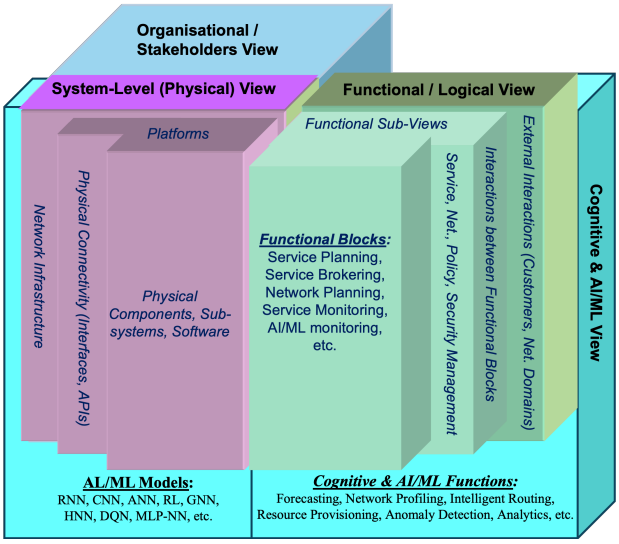


FIGURE 1. **Architectural views considered in Cross-domain Orchestration**

captured. This is partly needed because the nature of some views depends on the structures conceived in other views; for example, ML models documented in the Cognitive & AI View are associated with functional blocks belonging to the Functional View, and the System-level View is derived from the Functional View. However, it is also the case that only by augmenting the views with details of how they relate can a complete and systematically structured description of the overall architecture be obtained. Thus, our approach gains its effectiveness by providing a set of category-specific views and by documenting the interrelationships between those views.

A. ADMINISTRATIVE DOMAIN

Although the preceding sections of this paper have referred to the term "Domain" several times, this section formally defines an Administrative Domain to set the context for later sections. An Administrative Network Domain is an Autonomous System (as referred to in RFC 1930 [79]) comprising a finite amount of computing and communication resources segregated among several Edge/Cloud assets following a set of policies confined under a single administrative boundary and managed by a management & orchestration platform a.k.a. a domain orchestrator. Another term, "Task", that is referred to several times in the following text originates from **Task Oriented Networking** [80]–[82] and is defined as a *flow of processes performed by the collaboration of participating systems*, as explained in detail in Sec. IX-A

We propose Cross-Domain Orchestration as a hierarchical orchestration paradigm implemented as a hub-and-spoke model, where the spokes are the domain orchestrators. The Cross-Domain Orchestrator serves as a hub, coordinating between downstream domain orchestrators to provide cross-domain end-to-end services. To differentiate between the two levels of orchestration, we will refer to the domain orchestrator as an Intra-Domain Orchestrator (IDO), which manages and orchestrates resources within the administrative domain it oversees. Therefore, the CDO only negotiates with the downstream IDOs and does not interfere with the management and orchestration of the domain-level resources. The segregation of control preserves the autonomy of the administrative domains while keeping the CDO in a supervisory position that delegates tasks to IDOs through negotiation.

The top-down orchestration stream from the CDO to the domain resources may be realised as follows. The CDO as a software entity sits at the root of the orchestration hierarchy (e.g., a generic distributed system deployed as cloud instances). It communicates with several downstream IDOs that manage and orchestrate domain resources following a standardised mechanism (e.g., ETSI MANO [83]). Beneath the IDO are the controllers for computing and communication resources, such as hypervisors and network controllers, respectively. At the final stage, physical assets like servers and network segments host the virtual computing and networking infrastructure. Figure 3 depicts an outline of the top-down split-orchestration.

We justify the preservation of autonomy across the layers described above by four principles, which shall unfold in the remainder of this paper and influence the design pattern we propose. These are: First, CDO-IDO interaction through a Cross-Domain Communication Fabric; second, service negotiation by the CDO with the customer (service consumer) and the providers (service provider) through Service Level Agreements; third, Capability Exposure by the IDO to the CDO; and fourth, Continuous Monitoring of the cross-domain life cycle by the CDO.

B. END-TO-END CROSS-DOMAIN ELEMENTARY SERVICES

In REASON, we classify the E2E services provided by virtual network functions (VNFs) into four categories. Each category offers network service instances across multiple domains to cater to various service requirements, including customer E2E service composition.

1) Connectivity Service

This section describes differentiated connectivity services. Generally, a complex service is broken down into several elementary technical services, each managed at the domain level with specific granularity. These elementary services are aggregated at the multi-domain level to meet complex service needs. The scope of a cSLA associated with a particular complex service delineates where policies are enforced, such as geographic or topological regions. An elegant way to represent such aggregation is through a graph model, which enables the application of graph-theoretical principles and algorithms to abstract a complex service into a computable object. A Graph defines relationships between abstract objects called Nodes. Therefore, we identify five aggregation options described by Goderis *et al.* [84] to represent relations between elementary services treated as nodes.

1) *One-to-One or Pipe Model* service type: e.g., for seamless device-to-device or user-to-user connections.
2) *One-to-Many or Hose Model* service type: e.g., for efficiently distributing configuration information to many IoT devices.
3) *One-to-Any or Unspecified Hose Model* service type: e.g., for broadcast services.
4) *Many-to-One or Funnel Model* service type: e.g., for streamlined aggregation services.
5) *Any-to-one or Unspecified Funnel Model* service type: e.g., for dynamic converge-cast-like services.

2) Computing Resources and Services

These services offer a combination of cloud and edge computing capabilities to execute compute-intensive tasks, such as data processing and rendering, by provisioning physical assets (server clusters) and virtual assets (virtual machines or containers).

3) Security as a Service (SECaaS)

This service aligns with Security Service Level Agreements (SSLAs), ensuring it meets the specific security requirements of customers and businesses requesting different security classification levels. It can be derived from the c/pSLAs and domain security policies and must fulfil the criteria for cross-domain security management.

4) Auxiliary services

These services may include AI/ML as a Service, which can provide predictive functionality and analysis using service-aware ML models from domain-level service providers or third-party providers. Another service in this bracket is Content Delivery as a Service, where a provider prepares and delivers on-demand content to consumers via a web service. Other services in this category include VNF as a Service, where third-party providers offer a repository of ready-to-use VNFs, time synchronisation, location services, etc.

C. SPECIFIC EXAMPLES OF E2E COMPLEX SERVICES

In the context of the REASON project, the following use cases, given in summary, are specific examples of the composition of the E2E elementary services (described in IV-B).

The **Internet-Scale Metaverse** use-case (ISM-UC) promotes the use of Web3 architectural elements to enable symbiotic 3D internet, aiming to migrate internet users from traditional web-based interfacing to a simulated digital environment leveraging spatial computing. ISM is conceptualised to constitute services like Augmented and Vitual Reality (AR/VR) for rendering the environment that reliably connects a variety of end-user equipment using the Internet of Things (IoT) technology while providing decentralised security using Digital Ledger Technology (DLT), all together enhancing the Social Networking experience in a Metaverse. ISM's Key Value Indicators (KVIs) include Quality of User Experience (QoE/UX), privacy, digital identity, token-based asset tracking, sustainability and democratisation of content creation. Some of the Key Performance Indicators (KPIs) to ensure the delivery of such services include 5-100 Gbps of bandwidth with 0.1 to 20 ms of latency, Six-9s (i.e., 99.9999%) reliability, symmetric high capacity over long-distance communication, a scalable and reliable transport network, decentralisation of trust, interoperability, and energy consumption.

The **Industrial Metaverse** (IM-UC) is a spatial Metaverse use case that focuses on high-reliability and precision engineering for industrial applications. IM-UC targets digital twin and their scalable interaction by leveraging stringent communication requirements with sensor fusion and time synchronisation to ensure the interoperability of physical and virtual real-time systems while confirming security by design. IM-UC's KVIs enable spatial computing in industrial automation, healthcare, and remote management of industrial jobs, as well as offloading risky tasks from humans to machines. The KPIs for such services include device synchronisation, guaranteed channel capacity, position accuracy and redundancy.

The **Future Factory** use case (FF-UC) targets similar objectives as IM-UC but excludes special computing and emphasises more on Time-Sensitive Networking (TSN). It aims to provide a robust network infrastructure that supports stringent latency requirements by leveraging xHaul technology for seamless device collaboration across multiple access technologies, with QoE assurance (i.e., time, delay, and jitter-sensitive multi-access backhaul) to enhance the interoperability of machines in heavy manufacturing industries. FF-UC's KVI includes economic sustainability, democratisation of skills, and digital inclusion. The KPIs based on the application level are, near live (latency below 1.7ms with negligible jitter), two-way (with latency below 150 ms and jitter below 50 ms), multi-way (with latency below 50 ms and jitter below 25 ms) and distributed remote live (with jitter 15 ms and Jitter below 1 ms).

The **Virtual Production** use case (VP-UC) focuses on synchronising cyber-physical systems on a reliable communication fabric with precise location support. It aims to achieve holistic digital mirroring of a physical warehouse for real-time asset tracking and tracing, utilising autonomous robotics that operate in dense and dynamic environments. VF-UC leverages high-capacity, reliable networking, as well as digital twin and autonomous robotics technology, to achieve these goals. The KVIs are reduced electromagnetic radiation, trustworthy machine intelligence, scalability and adaptive networking. VP-UC's KPIs are precise localisation (below 1 cm), orientation accuracy (less than a degree), data rate (at least 1 Gbps), and latency (not exceeding 20 ms).

Finally, the **Sustainability, Service Differentiation, and Security** use case (SSD-UC) aims to reduce energy consumption and emissions of greenhouse gases by avoiding over-provisioning resources. It leverages various optimisation techniques to collaborate, such as resource allocation, policy enforcement, energy-aware scheduling, routing optimisation, performance monitoring and fault tolerance. In REASON, we realise that such optimisation occurs globally while provi-

TABLE 9. Brief description of Stakeholders' roles

Main Stakeholder	Brief Description
Cross Domain SP	CDO owner & Offers E2E Services
User/Customer	Consumer of Cross-Domain services
Content Provider	Provides contents
Network Providers	Offers network resources & connectivity
Terrestrial Net. Providers	Provides telecom core
Edge Provider	Provides edge computing
Cloud Provider	Provides cloud computing
Edge Provider	Provides edge computing
AI/ML Provider	Provides AI/ML as a service
Marketplace Provider	Provides catalogue of E2E services

sioning an end-to-end service across multiple domains. The KVIs are characterised by a reduced carbon footprint per bit, economic sustainability, and flexibility in power sourcing. The KPI's are power consumption and resource utilisation efficiency.

V. ORGANISATIONAL VIEW

A. STAKEHOLDERS ECOSYSTEM

This section presents the Organisational View (i.e. Business Ecosystem) 2, identifying the stakeholders with an interest in the CDO operation (Figure 2). The section also discusses cross-domain interconnection models from a business perspective, focusing on E2E service offerings. It also specifies the business opportunities that arise from CDO capabilities through seven monetisation models.

The Organisational View identifies the stakeholders who: 1) have stakes in, and are responsible/accountable towards, E2E cross-domain service offerings (e.g., various providers), 2) contribute assets (e.g., vendors), 3) are interested in and could benefit from the REASON project's outcomes (e.g., manufacturers and developers), and 4) care about the REASON project results (e.g., regulatory bodies and government). We identify the following ten main stakeholders of interest in Figure 2 and Table 9.

Customers can subscribe to the E2E services that a Cross-Domain Service Provider (CD-SP) offers. Customers nominate Users who are the recipients of these services, and the CD-SP is responsible for obtaining and delivering services from various providers without necessarily owning networking infrastructure. Content Providers (CPs) gather, create, and distribute digital information, offering it to users and other service providers. Network Providers (NPs) offer connectivity services, while Access Providers provide last-mile network connectivity. Terrestrial Network Providers (Core) interconnect network parts, while Edge providers deliver services close to the users' access point. Cloud Providers offer on-demand computing resources. AI/ML Providers deliver customised models and analytics, and Marketplace Providers offer platforms for advertising the service capability of CDO and the domains. Other stakeholders, such as device manufacturers and technology developers, may not be directly involved in service provisioning but can participate in the provisioning of infrastructure, platforms, or technologies.

B. CROSS-DOMAIN INTERCONNECTION MODELS FOR OFFERING END-TO-END SERVICES

We consider possible ways to place the CDO as an entity and enable interaction with the downstream domains, leveraging the centralised, distributed, and decentralised architectures of large-scale distributed systems as three models (i.e., Centralised or Hub, Cascaded, and Hybrid) described below. Please note that all orchestration-oriented interactions are open, asynchronous and stateless (i.e., RESTful)

The **Centralised or Hub Model** assumes the Cross-Domain Service Provider (CD-SP) to be a highly efficient business entity. The CDO is the central point for orchestrating and delivering services and resources across the E2E delivery chain. In the Centralised Model, the CDO is collocated in an operations centre (not with any specific domain), orchestrating and managing services across multiple domains. This model ensures that each domain handles its domain-level network resources and services effectively. The CDO operates following the Hub Model when collating with the source domain.

The **Cascaded Model** encourages collaboration since each domain's orchestrator negotiates agreements with its immediate neighbouring domain to establish an E2E service chain and delivery. The originating domain (e.g., CDO) takes responsibility for providing orchestration functionality to compose the E2E service delivery. Relevant information is passed between the participating domains, ensuring a seamless and inclusive process. With this model, service peers are also network-routing peers, further enhancing the collaborative nature of the Cascaded Model.

The **Hybrid Model** combines the centralised and cascaded models through a decentralised architecture with multiple CDOs, each orchestrating E2E services across a set of downstream domains, while interacting with other CDOs.

In REASON and this paper, we consider the Centralised Model to create the orchestration functionality, as shown in Figure 3, instilling confidence in its efficiency and capabilities.

C. CROSS-DOMAIN SERVICE OFFERING

The Salience Model [85] identifies stakeholders based on three key variables: Power, which represents their ability to influence a project; Legitimacy, which signifies their authority and level of involvement; and Urgency, which reflects the stakeholders' expectations and need for prompt action.

In this model, definitive stakeholders are the most direct and critical category of stakeholders, covering the three variables above. Figure 4 shows the definitive stakeholders that have been the focus of the REASON project for cross-domain service offerings. This figure depicts the interrelationship between various providers and customers. It demonstrates how providers can establish appropriate business or contractual relationships to offer end-to-end, cross-domain services.

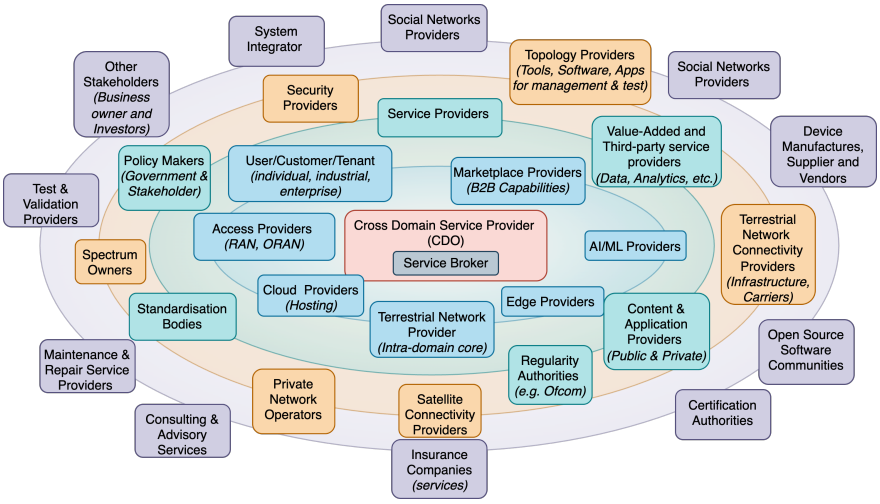


FIGURE 2. Organisational View - Business Ecosystems.

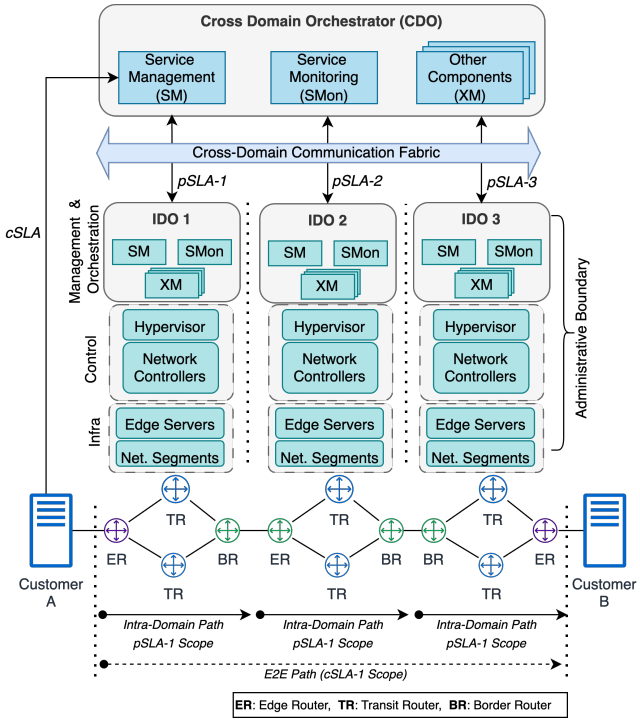


FIGURE 3. Centralised/Hub interconnection model.

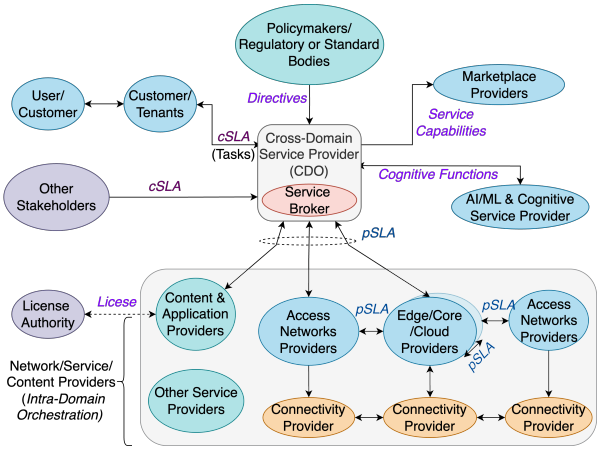


FIGURE 4. Definitive Stakeholders and their Interactions.

D. BUSINESS MODELS

Based on the formation of the four Architectural Views, we have identified seven business model opportunities as described below:

1) *Subscription Model*: This model provides customer-to-business (C2B) and business-to-business (B2B) service subscriptions. Customers can subscribe to the services fulfilled by the CDO. This model reduces uncertainty and risk by assuming the services will be available when needed based on the subscriptions made.
2) *Trading Model*: This model focuses on trading between the CDO entity and the IDOs for the services offered to the CDO through pSLA and the services the CDO provides to the enterprise customers via cSLA.
3) *Brokerage Model*: Service brokering brings providers and customers together on a platform, assuming the roles of Service Order Handling, Service Decomposition, and Service Composition.
4) *Auxiliary (Supporting) Service Model*: Specialised small and medium-sized enterprises (SMEs) offer highly sophisticated and novel services, such as training and deploying specialised AI/ML models for supporting CDO/IDO operations, as well as providing AI/ML-as-a-service to customers.
5) *Advertising Model*: A marketplace provider offers a service in the form of a platform for service capability advertisement, instantly providing a route to the common services offered by the entities that own CDOs and IDOs.

6) *Infomediary Model*: The CD-SP or a third-party company gathers valuable data about network status and customer data and analyses and uses the information to tune network configurations and AI/ML model performance.
7) *Utility Model*: This "on-demand" or "pay as you go" approach exploits services that are either already provisioned and available for use, supplementing the Subscription Model, or created on-the-fly.

VI. FUNCTIONAL ARCHITECTURE VIEW

The Functional Architecture View (FA) represents the high-level technical architecture of the CDO. This view provides a solution-independent description of the functions, activities, and resource and information exchanges required to achieve the mission of the cross-domain service offering. This section outlines the functional architecture which is represented in **five Sub-Views**, namely: Cross-domain Service Management Sub-View (SM-SV) described in Sec. VI-B, Policy Management Sub-View (PM-SV) described in Sec. VI-C, Network Management Sub-View (NM-SV) described in Sec. VI-D, Trust & Security Management Sub-View (T&SM-SV) described in Sec. VI-E, and the Service Monitoring Sub-View (SMon-SV), described in Sec. VI-G. Cognitive Functions (CFs) which support the functional architecture are described in the Cognitive & AI/ML View (Sec. VII-B).

The CDO Functional Architecture is shown in Figure 5, which also depicts the organisation of various Functional Blocks (FBs) grouped in sub-views. In the figure, we have used acronyms of the FBs that have appeared frequently in this paper; the rest of the FBs with limited mentions are named in full. Additionally, it refers to the various interactions between the downstream domains through a secure communication channel we refer to as the CDO Communication Fabric (explained further in Sec. VI-F3) and interfacing with the E2E AI Plane (Sec. VII-A). While offering an E2E service, CDO and IDO provide monitoring capabilities with separate concerns. While the IDO's responsibility is to manage, orchestrate, and monitor domain resources and service compliances within its administrative boundary, the CDO is responsible for end-to-end service level delivery and compliance, utilising the resources of the participating domains. That said, the CDO does not interfere with the autonomy of the domains. Therefore, it negotiates any service placement or task delegation with the IDOs. Content providers are onboard with their service offerings on the domains. The IDOs advertise these capabilities to the CDO, which composes them into complex tasks. The CDO advertises the complex tasks as end-to-end (E2E) service offerings for customer use. The customer places a task request with the CDO, which the CDO decomposes into an end-to-end (E2E) service partially fulfilled by the underlying peer domains after negotiation. The Marketplace provides a portal for customers to choose from a catalogue of the various Tasks the CDO offers. Various Policymakers, including business and public authorities, can also define policy constraints at the PM-SV through the CDO communication fabric.

A. CDO MANAGER

The CDO Manager oversees all functionalities in the architectural sub-views; however, its exact role depends on the level of autonomy the CDO operates at (described below). It manages the activities that support the CDO's operating functions. It comprehensively understands the entire CDO functionality and can manage and request supporting actions from various entities. It is worth mentioning that the CDO AI/ML Manager (CAM), a component of the CDO Manager, facilitates the CDO's interaction with the AI Plane to provide cognitive support for various end-to-end (E2E) services. The CDO AI/ML Agent (CAA) accompanies CAM by providing interfaces and endpoints through which it makes requests to the AIO (AI Orchestrator). In return, it receives an ML service descriptor (in the form of a pipeline) from the AIO with some deployment suggestions (such as resource requirements and placement). CAM makes subsequent invocations of various CDO functions to handle a successful resource allocation and pipeline placement. Sec. VII-A describes the operating principles of CAM and CAA in more detail.

1) Four Levels of Autonomy

Future Open Networks are envisioned to be autonomously controlled and managed [86]–[88]. However, transitioning from a human-controlled system to full autonomy poses significant challenges. These include the maturity of automation technology, harmonisation of AI/ML functions and decision-making processes, the adequacy of training datasets for data-driven models to match the decision-making accuracy of humans, and, at the same time, maintaining trustworthiness. Therefore, the method of control by the CDO is expected to evolve gradually, as indicated below:

- ***Level-1****: Full Human Control*: In this initial step, a human, specifically the CDO Manager, possesses complete control over every aspect of the CDO's Orchestration and Management (C&M) functions.
- ***Level-2****: Human In the Loop*: The CDO performs some functions intelligently and independently but requires a human to perform functions that complete the CDO's O&M task cycle.
- ***Level-3****: Human On the Loop*: The CDO performs all functions intelligently and semi-autonomously. However, a human may intervene to stop or modify the outcome before the task is completed.
- ***Level-4****: Human Starts the Loop*: In the final step, a human sets the operational parameters and initiates the CDO operation intelligently and autonomously in harmony; the CDO requires no further human interaction to complete the task.

2) Service Level Agreements (SLA)

The Service Level Agreement is a formal contract in which the orchestrator (CDO/IDO) agrees to fulfil a service request. The **Customer SLA** (cSLA) is an agreement between the customer and the CDO for a service offering, including the

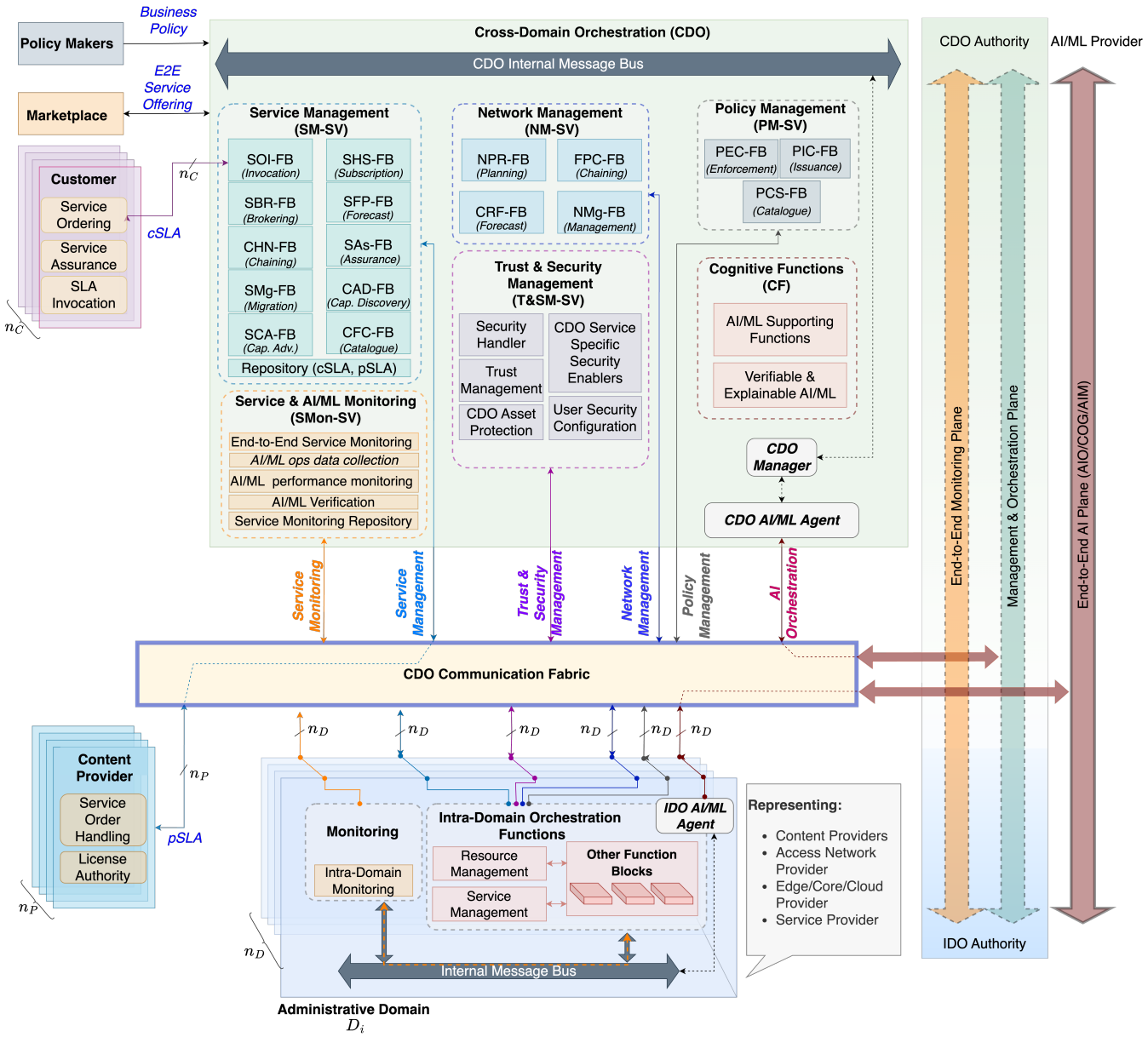


FIGURE 5. Functional Architecture View - Cross Domain Orchestrator and its interactions.

constraints on a customer agreement before subscribing to an E2E service. A **Provider SLA** (pSLA) is an agreement for a bulk of differentiated services that can fulfil the requirements of multiple customers. It is established between CD-SP and administrative domain providers through CDO and IDOs. As a service can be provided with various QoS levels, this will be reflected in the cSLA and the pSLA, as described by Georgatsos *et al.* [89].

3) Service Provisioning Cycle (SPC)

The service provisioning cycle (SPC), described below as a state diagram, governs the life cycle of AI-Native E2E services served across multiple domains. Its primary objective is to pre-provision pSLAs between domains for anticipated service demands from customers based on historical subscription data. Function blocks referred to in this description are described in detail in the following sections (Sec. VI-B and Sec. VI-D)

The entry point to the SPC is the Service Forecast & Provisioning (SFP-FB) function block, which receives historical subscription data (a time series of cSLAs) from the Service Order Handling and Subscription (SHS-FB) function block. The subscription data includes accepted and rejected customer service requests. Analysing the historical cSLAs and present subscription status, SFP-FB forecasts the anticipatory demands of services aggregated across the domains. The SFP-FB returns the anticipated aggregated service demands.

The Cross-Domain Resource and Function Forecast (CRF-

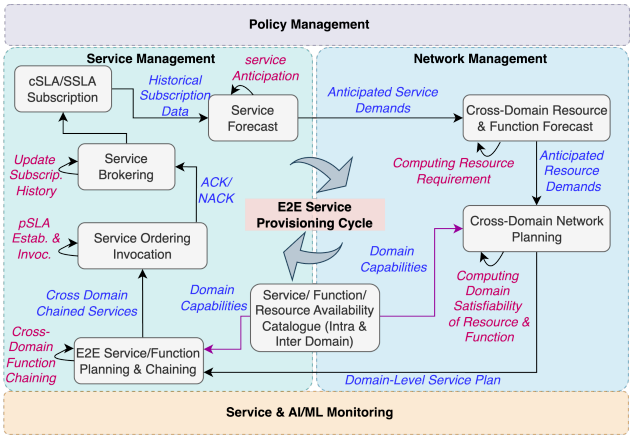


FIGURE 6. End-to-End Service Provisioning Cycle (SPC).

FB) function block receives the anticipated aggregated service demands from SFP-FB, computes the computing and communication resources required to satisfy the demand, and returns the anticipated aggregated resource demand across the domains.

The Cross-Domain Network Planning & Route Management (NPR-FB) function block receives the anticipated aggregated resource demands from CRF-FB. It then looks up the resource and function availability of the underlying domains from the Domain-Advertised Common Function Catalogue (CFC-FB) function block. It returns a domain-level service function plan that maps the elementary services to a feasible domain. The E2E Service Function Chaining (CHN-FB) function block receives the domain-level service function plan from the NPR-FB. Based on the domain-level plan, it computes the optimal chaining of various domains to establish E2E services and returns the cross-domain service-function chain (CD-SFC).

The Service Ordering and Invocation (SOI-FB) receives the CD-SFC from CHN-FB. First, it establishes and then invokes pSLAs between the participating domains based on business policies managed by the Policy Management sub-view. Upon receiving acknowledgements from the domains, SOI-FB confirms the availability of domain-level service and resources. In case pSLA invocation fails, SOI-FB signals CHN-FB for an alternate CD-SFC. If no CD-SFC is feasible, the respective customer service demands are marked as rejected (i.e., not feasible to be accepted by the CDO).

The Service Broker (SBR-FB) receives confirmation from SOI and makes the corresponding cross-domain service offerings available to the customer in the marketplace. Finally, anticipated services (both feasible and infeasible) are included in the subscription data.

B. SERVICE MANAGEMENT SUB-VIEW (SM-SV)

The Service Management Sub-View is responsible for managing the overall lifecycle of an E2E service, described as the SPC (see Sec. VI-A3). This section describes the various Functional Blocks related to the operation of SM-SV and its interactions with external customers, internal CDO Functional Blocks, and IDOs (Figure 7); all interfaces are RESTful.

1) Service Handling and Subscription Functional Block (SHS-FB)

The Service Handling and Subscription Functional Block (SHS) is the CDO's point of contact for customers, providing clients with services across multiple domains. In addition, it implements the server side of the SLA negotiation process with the customer, performing subscription-level admission control and handling the subscription of cSLAs [90]. The cSLA defines the terms of access, which are negotiated and agreed upon between the CDO and the customer.

2) Service Ordering and Invocation Functional Block (SOI-FB)

An IDO advertises its capabilities to the CDO via the marketplace in the form of elementary tasks. The CDO composes these elementary tasks into several complex tasks for the customer to choose from, with an associated level of QoS. The CDO can initiate negotiations with the candidate domains to provide services to meet QoS needs and fulfil anticipated demands. Further, it establishes service-specific pSLAs with the respective domains. The composition of such pSLAs contributes to the cSLA offer of the E2E service corresponding to the complex task. A cSLA negotiation occurs between the CDO and the customer before establishing an E2E service and tearing it down when the cSLA has expired or can no longer be offered. Once established, the CDO informs the corresponding IDOs to commit the respective domain-level resources, maintaining the pSLAs. The Service Ordering function establishes contracts between CDO and the peered domains (IDOs) as pSLAs, and the Service Invocation function ensures the providers' resource availability at service invocation time for immediate use by customers, utilising a set of admission control algorithms.

3) Service Brokering Functional Block (SBr-FB)

IDO closes such negotiation with a concluding acknowledgement we refer to as Domain Technical Response that includes either an acceptance with an agreeable plan or a refusal with a justification

This Functional Block receives and handles new customer service requests through cSLAs from SHS-FB and provides domain-level resources for E2E services in advance, leveraging the forecast received from the SHN-FB. It gives the service decomposition, i.e., a mapping from complex tasks to elementary tasks, and the service composition, i.e., a mapping from elementary tasks to complex tasks. It processes the service composition to make a function composition instance. If the current state of the provisioned resources fails to satisfy the composition instance, SBr-FB, through the SOI-FB, initiates fresh requests to the corresponding IDOs. Otherwise, SOI-FB invokes domain-specific function

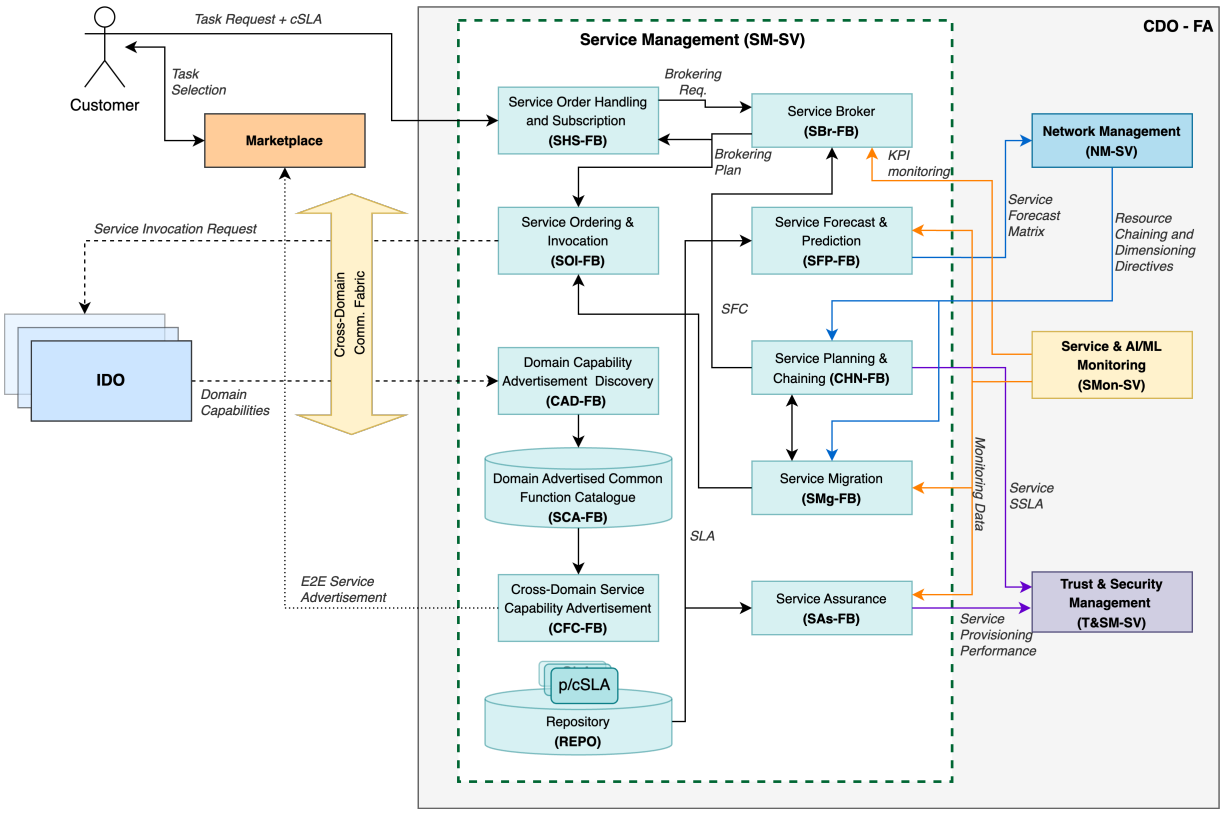


FIGURE 7. **Internal and External Interactions of Service Management Functional Blocks.**

compositions through negotiation with the IDOs. An IDO closes such negotiation with a concluding acknowledgement we refer to as Domain Technical Response that includes either an acceptance with an agreeable plan or a refusal with a justification. The factors influencing such decisions include infeasible pSLA, technical restrictions, policy constraints, unsatisfactory charges and KPI targets. The SBr-FB proposes a Brokering Plan to the SOI-FB, which contains details of the task owner, function composition, and associated costs. It provides the service composition as an explainable response, i.e., a response backed by policy-based reasoning, e.g., topology structure, high charges, lower KPIs, task duration, etc. Re-brokering might happen based on analytics. The brokering cycle continues until the SM-SV, via SBr-FB, aggregates a brokering plan with pSLA that is agreed upon and discovered across all the IDOs.

4) Service Forecast and Prediction Functional Block (SFP-FB)

This function forecasts and aggregates service demands using historical usage data and service requests. It anticipates domain-level resource requirements before initiating a new provisioning cycle and utilises historically established and failed pSLAs and cSLAs to enhance the accuracy of future service estimates. SFP-FB is utilised for pSLA negotiation between the CDO and the IDOs.

5) Service Planning & Chaining Functional Block (CHN-FB)

This function determines the required domain-level resource type (e.g., computing and connectivity, etc.), quantity (e.g., number of CPU or GPU cores, storage volume, memory capacity, etc.), and geographical location and the functions that chain them into an E2E service as Service Function Chaining (SFC) that complies with the predicted customer demand. The interconnection between the service functions may span beyond any administrative boundary, requiring additional network provisioning. Such provisioning includes the composition of VNFs in an SFC, embedding the SFC into a substrate network and scheduling the VNF instantiation from a shared repository. SPC can combine several VNFs to build a super-service, providing more flexibility in service composition and reusability and promoting agile practices, such as rapid development and deployment of services for customer use.

6) Service Migration Functional Block (SMg-FB)

This function manages the migration of services across the domain boundary to accommodate any network dynamics or demand fluctuations (e.g., sudden unavailability of service or resources due to failure, or avoiding disruption during rolling updates). It optimises the overall resource utilisation, ensuring efficient service delivery. When the Service Monitoring (SMon) detects a victim service that fails to receive the requested QoS, the CDO manager triggers a three-step

process at the SMg-FB. By leveraging the Common Function Catalogue, the SMg-FB first attempts to discover another domain capable of hosting the victim service, retaining the current domain settings. In the event of an unsuccessful attempt, it initiates the service by selecting a new domain with the updated configuration. Failing that, it enters the service re-provisioning cycle. In summary, strategic migration enables the seamless relocation of live services across domain boundaries to achieve optimal performance tuning, scalability, and resilience, while ensuring that services meet the required performance thresholds in dynamic Future Open Networks.

7) Cross-Domain Service Capability Advertisement (SCA-FB), Domain Capability Advertisement Discovery (CAD-FB) and Cross-Domain Advertised Common Functions Catalogue (CFC-FB)

The service manager handles the advertisement of cross-domain services by coordinating three function blocks. Each IDO spontaneously advertises the domain capability to the CDO, where the CAD-FB sits at the receiving end. CDO maintains a database that stores all discovered capabilities and their advertising domain information, which we refer to as CFC-FB. Ideally, the FB is not the database but an interface behind which the actual database resides. When composing cross-domain services, the CDO interacts with CFC-FB to calculate the capabilities available across domains. Finally, the SCA-FB abstracts the domain-level capabilities and advertises cross-domain capabilities to the marketplace.

8) Service Assurance Functional Block (SAs-FB)

The Service Assurance function enables the CDO to monitor and predict probable cross-domain network issues, ensuring compliance with the QoS negotiated between the customer and the CDO in the cSLA and E2E services being offered. "Service Assurance" receives the monitored performance statistics from the "Service & AI/ML Monitoring" functions (see Sec. VI-G) and compares the data with the contracted service levels agreed in the SLAs to confirm that the service peers (domains) are delivering the agreed service levels. The "Service & AI/ML Monitoring" receives monitoring information from peered domains (IDOs) and constructs an E2E service monitoring profile for CDO services.

C. POLICY MANAGEMENT SUB-VIEW (PM-SV)

A policy is a set of rules to control the state of one or more managed objects that affect a system's overall behaviour [91] [92]. The Policy Management influences the behaviour of various CDO functions. We classify the policies into three categories: Government Policies (e.g., national security, peering restrictions, and GDPR), Business Policies (e.g., value-added services such as resource reservation, charging, and interoperability between other domains), and Configuration Policies (e.g., customer service security, authorisation, and network management). Policies derived from a business intent must coexist harmoniously with other policies for a stable system. The REASON architecture promotes interoperability by using standard-based policy definitions to enable end-to-end (E2E) services, allowing operators to interface through open APIs.

The remainder of this subsection describes the three Functional Blocks of the Policy Management Function.

1) Policy Enforcement and Compliance Functional Block (PEC-FB)

This Functional Block focuses on comprehensive policy management within the CDO, ensuring seamless creation, execution, and integration of policies through the following capabilities: 1) Policy Editing enables the crafting of different policies to meet E2E service requirements; 2) Policy Language Translation facilitates interoperability across diverse platforms or languages; 3) Policy Validation provides mechanisms to ensure consistency through conflict detection and policy verification; 4) Policy Broker manages and federates policies from different domains, ensuring that cross-domain policies work harmoniously; 5) Policy Decision considers contracts, capabilities, constraints; 5) Policy Execution to ensure policies are effectively advertised and enforced. Furthermore, an event bus is embedded within the CDO architecture to handle internal communication and coordination between components, enabling real-time responsiveness across the policy management paradigm.

2) Policy Issuance and Consumption Functional Block (PIC-FB)

The Policy Issuance and Compliance function manages and enforces policies. It has two primary responsibilities: First, Policy Issuance, which creates and formats policies; second, Policy Consumption Specification, which describes the policy consumption rules by application, individuals and other architectural components of REASON. These consumers apply the policies in their workflows, adhering to the laws and regulations outlined.

3) Policy Catalogue Service Functional Block (PCS-FB)

The PCS-FB operates as a repository. The policy repository stores the policies, their descriptors, and templates related to the target managed service and resource instances.

D. NETWORK MANAGEMENT SUB-VIEW (NM-SV)

This section discusses the four FBs that constitute Inter-domain Network Management Sub-View at the inter-domain level, namely, domain-level interconnections, resource/function chaining, network management run-time operations, and customer resource forecast. Figure 8 summarises this section by depicting the various interactions between the function block internal and external to the network management; all interfaces are RESTful.

1) Cross-Domain Network Planning & Route Management Functional Block (NPR-FB)

This Functional Block establishes a configurable routing fabric between domains and those already registered to instan-

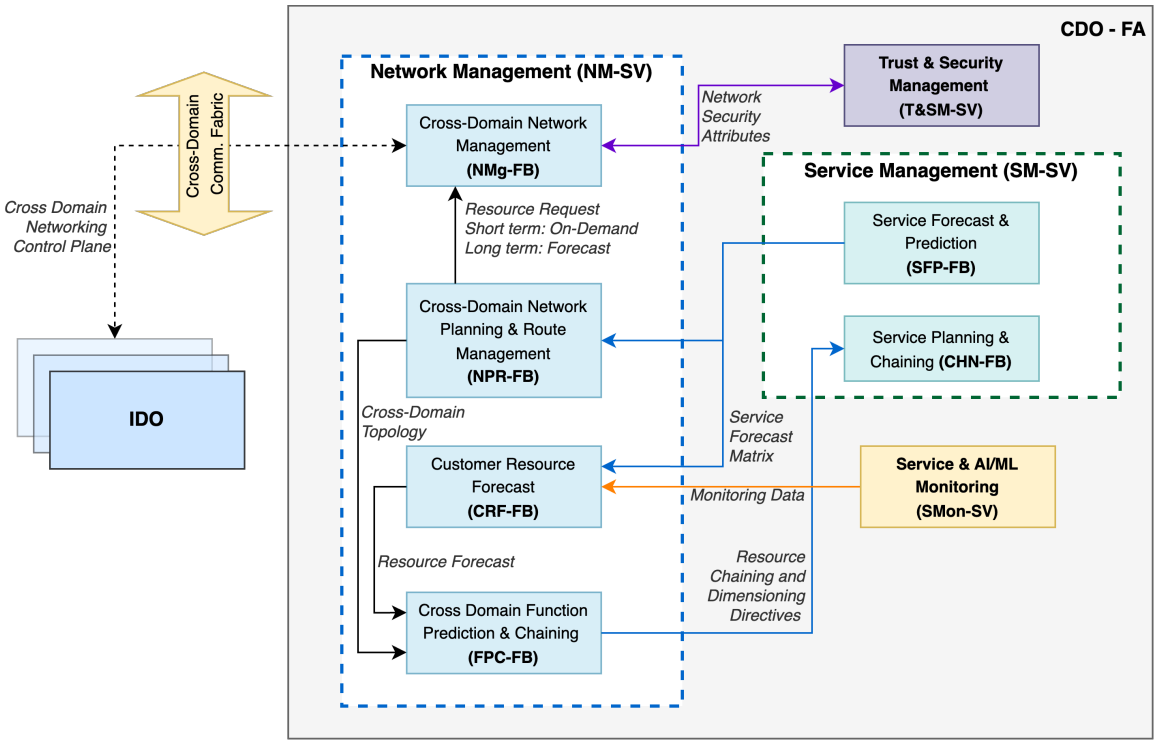


FIGURE 8. Internal and External Interactions of Network Management Functional Blocks.

tiate end-to-end (E2E) services, complying with the cSLA requirements. The provisioning of such fabric provides a virtual instance of a dedicated network control plane specific to the E2E services. CDO can leverage Policy-Based Routing (PBR) models defined in RFC 1104 [93] to control inter-domain traffic flow forwarding using custom routing policies (i.e., path-finding algorithm and metric) specific to a service requirement. For instance, an E2E service that aims to reduce energy consumption may use a custom metric with energy consumption as a parameter so that the routing protocol using such a policy prioritises a particular path with lower cumulative energy consumption. Our previous work [94] presents a framework called *Intelligent Routing as a Service* (iRaaS), which offers a client-server model for application-level, customisable PBR capability.

2) Cross-Domain Function Prediction & Chaining Functional Block (FPC-FB)

When an SPC instantiates, the Service Forecast function within the SM-SV produces a Service Forecast Matrix (SFM) that records the type, quantity, quality, and geographical location of each service provisioned. The route plan and resource forecast information predict the resources and function chain that fulfil the anticipated service demand. Furthermore, it maps the predicted resources to the capabilities (both functional and resource-based) advertised by the domains and provides them to the SPC. Thus, it accommodates the predicted demands of the advertised capabilities.

3) Cross-domain Network Management Functional Block (NMg-FB)

This function ensures that run-time operations across multiple domains are realised. Resource provisioning can occur over a range of time scales. In the long term, the NPR-FB requests new or additional resources and functions from the network peers (IDOs) based on new forecasts and provisioning cycles. In the short term and during runtime, it requests the creation of new resources and the modification of existing capabilities.

4) Customer Resource Forecast Functional Block (CRF-FB)

This function takes the Service Forecast Matrix from the Repository within the SM-SV, historical subscription and network usage statistics from the SMon, and related policies from the PM-SV to dimension the cross-domain routes and intra-domain resources. Additionally, it validates the accuracy of the resource forecast against actual resource usage and service requests, triggering various alarms from the IDO's Network Service functions. Moreover, it revises the forecasting model if the accuracy drops below a cutoff.

E. TRUST AND SECURITY MANAGEMENT SUB-VIEW (T&SM-SV)

The proposed CDO architecture assumes the domains have dedicated security enablers implemented and operated within their administrative boundary, which can follow the ITU-T X.805 standard [95]. The Trust and Security Management (T&SM) Sub-View encompasses the security aspects of services supplied to customers and the internal functions of the

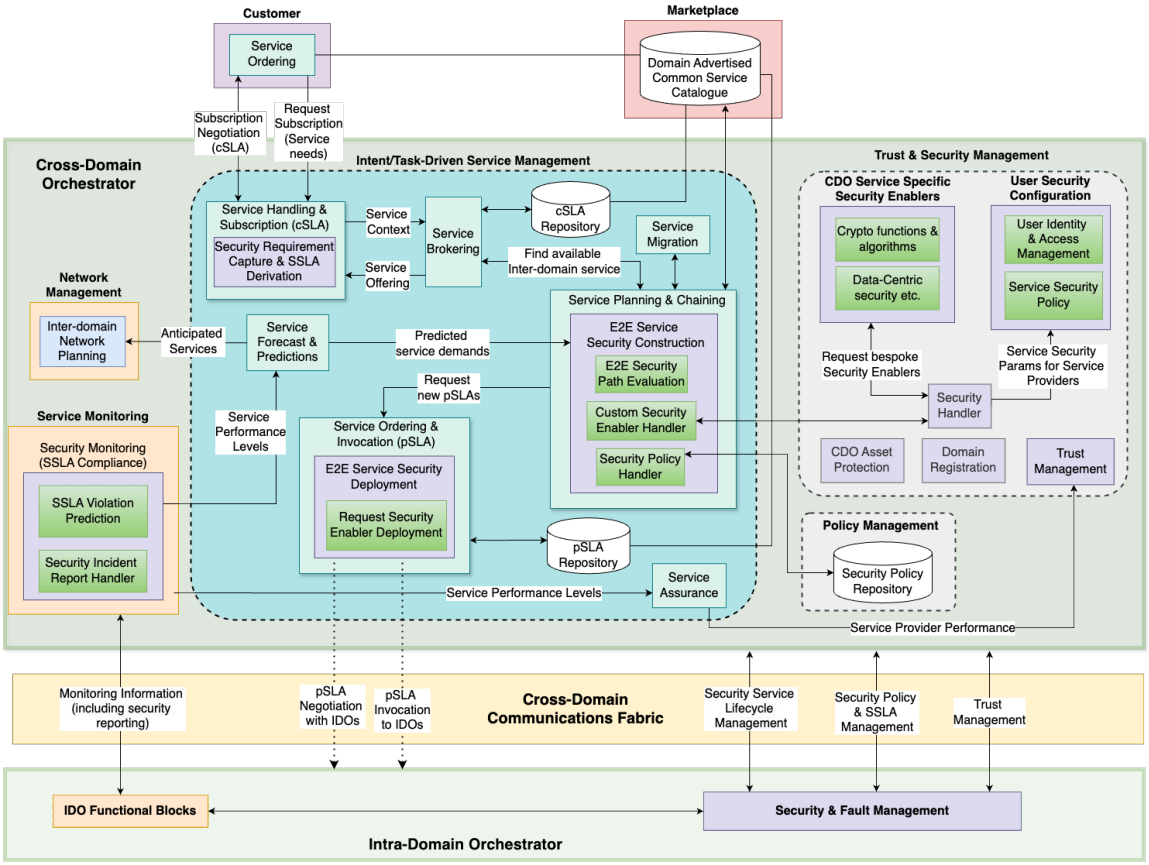


FIGURE 9. **Trust & Security Management Sub-View and its interactions with Functional Blocks in Other Sub-Views of the CDO Functional Architecture.**

CDO. The T&SM Sub-View provides a centralised cross-domain security management framework that creates an E2E service perimeter of the CDO and participating IDOs. The T&SM supports the distribution of security functions by delegating security responsibilities to participating IDOs as described in the Security Management and Orchestration of the HEXA-X project [96]. Figure 9 decomposes the T&SM Sub-view, provides further details about its internal Functional Blocks, and depicts the interactions with other functions performed within the CDO.

1) Domain Registration Process

The CDO is initially unaware of the underlying domains participating in the cross-domain orchestration. Therefore, domains based on their business interests register with CDO. The domain administrator submits a domain registration request to the CDO Domain Registration function (see Figure 9). The domain administrator would provide some relevant 'proof of identity' documentation via an out-of-band channel (e.g., in an email) to the CDO administrator, who would use this to verify the domain details and approve the registration request. Following successful registration, the CDO Manager/Administrator arranges for the deployment of a 'Domain Proxy' agent, which provides a means for the CDO and IDO Service Management and Orchestration functions to interact with each other (e.g., to discover/advertise domain capabilities, request allocation of resources, etc.).

2) Security Functions within Service Management & Service Monitoring

The CDO's Service Management ensures real-time compliance with E2E services from a security perspective and implements 'Security as a Service' (SECaaS) for customers. The SECaaS can be an automated function based on Security Service Level Agreements (SSLAs) derived from the c/pSLAs, security policies, and the ETSI Zero-touch Service Management (ZSM) approach [97]. To provide the various aspects of SECaaS, the CDO implements the following core functions, as outlined in the NIST Cybersecurity Framework [98].

1) *Identification*: Define customer/CDO security requirements for E2E services and document them as a security SLA. Establish an end-to-end (E2E) path per the security service level agreement (SLA), requiring each administrative domain to share security function information with the Chief Data Officer (CDO).
2) *Protection*: As part of automated service provisioning, ensure each administrative domain deploys security enablers to mitigate risks.

3) *Detection*: Analyse security compliance and monitor data from each domain for signs of cyber-attacks or SLA violations. Inform the CDO of any security incidents affecting service delivery.
4) *Response & Recovery*: Ensure security enablers are available, functioning, and resilient. Mitigate attacks and prevent future occurrences throughout the E2E path.

3) T&SM Sub-View Functional Blocks

1) *Security Handler*: This FB communicates bidirectionally with the SHN-FB. It processes SHN-FB requests for customised security features from a specific domain as a stand-alone or combined with other existing services to enhance security. It also provides user security configurations such as Authentication & Authorisation details passing to relevant FBs. It also interacts with other T&SM FBs to track request statuses and relay responses to SHN-FB in SM.
2) *CDO Service-Specific Security Enablers*: Customers can select standard security services from the Domain Advertised Common Functions Catalogue or request non-standard security enablers provided by the CDO. Examples of standard security services include VPN-as-a-Service (VPNaaS) and Content-based Security. It supports two service and asset protection strategies, i.e. Defence in Depth (DiD) [99] and Strength of Control (SoC). These can be requested by CDO and implemented by IDO. These strategies can also be implemented at a domain's ingress points, especially those with lower CDO trust.
3) *User Security Configuration*: This function transmits user security configurations to relevant entities, including user authentication process details, certificate server location, cryptographic algorithm suite, and key sizes. The configurations are flexible, accommodating options such as RADIUS for authentication or EAP-TLS for encryption key agreement. It is essential to consider user equipment capability, which may be limited by technology or domain requirements. User Identification, Authentication, Authorisation, and Accounting (IAAA) can be centrally performed under the control of the CDO. Some 5G projects (e.g., 5GZORRO [54]) have adopted decentralised architectures for identity management. Authentication of users occurs at the network level between users and their connected domain, with Content Service Providers authenticating users at the application layer.
4) *Trust Management*: The CDO must assess the reliability of each administrative domain offering services or resources before peering. This involves various trust-related functions such as trust reputation calculation and component certification. Trust computation is necessary to evaluate the level of trust among entities. The CDO requires a method to perform trust computations for each administrative domain, whereas the IDO may perform this task for the networks and components within its administrative domain. This involves gathering information, performing the trust computation, storing and disseminating trust levels, and updating trust levels for entities.
5) *CDO Asset Protection*: The CDO requires distributed protection functions for its physical and software assets. Security enablers should be embedded in the CDO based on a threat assessment to protect the assets. Additionally, CDOs and IDOs should authenticate each other to protect data in transit and at rest, as well as secure service endpoints against unauthorised access.

4) Security Aspects Delegated to the IDOs

The CDO T&SM is responsible for ensuring compliance with E2E service security criteria, relying on the IDO of each administrative domain to deploy, monitor, and manage the relevant security enablers. Therefore, the IDO must perform the following activities [10]:

1) *Identify the assets* to be protected and the security risks they face.
2) *Reduce security risks* by deploying appropriate security enablers as countermeasures to protect its assets.
3) *Monitor and detect* any signs of an ongoing attack on the assets, services, and network infrastructure by conducting security log analysis, anomaly and intrusion/threat detection, network scanning/probing, etc.
4) *Respond* to the attack with appropriate mitigating actions, focusing on containing the threats and limiting the impact on the functioning of the assets and delivering services.
5) *Recover* from the attack and learn lessons; informing the CDO of any ongoing issues affecting the security of its currently active services.

F. INTERNAL AND EXTERNAL COMMUNICATION OF CDO

1) Interactions between Functional Blocks within CDO

Setting up and coordinating provisioned and on-the-fly service offerings within a single service provisioning cycle ensures that the CDO's services are efficient, compliant, and responsive to the customers' needs. Figure 10 summarises and highlights the internal collaborative workflow among the CDO's Functional Blocks during the service setup and coordination phases. This coordination ensures services are deployed efficiently, securely, and in line with customer needs and multi-domain network policies. Significant interaction exists throughout the life cycle between the different Functional Blocks within the CDO. These blocks work together seamlessly, adjusting their interactions based on the specific service requests from CDO customers. Each CDO Functional Block has a specialised role, but its functions are closely interconnected, requiring smooth coordination and communication throughout the CDO communication fabric.

In the following subsections, we provide a brief overview of the details of each phase of the interactions, highlighting how these Functional Blocks collaborate to deliver end-to-end (E2E) services to customers.

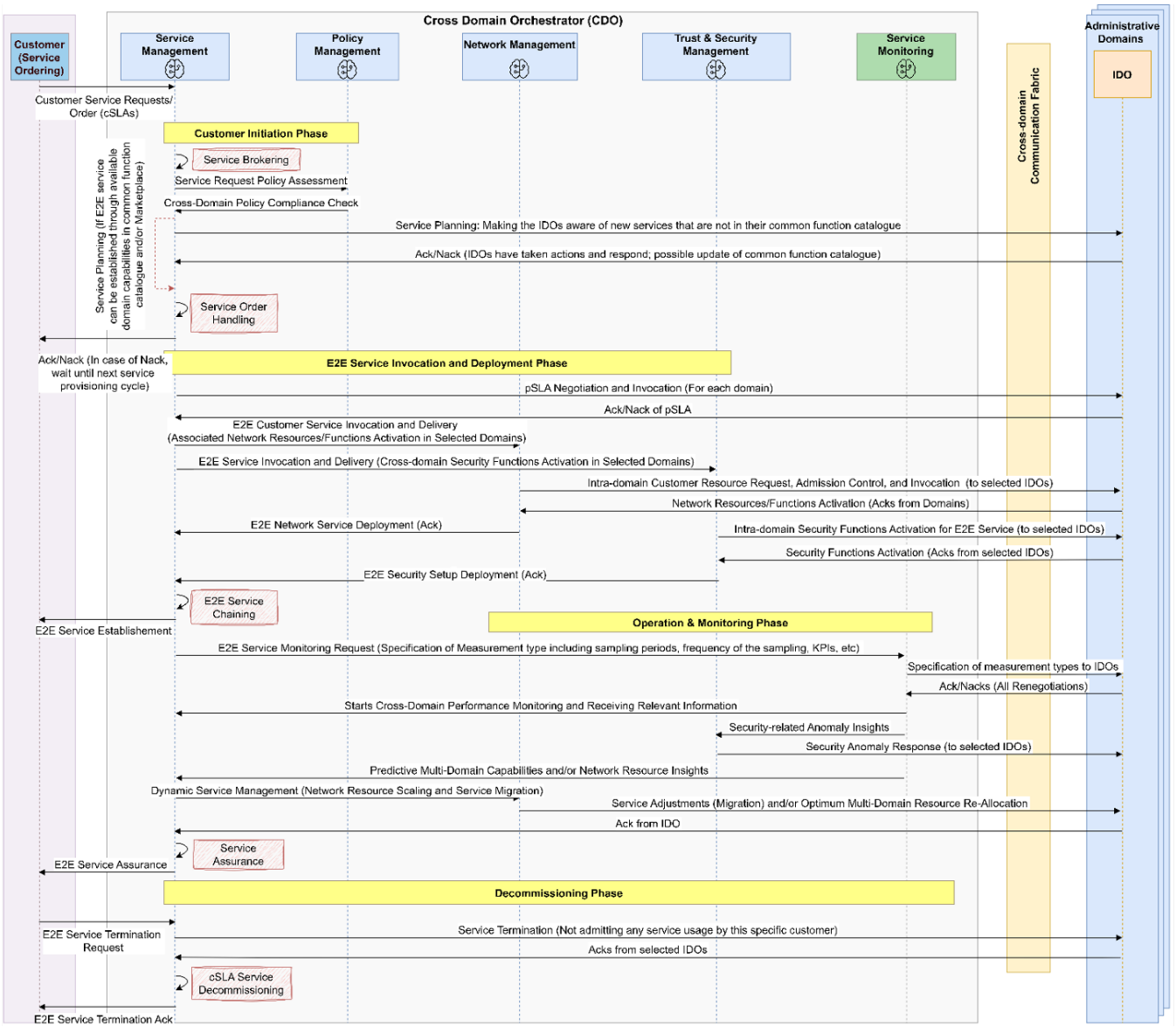


FIGURE 10. **Mapping workflow dynamics and interactions among CDO's Functional Blocks and between Customer, CDO and IDO per SPC phase.**

1) *Customer Initiation Phase*: The initial SPC allows the CDO to coordinate with IDOs for service planning and resource allocation. Customers are informed of service provision decisions, after which they can request services from the CDO. Requests are validated for feasibility and policy compliance.
2) *E2E Service Invocation and Deployment Phase*: The E2E service invocation and deployment phase involves deploying planned services. Upon an SPC initialisation, pSLA negotiations and invocations are carried out for each domain. Then, each chained IDO activates the necessary network resources/functions and security components in the selected domains. Once all components are in place, they are integrated and chained across domains to form a cohesive E2E service. These are the CDO services that a customer can select and order from the Marketplace. Customers may use these services or request specialised ones.
3) *Operation and Monitoring Phase*: Continuous service monitoring is crucial for maintaining service quality and efficiency. The CDO makes a domain-level service monitoring request for IDOs' service monitoring. Continuous monitoring is conducted to ensure the service operates within the defined scope and specified parameters. CDO's Service Monitoring (SMon) FBs compile and aggregate the IDO's monitoring information to achieve E2E service monitoring.
4) *Decommissioning Phase*: As services are no longer needed, the CDO must ensure an efficient process for releasing resources that are put in place. When a customer requests service termination or cSLA time expires, the process should involve controlled termination and noti-

fication to the customer that they no longer have access to the service.

2) Interactions between CDO Manager and AI/ML Provider

The CDO manager can enhance the operation of the various Functional Blocks within sub-views by incorporating trained AI/ML models through an existing contractual agreement with an external AI/ML provider. Alternatively, CDO may have its own internal AI/ML supplier. The CDO AI/ML Manager (CAM), part of the CDO manager, handles such interaction, which is described in the next section (Sec. VII). Various AI/ML models required to support Functional Blocks are detailed in the next section and depicted in Figure 12.

3) Interconnection between the CDO and IDO

The CDO Communication Fabric establishes a secure E2E connection between IDOs and CDO. At the system level, the topology is hub-and-spoke, where the CDO, being the hub, manages multiple connections, each terminating at an IDO. Each IDO is attached to the southbound interface of a dedicated communication fabric instance, allowing for isolation, scalability, and multi-tenancy. Once established, the CDO Functional Blocks run all control loops through the fabric, as depicted in Figure 5.

G. SERVICE & AI/ML MONITORING (SMON-SV)

The SMon-SV performs several activities: 1) It receives domain-level service monitoring information from IDOs and aggregates them to make sure the E2E service delivery is compliant with agreed SLAs; 2) It keeps track of various CDO FBs logs, Runtime Data Collection & Aggregation FBs; 3) It organises collection of AI/ML related data generated during runtime operations; 4) It ensures runtime AI/ML Verification and Assurance of the AI/Ml models employed by CDO via interaction with AIO. The Repository acts as a local storage and provider of monitoring data to other FBs and AIO. We encourage the reader to refer to this paper [100], which covers the architectural principles we follow in in-service monitoring.

VII. AI/ML & COGNITIVE VIEW

We envision the FON to be AI-Native, i.e., its various Functional Blocks will be capable of leveraging AI/ML & cognitive support to accelerate and optimise O&M operations. The term cognitive will be used because cognitive entities operating within a network exhibit some form of intelligence. This may be because they incorporate human intervention and decision-making or AI.

The Functional Blocks contained within the Functional Architecture View are described in Section VI, which covers their roles and responsibilities, as well as how they interact to achieve cross-domain orchestration. AI/ML and cognitive functions will support these Functional Blocks. Since the relationship between the Functional Blocks and their respective AI/ML & cognitive support functions can be one-to-many, presenting these support functions superimposed on the FA-SV is challenging. We leverage the multi-view approach to address this challenge by instantiating the AI/ML & Cognitive View. This view establishes a connection between the Functional Architecture View and various cognitive functions at the level of the Functional Blocks.

A. END-TO-END COGNITIVE ORCHESTRATION FRAMEWORK

The E2E Cognitive & AI framework provides three services which attend to the AI/ML models participating in CDO orchestration: AI Orchestration, Cognition, and Runtime Monitoring. In outline, the AIO automatically manages the AI model lifecycle. Cognition performs a high-level consultative and analytical role regarding AI models and Runtime Monitoring, processing data related to the models. We will refer to the functions supplied by these three services and the AI/ML models themselves as Cognitive Functions (CF). The **Cognitive Functions** will be executed collaboratively to support E2E service offering and CDO internal operations. For the subsequent discussion, we assume that the CDO operates at level 2 autonomy at most (see Sec. VI-A). We recognise that there is a need for further research to explore procedures for establishing the harmonised operation of Cognitive Functions at level 3 autonomy.

The **CDO AI/ML Manager** (CAM) is an entity within the CDO AI/ML & Cognitive View responsible for overseeing the AI/ML orchestration within the CDO's boundary as discussed in the Functional Architecture View (Section VI-A), CAM is responsible for a subset of the CDO Manager's functionality, its role being to acquire cognitive support for the various CDO Functional Blocks. Once CAM has compiled the requirements for a specific instance of cognitive support, it consults the Cognition service to determine which AI/ML models are required and how those models can be rendered trustworthy at both design time and runtime.

We assume the AIO is managed by a third-party provider with a repository of varied machine-learning models populated by entities beyond the CDO's administrative boundary. The AIO provides an interface through which the CDO requests Cognitive Functions. Requests may include attributes such as model description, runtime constraints, and resource availability. In response, the AIO returns an ML pipeline to automate the deployment process, accompanied by placement suggestions. The CDO leverages the acknowledgement from the AIO to either deploy the pipeline for its internal operation or convey it to the participating domains through Service Ordering and Invocation (Sec. VI-B2). The **CDO AI/ML Agent** (CAA) is an entity within the CDO AI/ML & Cognitive View that operates in conjunction with CAM to facilitate interfacing with AIO by acting as a proxy and as a security measure, primarily to isolate the CAM from external communication risks. Once pipelines are deployed, the Service and AI/ML Monitoring function monitors their runtime performance. Together with input from the Cognition service, it assists CAM in determining whether the models

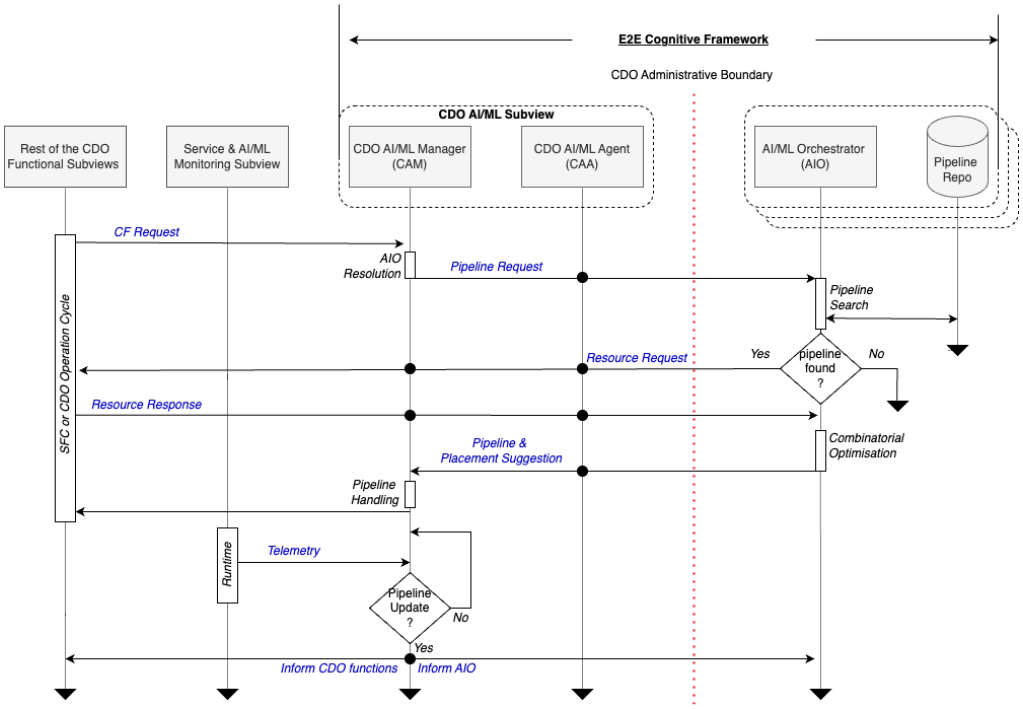


FIGURE 11. E2E Cognitive Framework & CDO-AIO interfacing.

require tuning or retirement based on telemetry data, such as accuracy and resource consumption. Figure 11 illustrates a schematic diagram of the E2E Cognitive & AI Framework spanning the CDO's administrative boundary. It describes the lifecycle of the CFs through the design and runtime phases, as explained below.

The **design phase** is initiated with a Cognitive Function request sent from the CDO Manager to the CAM concerning a CDO Functional Block that participates in an SPC or CDO internal operation. CAM selects a suitable AI/ML provider that has previously registered with the CDO. CAM requests a pipeline to the AI/ML provider via CAA. AIO starts processing the pipeline request by searching its pipeline repository. If a corresponding pipeline exists, the AIO requests an updated resource profile that lists the specific needs of the particular AI/ML model placement. This request is sent to one of the relevant CDO Functional Blocks via CAA and CAM. If a pipeline doesn't exist in the repository, the AIO responds with an NAK, which may trigger the CAM to look for alternative AIO options. If the AIO receives a resource profile, it begins a Combinatorial Optimisation process, as described elsewhere in this article [101], which leads to the return of a pipeline accompanied by placement suggestions. CAM receives this response from AIO and begins a pipeline handling process, communicating with the relevant CDO Functional Blocks to deploy the pipeline.

During the **runtime phase**, the Service AI/ML Monitoring functions continuously monitor the performance of the deployed pipelines, passing on information to the CDO manager and CAM to enable decisions to be made about the pipeline lifecycle (e.g. deciding to retire a model if its accuracy falls below a provided threshold).

B. COGNITIVE FUNCTIONS

Figure 12 presents a snapshot of the AI/ML & Cognitive View and how it relates to the Functional Architecture View. The following sections detail the AI/ML & Cognitive architectural Sub-Views and their reference set of FBs.

The Cognitive & AI/ML View is organised into sub-views, corresponding to a Functional Architecture Sub-View (i.e. SM, NM, and TS&M), as discussed in Sec. VI. Furthermore, each Cognitive & AI/ML Sub-View specifies Cognitive Functions, which support the Functional Blocks within the corresponding Functional Architecture Sub-View. Due to limited space, we have only included a number of these required AI/ML and Cognitive Functions. The Policy Management Sub-View differs from the other Sub-Views because the industry may not yet be ready to rely on AI for tasks like policy management [102], [103]. It should be noted that at the time of writing this paper, due to limited space, we cannot include all of the possible Cognitive and AI/ML supporting functions that could be utilised as intelligent functions within the CDO. Therefore, the set of Cognitive Functions given in this AI/ML View is not exhaustive.

1) Service Management related Cognitive Functions

This section discusses the Cognitive Functions that we found relevant for assisting the various Functional Blocks within the Service Management Sub-View. These applicable supporting Cognitive & AI/ML functions are summarised in Table 10.

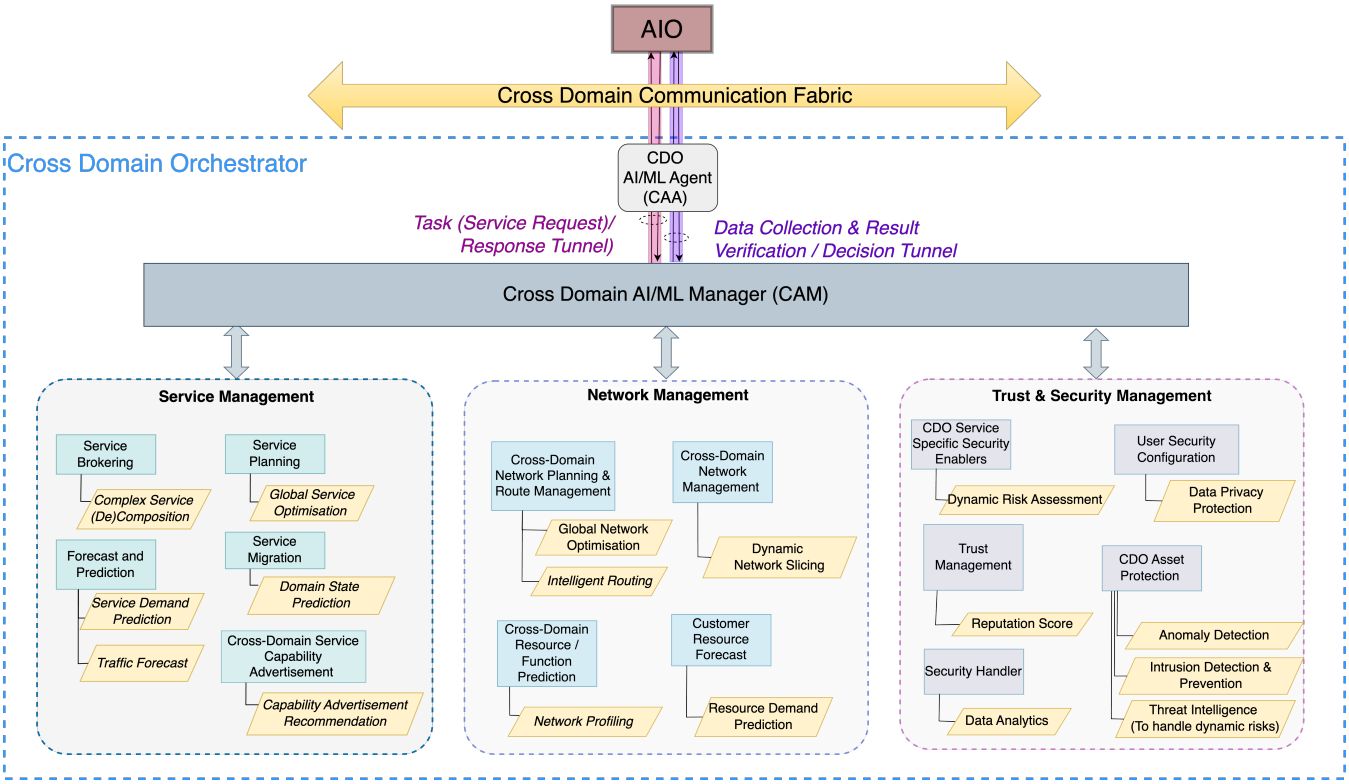


FIGURE 12. Snapshot of AI/ML & Cognitive View.

TABLE 10. Cognitive & AI/ML Functions relevant to Service Management.

Cognitive Functions	Applicable ML Models	Ref.
Complex Task (De)composition	Deep Q-Network (DQN) for reinforcement learning (RL)	[104], [105]
Service Demand Prediction	Recurrent Neural Network (RNN) with Long Short-term Memory (LSTM); Multi-objective RL using Q-learning	[11], [77]
Domain State Prediction	DQN/LSTM	[73], [106], [107]
Advertisement Recommendation	Transformer, Graph Convolutional Network (GCN)	[108]
Service Profiling	Multi-objective RL using Q-learning	[77], [109], [110]

The **Complex Task (De)composition** function assists the Service Brokering Functional Block (Sec. VI-B3) in decomposing a Complex Task into its constituent Elementary Tasks through a graph structure. DeepBroker [105], a cloud brokering application which performs a related task, assigns virtual instances of cloud services to cloud applications through a Deep Q-Learning model. Input states incorporate both a new user request and currently leased Virtual Machine (VM) instances. The actions output by the reinforcement learning (RL) model guide the selection of specific instances of VM types (idle or new) whose capacity can satisfy the resources needed to process the new request. It uses a reward function based on network latency and cost.

Service Demand Prediction supports the Service Forecast and Prediction Functional Block (Sec. VI-B4) by providing a forecast of service demands. It utilises historical cSLA and pSLA issuance data to give an estimate of the anticipated service demand. Service demand prediction can initiate resource and traffic forecasting. Although we have not found an exact match for AI/ML-based service demand prediction in the literature, a relevant work by Vasilakos *et al.* [77] proposes an RL-based VNF profiler to optimise resource allocation.

Domain State Prediction assists the Service Migration Functional Block (Sec. VI-B6) by providing predictive statistics describing underlying domain states based on their historical usage and reliability data. These statistics enable hosts to be chosen proactively when migrating services. To achieve such capability, a predictive model can leverage historical service monitoring data, cross-domain topology from Network Planning and Chaining (Sec. VI-D1) and advertised capabilities from the Common Function Catalogue (Sec. VI-B7) to compute new service routes for migration and inform the Service Order Handling (sec VI-B2). AI/ML models have been developed to select a target host for migration, with Toumi *et al.* [106] reporting that the use of Deep Q-Networks (DQNs) in conjunction with Long Short-term Memory (LSTM) layers is a common approach.

TABLE 11. Cognitive & AI/ML Function relevant to Network Management.

Cognitive Functions	Applicable ML Models	Ref.
Global Network Optimisation	Residual Network (ResNet), Deep RL	[111]
Intelligent Routing	RL using Q-learning; Deep RL	[112], [113]
Resource/traffic Demand Prediction	RNN (LSTM), Federated Learning; Spatio-Temporal Neural Networks with LSTM and multi-layer perceptron (MLP); Gated Recurrent Unit (GRU), basic RNN, CNN	[114]–[117]
Dynamic Network Slicing	Deep RL	[118], [119]
Network Profiling	RL using Q-learning; Q-learning via State–action–reward–state–action (SARSA)	[120], [121]

Advertisement Recommendation assists the Cross-Domain Service Capability Advertisement Functional Block (Sec. VI-B7) by providing Customer-specific recommendations for capabilities (i.e. Complex Tasks) based on their historical behaviour or class they belong to. The objective is to leverage such recommendations to maximise the impact of the advertisements, where significant factors are performance, cost, service level, and reliability.

Global Service Optimisation can assist the Service Planning Functional Block (Sec. VI-B5) in preparing a brokering plan with proactive service provisioning. ML models can be trained with anticipated services from the Service Forecast Functional Block (Sec. VI-B4), and with multi-domain network topology properties from the Cross-Domain Network Planning & Route Management (Sec. VI-D1) Functional Block, to prepare a brokering plan in advance. To our knowledge, the literature does not provide any material that exactly matches this case.

Service profiling is part of the Service Planning & Chaining Functional Block. The profiler accommodates multiple resource types and KPIs and tries to converge towards optimised resource configurations efficiently. It also leverages online learning ML techniques to effectively adapt to the dynamics of open networks (Vasilakos *et al.* [77]).

2) Network Management related Cognitive Functions

This section discusses the Cognitive Functions supporting the various Functional Blocks within the Network Management Sub-View, summarised in Table 11.

Global Network Optimisation supports the planning side of the Cross-Domain Network Management FB (Sec. VI-D1) by using the network topology and state as inputs to generate a Network Policy Set. Yin *et al.* [111] propose a game-theoretic approach that relates node layout and topology planning challenges in network planning to chess game problems. They recommend treating network coverage and connectivity as key factors when developing evaluation criteria in network planning. Their methodology employs a Combined Monte Carlo Tree Search and self-play to generate sample data for network planning. The data is used for training the ML model within a reinforcement learning scheme. The core ML model architecture comprises a residual convolutional neural network (CNN) backbone. This first stage of the network then branches into two separate second-stage networks: i) a planning strategy (policy) network, which outputs actions to modify an input network configuration, and ii) a value network, which outputs an evaluation score for the same input network configuration.

Intelligent Routing assists the routing side of the Cross-Domain Network Planning and Route Management (VI-D1) in determining the paths for requests and data across administrative domain boundaries. It takes an Input Network State Graph and produces a set of routes (including the path and next hop) for each destination prefix or Autonomous System (AS). Hsu *et al.* [113] propose the Energy-efficient Event-driven Deep Reinforcement Learning (EEDRL)-Dijkstra method that combines deep reinforcement learning with an enhanced Dijkstra algorithm to optimise energy consumption and adapt to routing requests while meeting delay constraints. This centralised approach significantly reduces overhead compared to distributed systems and has outperformed traditional routing methods, highlighting its potential for sustainable network operations in future 6G systems.

Resource/Traffic Demand Prediction supports the Customer Resource Forecast (Sec VI-D4) by estimating user traffic volume at specific network points over time. AI and ML techniques, including RNNs, LSTMs, and Transformers, are fit for this purpose, along with classical forecasting methods. A model receives a time series of traffic profiles as input and outputs the predicted traffic load. Nan *et al.* [114] present a supervised federated learning approach using LSTMs to predict mobile network traffic, utilising historical call data to forecast future call characteristics.

Dynamic Network Slicing assists the Cross-Domain Network Management Functional Block (Sec. VI-D3) by proactively provisioning compute and communication resources in advance to support Service Function Chain (SFC) migration. The function takes network monitoring information as input and estimates anticipatory network capacity and required resources. Deep Reinforcement Learning (DRL) and Bayesian models are well-suited for this purpose. Addad *et al.* [118] propose a DRL-based model to predict Service Function Chain migration and bandwidth allocation.

Network Profiling supports the Cross-Domain Function Prediction & Chaining Functional Block (Sec. VI-D2), which optimizes the allocation of network resources. ML models predict the network resources and functions that may be needed. These predictions enable the provisioning and allocation of available network resources and functions as needed. Reinforcement learning approaches have proven effective in this area. ML models might take a time series of network states and a resource matrix (including available and utilised resources) as input. They might then output a list of functions,

TABLE 12. Cognitive & AI/ML Functions relevant to Trust and Security Management.

Cognitive Functions	Applicable ML Models	Ref.
Data Analytics	Hidden Markov Model	[122]
Dynamic Risk Assessment	Graph Neural Network (GNN)/RL, recurrent GNN, Federated learning, RNN/LSTM; Hidden Markov Model	[122], [123]
Data Privacy Protection	Federated learning (via homomorphic encryption)	[124], [125]
Reputation Score	K-means, Random Forest; Fuzzy C-means, Support vector machine (SVM), k-nearest neighbors (KNN); RL using Q-learning	[126]–[131]
Anomaly Detection	LSTM, other ANNs, SVM	[132]
Intrusion Detection and Prevention	ANN and Random Forest classifiers; Logistic Regression, Decision Tree, K-Means; CNN/Federated Learning	[133]–[136]

their probability of invocation, and a forecast for resource consumption. RL with Q-Learning can also be used to select a handover domain. Souza *et al.* [120] propose a Reinforcement Learning-based approach, using Q-Learning, for a smart inter-domain handover of moving devices. The model is supplied with a tuple that includes the position of a user's device at time t, the position of the same device at time $t + 1$, and the name (i.e. identifier) of the domain to which the device is connected at time t. It returns the domain name to which the user's device should connect at time $t+1$ as output. Increasing the time a moving device is connected to the same domain has a positive impact on the reward. Conversely, switching from one domain to another tends to reduce the reward.

3) Trust & Security Management Related Cognitive Functions

This section describes the Cognitive Functions we found relevant for supporting the Functional Blocks within the T&SM Sub-view. They are summarised in Table 12.

Data Analytics can improve the Security Handler Functional Block by managing network failures and incidents. By monitoring data at consecutive time intervals, anomalies can be detected, allowing for the identification of both non-malicious failures and malicious attacks, such as Distributed Denial-of-Service (DDoS) attacks. Incident classifiers can be developed by training models on event logs, formatted as text, and applying clustering techniques to categorise incidents. Various algorithms can be utilised here, including supervised (Decision Trees, Random Forest), unsupervised (K-Means), semi-supervised (Univariate Gaussian), and Hidden Markov Models (HMM).

Dynamic Risk Assessment (DRA) can support the CDO Service Specific Security Enablers Functional Block in protecting CDO functions and networks from dynamic external threats. Open network connectivity and ML both change the game entirely. The challenge is to maintain operation in the face of imminent and potentially catastrophic security threats, including 1) unknown threats and vulnerabilities; 2) the evolution of known threats; 3) new threats or zero-day vulnerabilities; and 4) changes in assets, mainly addition, modification or removal of assets. Static Risk Assessment assumes that the system is built to a specification and that epochs for assessing and revisiting the risks are long (e.g. months). In Dynamic Risk Assessment, the epochs of re-assessment must be much shorter than those of the traditional systems. It requires continuously monitoring and assessing the operational state and deploying a 'Mitigation Plan' in near real-time with 'Justifiable Confidence' of 'Good Outcome' in the face of any likely imminent threats. By enhancing the capability of intrusion detection systems, they can monitor network infrastructures to identify malicious attacks and possibly trace the footprints of unknown threats. In [137], a security risk assessment methodology (SecRAM) is developed for systematic application to an emerging network architecture to identify run-time threats, assess the impact and likelihood of the occurrence of attacks relevant to the threats, evaluate the architectural design principles; and validate the built-in security enablers and mitigation actions that are devised to combat such attacks. ML-based defence systems facilitate automated monitoring of network elements. The intended model can utilize input from a system architecture that describes the high-level design as a weighted graph, where the nodes represent modules and the edges indicate the degree of coupling between these modules. This approach helps identify a set of nodes with varying degrees of vulnerability. Deep Neural Networks (for classification), Bayesian models, fuzzy systems, and Graph Neural Network (GNN) models are well-suited for addressing such challenges. Although we did not find specific literature relevant to DRA while writing this paper, Ramezanpour *et al.* [123] provide foundational research directions for AI-driven security in next-generation networks. Hu et al. [122] propose a two-stage network security risk assessment framework that utilises an improved Hidden Markov Model (IHMM), which identifies risks based on operations, vulnerabilities, and threats, thereby providing timely insights into security vulnerabilities.

Data Privacy Protection enhances the Authentication and Authorisation (AA) capability of the User Security Configuration Functional Block. Machine Learning (ML) models can create data encryption strategies, such as ISAKMP policies, to enhance security and address privacy concerns. For instance, techniques such as a Convolutional Neural Network (CNN) utilising homomorphic encryption can detect attacks through Federated Learning. This approach helps protect privacy by using the type of communication task to determine the optimal ISAKMP policy. While researching, we found no similar work in the literature; however, Fakhouri *et al.* [124] provides a thorough overview of the role of ML in 5G security.

Reputation Score supports the Trust Management Functional Block by assigning reputation or trust scores, or a trustworthiness category, to input data. For example, a score which reflects a level of trust might be assigned to a time series

of compliance values from service requests and responses between peers. Given that this time series may be volatile, establishing trustworthiness is crucial. CDO can assign trust scores or labels to other domains using ML classifier models. If a domain is deemed untrustworthy, its communication may be rejected. In consensus-driven scenarios, reducing the influence of untrustworthy domains can be beneficial. ML models, such as random forests and reinforcement learning, can assess trustworthiness. A trained classifier can analyse compliance values and classify trustworthiness based on the reputation score. Sagar et al. [126] propose unsupervised and supervised learning methods for assessing the trustworthiness of IoT devices. After applying K-means clustering, random forests categorise trust levels as trustworthy, neutral, or untrustworthy.

Functions to support the CDO Asset Protection Functional Block include: 1) Anomaly Detection, 2) Intrusion Detection and Prevention, and 3) Threat Intelligence (they apply to IDO operations as well). Further details now follow.

Anomaly Detection is used to classify a data item as an anomaly if it is an outlier concerning what is considered standard data. For example, deep packet inspection (DPI), which is performed at ingress and egress points related to cross-domain orchestration, can be used to detect anomalies caused by intrusions. This is often the job of a firewall. A trained machine learning (ML) model can perform binary classification for anomaly detection, given a traffic stream or packet sequence as input. As a further step, a multi-class classifier can be applied to data identified as anomalous, sub-classifying anomalies into classes such as Eavesdropping, Replay, (Distributed) Denial-of-Service attacks, etc. Cevik *et al.* [132] focus on ML methods for anomaly detection to heighten the security of an avionics system.

Intrusion Detection and Prevention is a function which generally has to process anomalous traffic, with the input comprising a packet sequence. However, in contrast to the previous Anomaly Detection function, classification is intended to lead to a responsive action depending on the level and type of intrusion detected. A pre-emptive approach can leverage trained Machine Learning models to anticipate a compromise in advance by analysing intrusion patterns that indicate the manipulation of firewall rules. Considering the short and efficient operation window required, a low-complexity Decision Tree or Random Forest is recommended over an extensive artificial neural network (ANN). Sarhan *et al.* [133] investigated a Deep Feed Forward Network classifier (relatively small and shallow) and a Random Forest classifier. These binary classifiers assigned an 'attack' or 'benign' label to input data. Saghezchi *et al.* [134] detect Distributed Denial-of-Service (DDoS) attacks using Supervised Learning (Logistic Regression, Decision Tree, Random Forest), Unsupervised Learning (K-Means), and Semi-Supervised Learning (Univariate Gaussian algorithm). Hijazi *et. al.* [135] proposes the detection of attacks using Federated Supervised Learning (with homomorphic encryption) to train a CNN.

Threat Intelligence focuses on the structured collection, analysis, and dissemination of data regarding potential or existing cyber threats. When writing this paper, we found no literature reporting the use of machine learning (ML) models to perform threat analysis in the context of cross-domain orchestration.

4) Cognition & AI/ML Capabilities

The Cognition service capability provides several supporting cognitive functions to the CDO, including designing machine learning (ML) models, reasoning capabilities, verifying ML models, and explaining ML model behaviour. These functions are needed to understand the behaviour and trustworthiness of the AI/ML functions supporting the CDO. This section describes the last two functions that have just been listed.

Verification & Assurance refers to the general process of gaining confidence that a system functions according to its specified requirements. The first step in the verification process is to capture the requirements, which may involve converting high-level, qualitative requirements into low-level, technical ones. These technical requirements are often expressed as quantitative properties of the system. The next step is to verify the system against these requirements using formal verification, testing, or a combination of both. Verification can be undertaken at design time or runtime, and at various system levels, including the system level, subsystem level, and component level. Such multi-level verification will be required for an AI-native 6G network, from the top system-of-systems level down to the level of AI-enabled components. Different AI-specific verification methods will be necessary at each level of implementation. It may also be required to apply multiple AI-specific verification methods to the same AI-enabled network constituent, whether a component or subsystem. In such cases, verification methods may complement or reinforce each other.

On the other hand, an assurance process provides a broader assurance argument for trustworthiness. This involves drawing on various forms of evidence and verification results to construct a safety or security case for assurance purposes.

Explainability & Interpretability are understood as follows. An explainable AI application justifies its output or decision in terms humans can understand [104]. For an AI application to be trustworthy, it must generate accurate and clear explanations. The explanation is aimed at an AI user rather than an AI developer. The purpose is to make the processes behind the decisions or predictions made by the AI more understandable and transparent. Explanations also contribute to verifying the output of an AI component, thereby allowing for greater confidence that the system is behaving correctly according to its requirements. Explainability is also related to uncertainty quantification. An AI application that quantifies the uncertainty of an output provides the user with information they can use to decide how to process the output. In contrast, interpretability is aimed at both developers and regulators, providing greater technical detail about AI models and how they operate.

In summary, explainability and interpretability help the CDO Manager and stakeholders to better understand the reasoning behind the decisions made by cognitive & AI/ML functions during their operation. This greater insight eventually builds trust and reliance on intelligent autonomous control. It also encourages the CDO Manager to progress towards a higher level of autonomy (i.e., levels 3 and 4 as defined in Sec. VI-A).

VIII. MAPPING OF REQUIREMENTS TO FUNCTIONAL ARCHITECTURE

Before we conclude discussion regarding the Functional Architecture (Sec. VI) and Cognitive & AI/ML Views (Sec. VII), and proceed towards the System-Level Architecture View, it is necessary to state how the various Functional Blocks described in those sections fulfil the Cross-Domain Orchestration requirements described in Sec. III-B. Table 13 maps the various requirements, denoted by their requirement IDs, to the corresponding Functional Blocks that fulfil the requirements, along with respective sections in this paper. Our goal in this short section is to provide a relation between the requirements and the various functions that satisfy them, which justifies the CDO design objectives within the REASON project.

TABLE 13. Mapping between Requirements IDs, Functional Blocks and their associated sections.

Req ID	Mapped Functional Block	Sec.
Stakeholder Requirements		
STK-1	Service Order Handling & Subscription	VI-B1
STK-2	Service Ordering & Invocation	VI-B2
General Technical Requirements		
TECH-GEN-1	CDO Internal Message Bus	VI-F1
TECH-GEN-2,3	CDO Communication Fabric	VI-F3
TECH-GEN-4	FBs in Network Management SV	VI-D
TECH-GEN-5	FBs in Policy Management SV	VI-C
TECH-GEN-6	Cross-Domain Network Planning & Route Management	VI-D1
TECH-GEN-7	Enter Functional View	VI
Cognitive Requirements		
TECH-COG-1	Global Network Optimisation	VI-D
TECH-COG-2	Network Management related Cognitive support functions	VII-B2
TECH-COG-3,4	CDO AI/ML Manager (CAM) & AI/ML Agent (CAA)	VII-A
Security Requirements		
TECH-SEC-1,2	FBs in Trust & Security Management SV	VI-E
Measurement Requirements		
MSR-1,2,3	FBs in Service & AI/ML Monitoring SV	VI-D
Policy Requirements		
POL-1	FBs in Policy Management SV	VI-C
POL-2,3	FBs in collaboration with T&SM and PM SV	VI-E,VI-D
Non-Technical Environmental Requirements		
NT-ENV-1	FBs in Policy Management SV	VI-C
Non-Technical Ethical Requirements		
NT-ETH-1	FBs in collaboration with T&SM and PM SV	VI-E,VI-D
NT-ETH-2	Cognition Capabilities in AI/ML View	VII-B4

IX. SYSTEM-LEVEL ARCHITECTURAL VIEW

The System Level Architecture View (SA) aims to describe, from an implementation perspective, the assets and interfaces of various tangible and intangible resources needed for CDO deployment. There should be a mapping between FA Functional Blocks (Sec. VI) and SA assets that can be one-to-one (one FA Functional Block maps to one SA component/asset), one-to-many or many-to-one, depending on the degree of complexity of the functions described in the FA. As the SA covers a considerable part of the CDO architectural framework, we only focus on the Service Management Sub-View in this paper. Thus, this section has three objectives: 1) Provide the detailed interaction and workflows of SA components; 2) Provide a timeline of stakeholder participation in a service delivery chain, using an example scenario to summarise the participation of the relevant stakeholders described in Sec. V-A; and 3) Describe the implementation of a CDO Service Management function for Proof-of-Concept purposes.

A. COMPONENT LEVEL INTERACTION & WORKFLOWS

Figure 13 depicts the reference model of interaction between various SA components to achieve cross-domain orchestration. The CDO interfaces with the IDOs through the CDO Communication Fabric (Sec. VI-F3). The fabric employs a hub-and-spoke model, where the API Gateway on the CDO side serves as the hub and connects each underlying IDO through a Domain Proxy (Dom-Proxy). The role of the Dom-Proxy is to facilitate platform-agnostic communication across the fabric regarding IDO platforms. It implements a platform-dependent Dom-Proxy plugin between the Dom-Proxy and the underlying orchestrator API to provide instruction-level translation and data modelling. The CDO communicates with the AIO through the CDO AI/ML Agent.

Each domain has a defined administrative boundary and contains a pool of computing and communication resources distributed in a set of Edge/Cloud servers. The IDO manages its domain resources through an IDO Communication Fabric.

The Marketplace is a component (it can be a third-party entity) where the CDO publishes the service offering by composing various capabilities advertised by the IDOs. The Marketplace presents such offerings to the Customer as a catalogue.

The reference model distinguishes between three types of operation cycles that involve cognition. The first is a customer-service operation that leverages AIO to facilitate customer-centric AI/ML-based end-to-end services. The second is the lifecycle management of the AI/ML support functions for CDO operations (Cognitive Functions). Finally, the

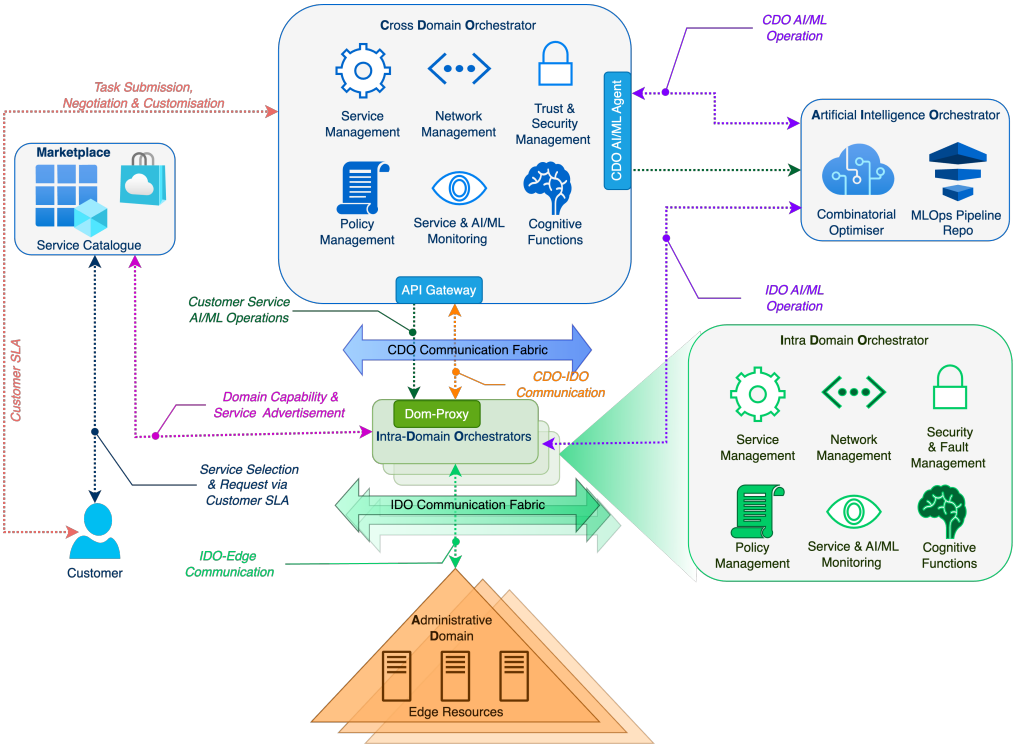


FIGURE 13. **Reference model of interaction between Customer, CDO, IDO and AIO components for realising Cross-Domain Orchestration and E2E service delivery.**

third kind involves IDOs leveraging the Cognitive Functions supplied by the AIO in their internal IDO operations. However, the IDO-AIO interaction falls outside the scope of cross-domain orchestration. Therefore, we omit an explanation of this interaction in this paper, shown in Figure 13.

The Customer can choose a Complex Task (cross-domain) from the marketplace and submit a request to the CDO in the form of a cSLA. The CDO breaks down complex tasks into elementary tasks, maps them to advertised domain capabilities, and initiates the formation of cross-domain E2E service delivery.

The subsequent sections describe various workflows based on this reference model.

1) Domain Registration

Before a domain participates in the cross-domain orchestration, it must register with the CDO if it is in its business interest. The Domain Registration Service (DRS) within the Cross-Domain Trust & Security Management is responsible for conducting the registration procedure in coordination with the Security Policy Repository and Domain Registry. The workflow in Figure 14 depicts the interaction between various components that results in a successful domain registration.

At first, the domain admin (IDO Manager) creates an account with user information at the CDO registry. As the CDO has not authenticated the domain, these initial interactions occur through out-of-band communication through a Web Portal. Next, the IDO Manager initiates a domain registration request (*DOM-REG-REQ*) with a Proof of Identity (POI) through the portal to the domain authentication service (DAS), which triggers a domain registration approval (*REG-APPROVAL*) process for the CDO Manager. Upon successful approval by the CDO Manager, DAS updates the domain registry. It also updates the Security Policy Repository (SPR) with an IDO Access Policy for the registering domain as defined in the Policy Manager. The Domain Enrollment Service (DES) fetches the corresponding Access Policy from SPR, generates IDO Credentials and updates the Domain-Proxy Management Service. The DRS deploys a (Dom-Proxy) service at the IDO that establishes a secure session with the API Gateway on the CDO side. The Dom-Proxy and the API Gateway become the two end-points of the CDO Communication Fabric (CDO Fabric).

When a domain completes registration and gets access to the CDO Fabric, CDO-IDO communication switches to the In-Band mode. In addition to informing the API Gateway about the new session, the Dom-Proxy Manager instantiates a Keepalive service for the IDO. The Keepalive service routinely checks the IDO's health using a two-way Hello protocol over a defined period (t_{hello}). The Dom-Proxy replies with an ACK as it receives a HELLO. If the IDO fails to respond within a defined Teardown Window t_{trd}, the Keepalive service considers the IDO not active. Hence, it updates the Domain Registry and signals the CDO manager to terminate the IDO session.

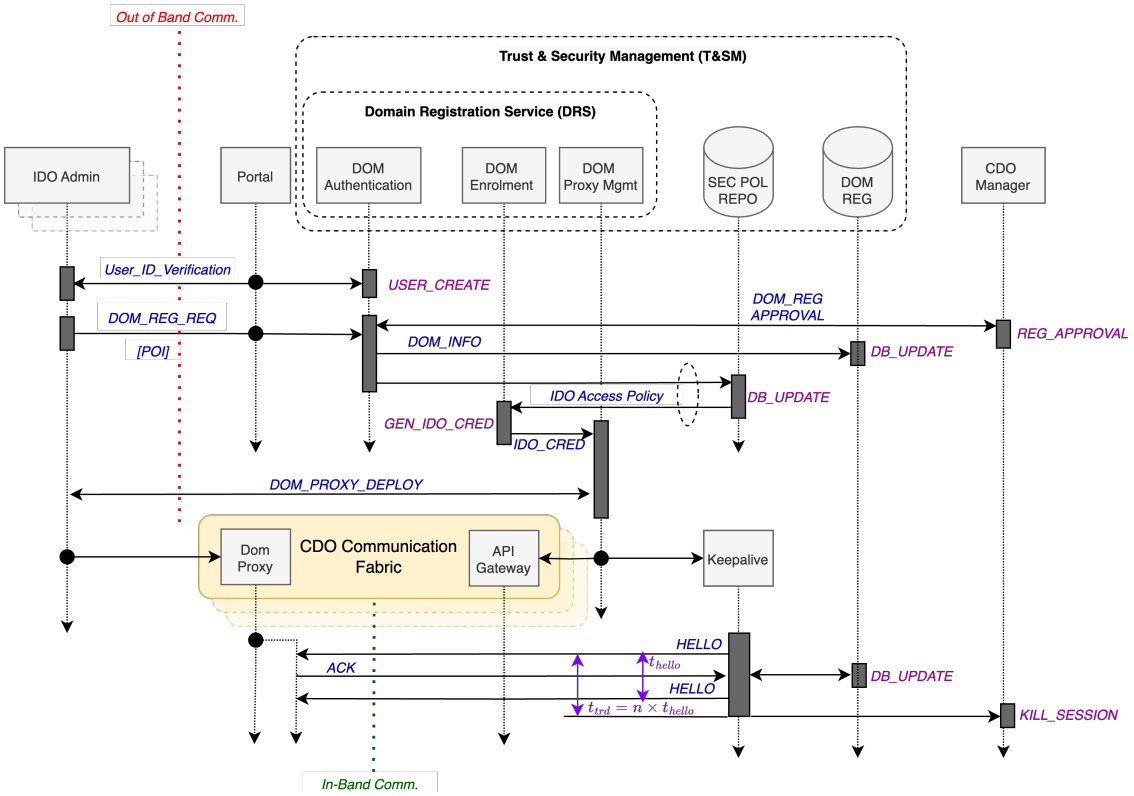


FIGURE 14. Domain Registration workflow.

2) Capability Advertisement

The Capability Discovery phase begins as soon as the CDO Fabric becomes operational. However, the process could be solicited (initiated by the CDO) or unsolicited (initiated by the IDO).

At first, the CDO uses the solicited approach, where the Domain Capability Discovery Service (Sec. VI-B7) initiates a discovery mechanism by polling the Dom-Proxy with a Domain Capability Request (DOM-CAP-REQ). The Dom-Proxy conveys the request to the corresponding IDO function to retrieve the capabilities the corresponding domain wishes to advertise. The capability includes information about various domain-level services and resources (computing and communication).

Dom-Proxy formats the IDO's response (DOM-CAP-RSP) and sends it to the CDO side, where the Domain Capability Discovery Service records it in the Domain Advertised Common Function Catalogue. However, in the case of an alteration of capabilities (i.e., service or resource) at the domain level, the IDO should use unsolicited mechanisms to inform the Dom-Proxy. The Dom-Proxy may also provide this feature by setting a listener at the IDO, which constantly monitors the domain capabilities. In both cases, the Dom-Proxy collects, formats and sends updated capability to the CDO (DOM-CAP-UPD) for further operations. Figure 15 illustrates the capability advertisement workflow.

3) Task Composition

In the context of cross-domain orchestration and Task-Oriented Networking, as discussed above, we define a Complex Task (CT) as a cross-domain end-to-end (E2E) service composed of several Elementary Tasks (ETs) that map onto domain-advertised capabilities. In a simple setup, a CT may be a distributed Service Function Chain (SFC) across domains, with a connection between the functions associated with a set of QoS constraints. However, we use a graph structure to describe a CT more generically, using a nonlinear representation. The graph representation provides a framework for applying various graph-theoretic principles to tackle miscellaneous task decomposition and placement problems.

Figure 16 illustrates a scenario where the IDOs advertise domain capabilities (e.g., Rendering, Encryption, Transcoding, etc.). We consider such capabilities as ET within the Marketplace. A Task Composition process stitches the ETs together to form a CT. The customer's cSLA influences the individual QoS constraints between the ETs. Therefore, an optimal overlay of this graph on top of the multi-domain topology of the participating domains describes the task decomposition. In this case, we advocate for a bottom-up approach where the CDO proactively composes the ETs into CTs, and the Customer chooses from existing CTs. However, the opposite is possible with an on-demand decomposition, though at the cost of high computational requirements.

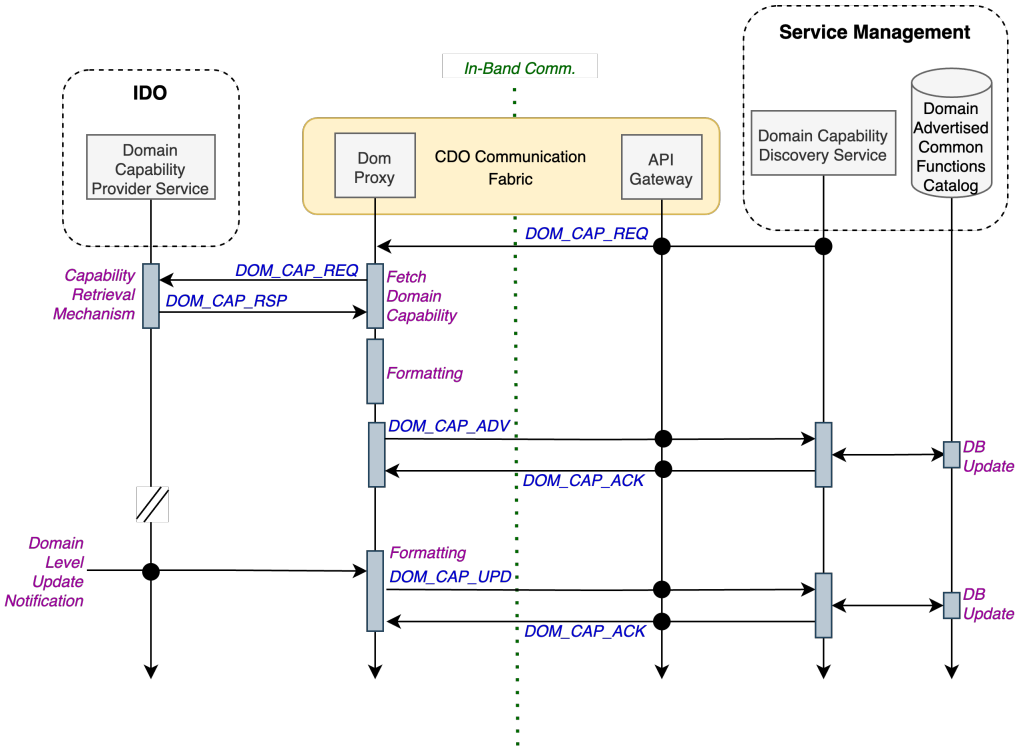


FIGURE 15. Domain Capability Advertisement workflow.

4) Task Negotiation

The Task Negotiation process takes place between the Customer and the CDO. After a Customer selects a Complex Task from the Marketplace, they receive a template of the cSLA Request, which includes a task descriptor. The Customer may customise the description (e.g., specifying boundary conditions) and submit a cSLA Request. The CDO Service Manager performs Brokering and acknowledges the Customer to see if it can meet the SLA constraints as a cSLA Offer. If the cSLA Offer differs from the cSLA Request, the Customer may choose to reject the proceedings, which signals to the CDO not to advance for the Service Invocation phase. In this case, we only consider a binary choice for the Customer; however, a more progressive negotiation mechanism with an associated negotiation protocol may be considered. Figure 17 illustrates the workflow of a binary negotiation procedure.

5) Service Brokering & AI/ML Embedding

After the Customer chooses and submits a Complex Task request, the CDO Service Brokering Function looks up the corresponding Graph definition for the CT. However, incorporating cognitive functions requires an additional step. In this context, we refer to the two-stage process as Brokering and Embedding, where the former breaks down a Complex Task into its Elementary constituents, and the latter embeds an MLOps pipeline within the Graph. The pipeline is sourced from the AIO if the customer requests an AI/ML service.

To achieve the above, the CDO expects the underlying domains to set an "m-flag" (ML Flag) for advertised capabilities that require AI/ML & cognitive support. The CDO also maintains a "D-set" (Domain Set), which refers to the domains that advertise the corresponding capability. It should be noted that only the CDO Manager initiates the request to the AIO for any Cognitive & AI/ML support function needed for CDO operation.

During the Brokering process, the Service Brokering Function within the Service Manager computes the optimal delegation of elementary tasks to the participating domains. It also derives the QoS applied between the Elementary Tasks from the cSLA.

After Brokering, ETs with a set m-flag require AIO support. The Embedding process "embeds" the pipelines supplied by the AIO into the corresponding flagged ETs. The AIO's response also includes placement suggestions for pipeline stages, specifically targeting certain edges.

Figure 18 illustrates the Brokering of a CT into an SFC of three ETs with associated QoS. ET1 and ET3 are advertised exclusively by domains 1 and 2, respectively, and do not require AI/ML & cognitive support. Both domains advertise ET2, which does require AI/ML and cognitive support. After Embedding, ET2 gets split into a three-stage pipeline with a suggested edge-level placement from the AIO. The Service Ordering and Invocation Function uses the above description to negotiate task delegation with participating domains while provisioning an end-to-end (E2E) service.

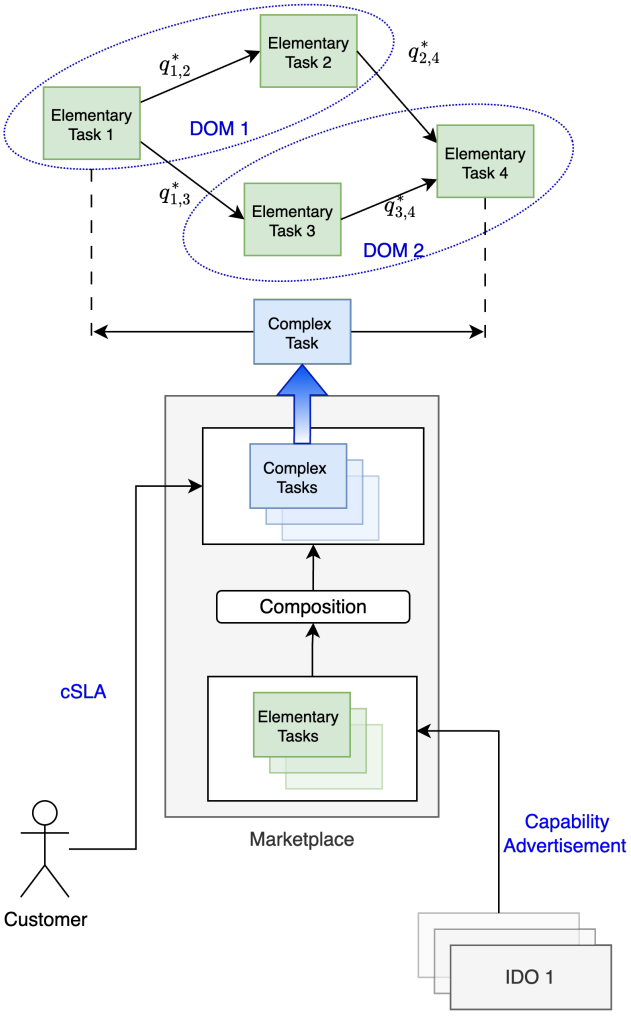


FIGURE 16. Task composition and cross-domain deployment.

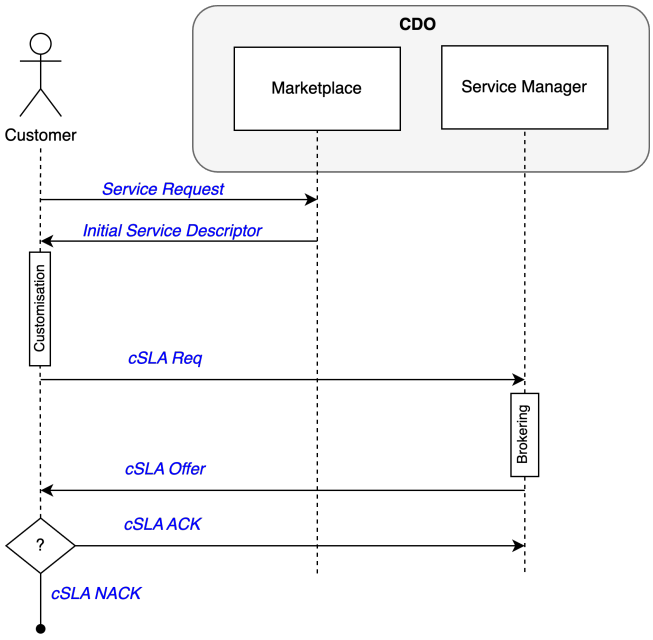


FIGURE 17. Task Negotiation with Binary Customer Choice.

B. STAKEHOLDERS' PARTICIPATION IN E2E SERVICE DELIVERY

Here, we describe the definitive involvement and activities of various stakeholders (as described in Sec. V-A) in the context of end-to-end cross-domain service provisioning and delivery. This section aims to provide a walkthrough of the operations and activities from the stakeholders' perspective in association with the Organisational View. Figure 19 depicts the storyline summarising the interaction between the stakeholders and various components described within the context of the four views in Sec. V to Sec. IX. Throughout the storyline, we shall assume that the CDO instance is operational.

To begin with, the **Domain Administrator** (IDO Admin) of a participating domain initiates the onboarding process, which results in access being gained to the CDO Communication Fabric (Sec. VI-F3) between the CDO and the Domain's IDO. At first, the Domain Admin registers himself with the CDO and provides Proof of Identity to complete User Authentication. Once authenticated, the Domain Registration process begins; CDO and IDO mutually authenticate each other. IDO installs a Domain Proxy, and the CDO establishes a secure one-to-one connection with the CDO (Sec. IX-A1).

The **Content or Service Provider** (C&SP) participates in the process after its target domains are registered. A prerequisite to the Service Onboarding process is that the infrastructure providers (e.g., Network, Edge, and Cloud) must have provisioned all relevant computing and communication resources. Initially, the C&SP registers itself with the domain platform and onboards its services and content. The C&SP may also include a pSLA to define the various QoS levels at which the customers consume the services. When the IDO becomes aware of the service onboarding, synchronisation between CDO and IDO occurs through the Capability Advertisement process (Sec. IX-A2). After that, the Marketplace offered by the Marketplace Provider synchronises with the CDO to update its Service Catalogue with composed services, i.e. the Complex Tasks (Sec. IX-A3).

The **AI/ML Service Provider** is viewed as an external entity loosely coupled to the process, but plays an integral role. As a prerequisite, it must have completed a repository attachment procedure that contains ML pipelines populated by third-party providers. Additionally, it must be registered with the CDO so that the CDO is aware of its existence when seeking to source cognitive services. Nevertheless, in addition to the CDO-AIO interaction (Sec. VII-A), the AI/ML Service Provider enables four crucial services to collaborate through cross-domain orchestration. Namely, the Pipeline Search service to find the most suitable ML Pipeline from the attached repository, the Combinatorial Optimisation & Selection services (FA FBs or Edges) to identify the best server on which to place the pipeline stages and, finally, the

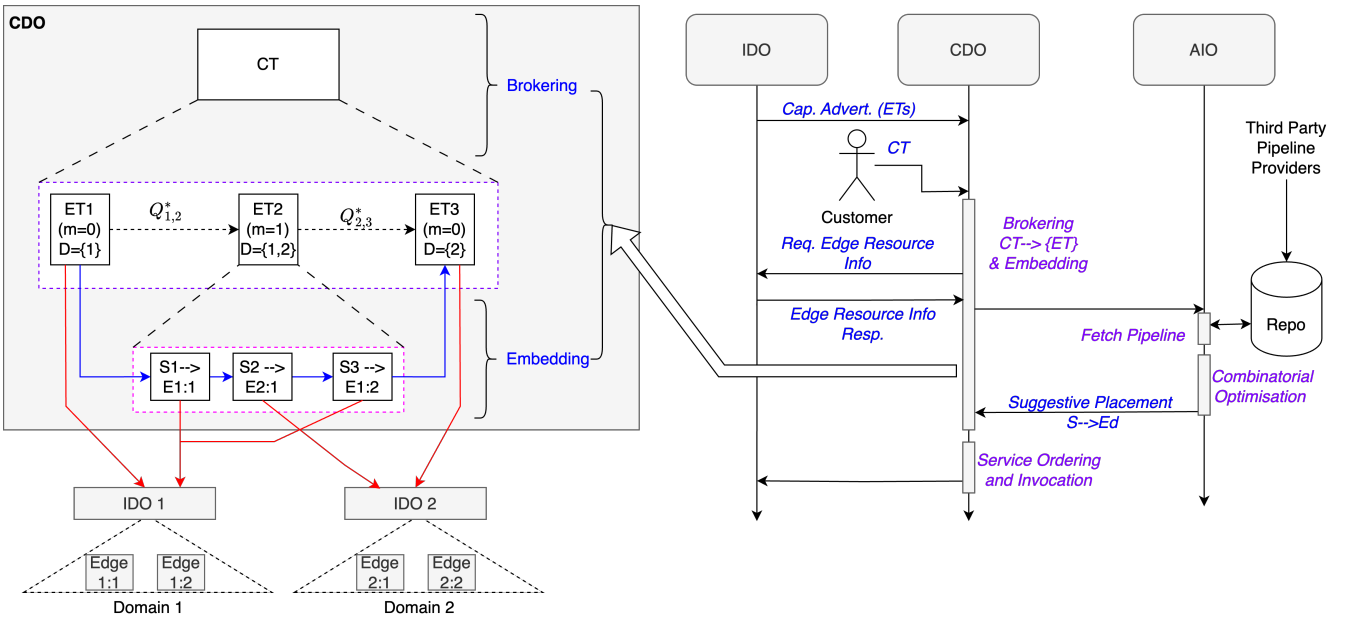


FIGURE 18. Task composition and cross-domain deployment.

Placement Suggestion service, which reports the CDO about the suggested placement.

The **Customer** interfaces through the Marketplace, ideally agnostic to the complex or elementary task definition. Such abstraction promotes user-friendliness and simplicity, eventually contributing to a positive user experience. The Customer selects a Task from the Marketplace catalogue and confirms its deployment after a successful cSLA negotiation (Sec. IX-A4).

Although the **CDO and IDO Managers** are not the orchestration process's primary stakeholders, describing their participation would complete the storyline. After the Customer confirms the selected Task, the CDO Manager involves various CDO functions to conduct the Service Brokering process (Sec. IX-A5), selects optimal network domains to which to delegate Elementary Tasks as per their advertised capabilities and negotiates pSLA with the IDOs to initiate the Service Provisioning Cycle (SPC). The IDO manager handles the operations within its administrative boundary to achieve the desired state. Once the E2E service becomes live for the Customer, the CDO and IDO enter into a closed-loop communication regarding monitoring and validation processes to maintain the stability of the E2E service.

C. SYSTEM-LEVEL ARCHITECTURE: IMPLEMENTATION OF CDO SERVICE MANAGEMENT

This section presents an instance of a CDO implementation interfacing with two IDOs. Although Sec. IX has addressed the entire Service Management Sub-View, the following implementation details are limited to Service Brokering. This section aims to provide a set of physical assets and software tools, along with details of their organisation, that, in combination, can deliver Service Brokering capability. Figure 20 depicts a bottom-up approach to the deployment under discussion. That said, it presents our take as one of the possible ways to implement the Service Brokering function with a specific toolset as a Proof-of-Concept deployment. The modular design of the CDO functions (i.e. views and subviews) allows it to be realised differently, keeping the nature of the service-based architecture intact.

We define administrative domains using a Kubernetes (K8S) [138] cluster of physical nodes containing compute and storage resources. The K8S control plane manages workload scheduling and internal networking across nodes within a cluster. K8S Services, created by HELM charts [139], are Elementary Tasks (ETs) within a domain. We use Istio [140] Service Mesh to provide internal connectivity between the ETs. In this instance, we use Nephio [141] as an IDO, which leverages the underlying K8S control plane to create workloads for the Nodes. The Domain Proxy Plugin translates the generic deployment instructions from the Domain Proxy into the orchestrator-specific description, making the CDO agnostic of the IDO platform. In this deployment, we use two IDOs connected to the CDO using a Dynamic Multipoint VPN (DMVPN [142]) tunnel, which establishes the CDO communication fabric through the Gateway Routers. DMVPN also establishes inter-IDO secure communication using a temporary IPSec tunnel [143] [144]. The life of the DMVPN tunnel is the same as that of the provisioned E2E service.

In CDO, the API Gateway is the northbound termination point of the CDO communication fabric. Various databases implemented using Postgres [145] help segregate various deployment-related information (e.g., TaskDB holds

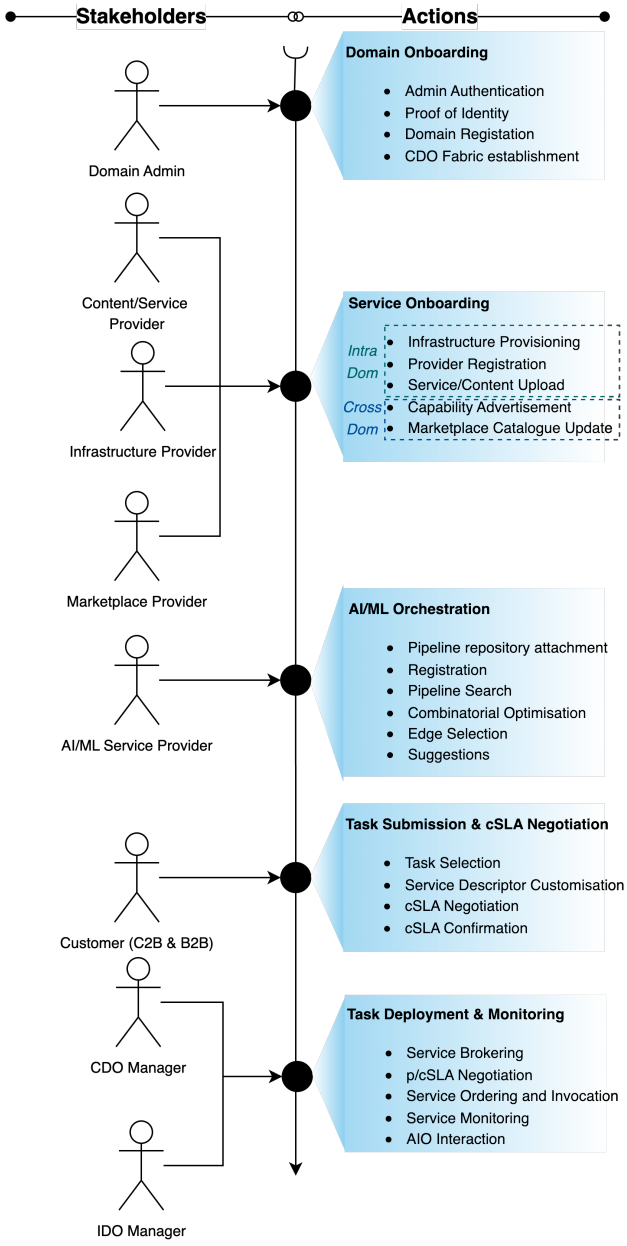


FIGURE 19. Storyline of stakeholders' participation in Cross-Domain Orchestration for E2E service delivery.

CT Composition, Capability DB stores domain-advertised capabilities, Domain Registry holds details of registered domains, and Deployment DB holds data for a running deployment). We use OAuth [146] for token-based authentication and key management. Graphana [147] visualises monitoring data stored in the InfluxDB [148] based Time Series DB. The Service Broker and other API endpoints in the CDO use FAST-API [149] for API exposure. We use the NetworkX [150] library to solve various graph computation problems for service brokering (e.g., linearising a graph representing CT into a sequence of ETs, preserving its call sequence using Topological Sorting).

Finally, the user interaction occurs at the Portal (web GUI),

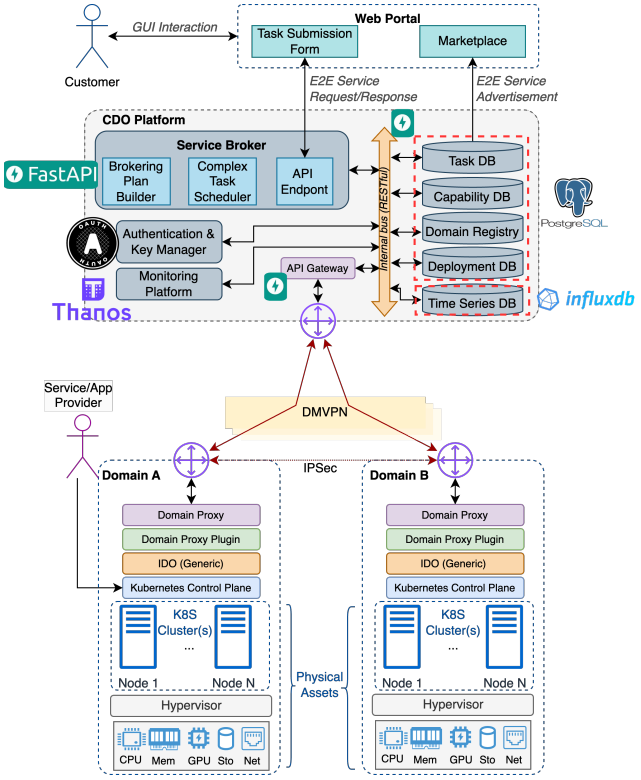


FIGURE 20. System-level architecture view - showing an instance of CDO with two underlying IDOs performing a Service Brokering function.

a client-side web application.

X. CONCLUSION & FUTURE SCOPE

This paper proposed a Cross-Domain Orchestration (CDO) multi-view architectural framework conceived within the context of the REASON project, which is intended to serve the Future Open Network. The proposed quad-view CDO architecture includes four distinct, well-defined views (Organisational, Functional, Cognitive & AI/ML and System-level). The relationship between the views and the correspondence between elements contained in different views are captured herein.

We surveyed recent EC projects beyond 5G and 6G, identifying the attribute gaps in state-of-the-art cross-domain orchestration and management. On this basis, we established CDO requirements which specify the elements of the multi-view CDO architecture. This cross-domain orchestration is designed to extend the geographical scope of an individual network domain by providing complex end-to-end services across multiple heterogeneous network domains. We identified AI/ML models that can provide cognitive support for CDO functions, thus extending network automation and promoting the optimisation of orchestration and network operation. We documented System-level CDO workflows, supported by Cognitive & AI/ML elements, which enable end-to-end service delivery. We described the nature of stakeholder participation, which allows the provision of such complex services across multiple domains. For proof of concept, the

System-level architecture is partially realised by implementing an instance of a Service Management function.

Some of the prominent challenges we observed with the emergence of cross-domain AI-native orchestration are the lack of standardisation in the SLA structure and negotiation protocols, which hinder interoperability across multiple administrative boundaries. Another challenge that concerns AI-Native networking is the standardisation of distributed intelligence and its adaptation to cross-domain telecom architecture. In summary, "A BGP Moment" but for a collaborative AI-Native SFC placement scenario. Finally, we envision the emergence of business models that enable ISPs, MNOs, and data centre providers to rent a proportion of their infrastructure to CDO SPs for mediating collaboration, resulting in higher-value services catered to customers that are not possible otherwise due to individual capabilities. Such models will eventually evolve into automated system-integration techniques for crafting novel, complex services that leverage elementary ones.

Since this article aims to provide a comprehensive overview of cross-domain orchestration for Future Open Networks, it primarily focuses on functional aspects. It only reports a limited implementation of the elements described, both AI/ML and non-AI/ML, rather than their complete physical realisation. Therefore, we aim to extend the implementation of the system-level architecture by assigning effective assets, models, and algorithms to the architectural functions as needed. It is also vital to achieve higher autonomy for Cross-Domain and Intra-Domain Orchestration through the operational harmonisation of the Cognitive &AI/ML elements.

ACKNOWLEDGMENTS

Work towards this paper is undertaken in the REASON project, partially funded by the UK Government, Department of Science, Innovation and Technology (DSIT) under the Future Open Networks Research Challenge (FONRC).

REFERENCES

[1] UK-GOV-DSIT, "Telecoms Diversification Taskforce Findings and Report," 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975007/April_2021_Telecoms_Diversification_Taskforce_Findings_and_Report_v2.pdf [Accessed 07-10-2024].

[2] 5GPPP, "The potential of the future connectivity systems for vertical industries," 2024, [Accessed 07-10-2024]. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2024/07/6GSTART-Verticals-Cartography-Whitepaper-Jul2024.pdf

[3] R. S. International Telecommunication Union, "Framework and overall objectives of the future development of imt for 2030 and beyond," https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2160-0-202311-I!!PDF-E.pdf, 2023, [Accessed 18-10-2024].

[4] M. K. Bahare, A. Gavras, M. Gramaglia, J. Cosmas, X. Li, O. Bulakci, A. Rahman, A. Kostopoulos, A. Mesodiakaki, D. Tsolkas, M. Ericson, M. Boldi, M. Uusitalo, M. Ghoraishi, and P. Rugeland, "The 6g architecture landscape - european perspective," 2023. [Online]. Available: https://zenodo.org/record/7313232

[5] Nokia, "Networks in 2030: Why an open future is essential," https://www.nokia.com/thought-leadership/articles/networks-2030-open-telecoms-future/, [Accessed 04-10-2024].

[6] Ericsson, "An introduction to data-driven network architecture," https://www.ericsson.com/en/blog/2020/10/data-driven-network-architecture, 2020, [Accessed 04-10-2024].

[7] R. Chataut, M. Nankya, and R. Akl, "6g networks and the ai revolution exploring technologies, applications, and emerging challenges," *Sensors*, vol. 24, no. 6, p. 1888, 2024.

[8] Y. Wu and J. Zhou, "Dynamic service function chaining orchestration in a multi-domain: a heuristic approach based on srv6," *Sensors*, vol. 21, no. 19, p. 6563, 2021.

[9] GSMA, "Generic Network Slice Template," chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gsma.com/newsroom/wp-content/uploads//NG.116-v9.0-1.pdf, 2023, [Accessed 18-12-2024].

[10] M. K. Bahare, A. Gavras, M. Gramaglia, J. Cosmas, X. Li, O. Bulakci, A. Rahman, A. Kostopoulos, A. Mesodiakaki, D. Tsolkas, M. Ericson, M. Boldi, M. Uusitalo, M. Ghoraishi, and P. Rugeland, "The 6g architecture landscape - european perspective," 2023. [Online]. Available: https://zenodo.org/record/7313232

[11] A. Collet, A. Banchs, and M. Fiore, "Lossleap: Learning to predict for intent-based networking," in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*. IEEE, 2022, pp. 2138–2147.

[12] "A holistic flagship towards the 6G network platform and system, to inspire digital transformation, for the world to act together in meeting needs in society and ecosystems with novel 6G services | Hexa-X-II Project | Results | HORIZON | CORDIS | European Commission — cordis.europa.eu," https://cordis.europa.eu/project/id/101095759/results, [Accessed 10-06-2024].

[13] K. Katsaros, I. Mavromatis, K. Antonakoglou, S. Ghosh, D. Kaleshi, T. Mahmoodi, H. Asgari, A. Karousos, I. Tavakkolnia, H. Safi, H. Hass, C. Vrontos, A. Emami, J. P. Ullauri, S. Moazzeni, and D. Simeonidou, "Ai-native multi-access future networks – the reason architecture," 2024. [Online]. Available: https://arxiv.org/abs/2411.06870

[14] 3GPP, "Management and orchestration provisioning," https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3274, 2025, [Accessed 31-01-2025].

[15] 3GPP, "Technical specification: Management and orchestration, architecture framework (rel 19), version 19.0.0," https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3416, 2025, [Accessed 24-01-2025].

[16] ETSI, "Etsi gs zsm 008 v1.1.1 (2022-07): Zero-touch network and service management (zsm); cross-domain e2e service lifecycle management," European Telecommunications Standards Institute (ETSI), Tech. Rep., Jul. 2022. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/008/01.01.01_60/gs_ZSM008v010101p.pdf

[17] J. Meredith, "Management and orchestration; 5g network resource model (nrm); stage 2 and stage 3," https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3400, 2025, [Accessed 31-01-2025].

[18] ETSI, "Zero-touch network and service management (zsm); end-to-end network slicing management and orchestration aspects," ETSI, Tech. Rep. ETSI GS ZSM 003 V1.1.1, September 2021, accessed: 2025-04-10. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/003/01.01.01_60/gs_ZSM003v010101p.pdf

[19] ETSI , "Zero-touch network and service management (zsm); enablers for artificial intelligence-based automation," ETSI, Tech. Rep. ETSI GS ZSM 012 V1.1.1, December 2022, accessed: 2025-04-10. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/012/01.01.01_60/gs_ZSM012v010101p.pdf

[20] ETSI, "Experiential networked intelligence (eni); system architecture," ETSI, Tech. Rep. ETSI GS ENI 005 V2.1.1, December 2021, accessed: 2025-04-10. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ENI/001_099/005/02.01.01_60/gs_ENI005v020101p.pdf

[21] "3rd generation partnership project; technical specification group services and system aspects; telecommunication management; study on a restful http-based solution set (release 14)," 3GPP, Tech. Rep. TR 32.866, 2017, accessed: 2025-04-10. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/32_series/32.866/32866-f00.zip

[22] M. Pope, "System architecture for the 5g system (5gs)," https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144, 2025, [Accessed 31-01-2025].

[23] "3rd generation partnership project; technical specification group services and system aspects; management and orchestration; security assurance specification for the 5g management system (release 16)," 3GPP, Tech. Rep. TS 28.554, 2020, accessed: 2025-04-10. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/128500_128599/128554/16.00.00_60/ts_128554v160000p.pdf

[24] ETSI, "Zero-touch network and service management (zsm); security aspects, including trust and policy management," ETSI, Tech. Rep.

ETSI GR ZSM 010 V1.1.1, July 2021, accessed: 2025-04-10. [Online]. Available: https://www.etsi.org/deliver/etsi_gr/ZSM/001_099/010/01.01.01_60/gr_ZSM010v010101p.pdf

[25] 3GPP, "3rd generation partnership project; technical specification group services and system aspects; policy and charging control framework (release 16)," 3GPP, Tech. Rep. TS 23.503, 2020, accessed: 2025-04-10. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123500_123599/123503/16.06.00_60/ts_123503v160600p.pdf

[26] J. Mangues-Bafalluy, "Final design and evaluation of the innovations of the 5g end-to-end service platform," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5ddd47b49&appId=PPGMS, 2021, [Accessed 14-11-2024].

[27] X. Li, C. Guimaraes, G. Landi, J. Brenes, J. Mangues-Bafalluy, J. Baranda, D. Corujo, V. Cunha, J. Fonseca, J. Alegria *et al.*, "Multi-domain solutions for the deployment of private 5g networks," *IEEE Access*, vol. 9, pp. 106 865–106 884, 2021.

[28] K. Katsaros, "5g-victori infrastructure operating system – final design specification," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5e7b58b17&appId=PPGMS, 2022, [Accessed 14-11-2024].

[29] A. Tzanakaki, "5g-victori end-to-end reference architecture," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5eaeaac83&appId=PPGMS, 2022, [Accessed 14-11-2024].

[30] G. M. Pérez, "Final design of zero touch service management with security and trust solutions," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f90691fe&appId=PPGMS, 2022, [Accessed 14-11-2024].

[31] N. P. Palma, "Final report on enablers and mechanisms for liability-aware trustable smart 5g security management framework," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f33779a5&appId=PPGMS, 2022, [Accessed 14-11-2024].

[32] E. Félix, "Trust management in multi-tenant/multi-party/multi-domain 5g environment," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5ec198c1e&appId=PPGMS, 2022, [Accessed 14-11-2024].

[33] Chafika Benzaid, Pol Alemany, Dhouha Ayed, G. Chollon, Maria Christopoulou, Gürkan Gür, Vincent Lefebvre, Edgardo Montes De Oca, Raul Muñoz, Jordi Ortiz, Antonio Pastor, Ramon Sanchez-Iborra, Tarik Taleb, Ricard Vilalta, and George Xilouris, "White paper: Intelligent security architecture for 5g and beyond networks," 2020. [Online]. Available: https://zenodo.org/record/4288658

[34] J. McNamara, "Evaluation of e2e 5g infrastructure and service slices, and of the developed self-learning ml algorithms," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f30944bf&appId=PPGMS, 2022, [Accessed 14-11-2024].

[35] P. Porambage, "Foundation of overall 6g system design and preliminary evaluation results," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e506934161&appId=PPGMS, 2023, [Accessed 17-10-2024].

[36] M. Ericson, "Foundation of overall 6g system design and preliminary evaluation results," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5fb281cbe&appId=PPGMS, 2023, [Accessed 17-12-2024].

[37] M. Ericson , "Analysis of 6g architectural enablers' applicability and initial technological solutions," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f330ff79&appId=PPGMS, 2022, [Accessed 17-12-2024].

[38] M. Gramaglia, "Final design of real-time control and vnf intelligence mechanisms," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e50229b7e5&appId=PPGMS, 2023, [Accessed 14-11-2024].

[39] M. Camelo, "Final daemon network intelligence framework and toolsets," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5fddb0649&appId=PPGMS, 2023, [Accessed 14-11-2024].

[40] F. Granelli, "Horse architectural design (it-1)," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e502292406&appId=PPGMS, 2023, [Accessed 17-12-2024].

[41] T. Jarvet, "Requirements, use cases and system architecture – Initial," https://adroit6g.eu/wp-content/uploads/2023/12/ADROIT6G_D2.1_Requirements-Use-cases-Architecture_Final.pdf, 2023, [Accessed 14-11-2024].

[42] V. Lefebvre, "Initial report on the intelligent and secure management, orchestration, and control platform," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5053a7fe7&appId=PPGMS, 2023, [Accessed 14-11-2024].

[43] RIGOUROUS, "Design plan of the multi-domain automated security orchestration, trust-management, and deployment," Jan. 2024. [Online]. Available: https://doi.org/10.5281/zenodo.10476147

[44] RIGOUROUS, "Design plan of the ai-driven anomaly detection, decision and mitigation," 2023. [Online]. Available: https://zenodo.org/doi/10.5281/zenodo.10476152

[45] P.-G. Consortium, "PREDICT-6G framework architecture and initial specification," Jun. 2024. [Online]. Available: https://doi.org/10.5281/zenodo.12167838

[46] PREDICT-6G Consortium, "D3.2 implementation of selected release 1 ai-driven inter-domain network control, management and orchestration innovations," 2024. [Online]. Available: https://zenodo.org/doi/10.5281/zenodo.12167665

[47] P.-G. Consortium, "D3.1 release 1 of ai-driven inter-domain network control, management, and orchestration innovations," 2023. [Online]. Available: https://zenodo.org/doi/10.5281/zenodo.12167712

[48] P. R. Grammatikis, "Across platform architecture and technical specifications," European Commission, Report Ares(2024)4749642, 2024, accessed: 2025-04-22. [Online]. Available: https://cordis.europa.eu/project/id/101097122/results

[49] X. Li, A. Garcia-Saavedra, X. Costa-Perez, C. J. Bernardos, C. Guimarães, K. Antevski, J. Mangues-Bafalluy, J. Baranda, E. Zeydan, D. Corujo, P. Iovanna, G. Landi, J. Alonso, P. Paixão, H. Martins, M. Lorenzo, J. Ordonez-Lucena, and D. R. López, "5growth: An end-to-end service platform for automated deployment and management of vertical services over 5g networks," *IEEE Communications Magazine*, vol. 59, no. 3, pp. 84–90, 2021.

[50] 5G-VICTORY, "About 5G-VICTORI - 5G-VICTORI — 5g-victori-project.eu," https://www.5g-victori-project.eu/about-5g-victori/, 2023, [Accessed 10-06-2024].

[51] S. Moazzeni, K. Katsaros, N. Ferdosian, K. Antonakoglou, M. Rouse, D. Kaleshi, A. Fernández-Fernández, M. Catalan-Cid, C. Vrontos, R. Nejabati *et al.*, "5g-vios: Towards next generation intelligent inter-domain network service orchestration and resource optimisation," *Computer Networks*, vol. 241, p. 110202, 2024.

[52] 5G-ZORO, "Zero-touch security and trust for ubiquitous computing and connectivity in 5G networks. | 5GZORRO Project | Results | H2020 | CORDIS | European Commission — cordis.europa.eu," https://cordis.europa.eu/project/id/871533/results, 2022, [Accessed 10-06-2024].

[53] J. M. Jorquera Valero, P. M. Sánchez Sánchez, A. Lekidis, J. Fernandez Hidalgo, M. Gil Pérez, M. S. Siddiqui, A. Huertas Celdran, and G. Martínez Pérez, "Design of a security and trust framework for 5g multi-domain scenarios," *Journal of Network and Systems Management*, vol. 30, no. 1, p. 7, 2022.

[54] K. Barabash, G. Carrozzo, D. Lorenz, K. Meth, and S. M. Siddiqui, "Zero-touch aiops in multi-operator 5g networks."

[55] INSPIRE-5Gplus, "INtelligent Security and PervasIve tRust for 5G and Beyond | INSPIRE-5Gplus Project | Results | H2020 | CORDIS | European Commission — cordis.europa.eu," https://cordis.europa.eu/project/id/871808/results, [Accessed 10-06-2024].

[56] 5G-CLARITY, "Beyond 5G multi-tenant private networks integrating Cellular, WiFi, and LiFi, Powered by ARtificial Intelligence and Intent Based PolicY | 5G-CLARITY Project | Results | H2020 | CORDIS | European Commission — cordis.europa.eu," https://cordis.europa.eu/project/id/871428/results, [Accessed 10-06-2024].

[57] T. Cogalan, D. Camps-Mur, J. Gutiérrez, S. Videv, V. Sark, J. Prados-Garzon, J. Ordonez-Lucena, H. Khalili, F. Cañellas, A. Fernández-Fernández, M. Goodarzi, A. Yesilkaya, R. Bian, S. Raju, M. Ghoraishi, H. Haas, O. Adamuz-Hinojosa, A. Garcia, C. Colman-Meixner, A. Mourad, and E. Aumayr, "5g-clarity: 5g-advanced private networks integrating 5gnr, wifi, and lifi," *IEEE Communications Magazine*, vol. 60, no. 2, pp. 73–79, 2022.

[58] J. Mcnamara, D. Camps-Mur, M. Goodarzi, H. Frank, L. Chinchilla-Romero, F. Cañellas, A. Fernández-Fernández, and S. Yan, "Nlp powered intent based network management for private 5g networks," *IEEE Access*, vol. 11, pp. 36 642–36 657, 2023.

[59] A. Tzanakaki, "Final system architecture and its evaluation," https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5f3095974&appId=PPGMS, 2022, [Accessed 14-11-2024].

[60] DAEMON, "Network intelligence for aDAptive and sElf-Learning MObile Networks | DAEMON Project | Results | H2020 | CORDIS | European Commission — cordis.europa.eu," https://cordis.europa.eu/project/id/101017109/results, 2024, [Accessed 10-06-2024].

[61] P. Soto, M. Camelo, D. De Vleeschauwer, Y. De Bock, C.-Y. Chang, J. F. Botero, and S. Latré, "Network intelligence for nfv scaling in closed-loop architectures," *IEEE Communications Magazine*, vol. 61, no. 6, pp. 66–72, 2023.

[62] C. Fiandrino, G. Attanasio, M. Fiore, and J. Widmer, "Toward native explainable and robust ai in 6g networks: Current state, challenges and road ahead," *Computer Communications*, vol. 193, pp. 47–52, 2022.

[63] HORSE, "Holistic, omnipresent, resilient services for future 6g wireless and computing ecosystems," https://horse-6g.eu/, 2023, [Accessed 22-11-2024].

[64] M. Garrich, J.-L. Romero-Gázquez, F.-J. Moreno-Muro, M. Hernández-Bastida, M.-V. B. Delgado, A. Bravalheri, N. Uniyal, A. S. Muqaddas, R. Nejabati, R. Casellas *et al.*, "It and multi-layer online resource allocation and offline planning in metropolitan networks," *Journal of Lightwave Technology*, vol. 38, no. 12, pp. 3190–3199, 2020.

[65] ADROIT6G, "ADROIT6G project home — adroit6g.eu," https://adroit6g.eu/, 2024, [Accessed 04-10-2024].

[66] DESIRE6G, "DESIRE-6G: Deep Programmability and Secure Distributed Intelligence for Real-Time End-to-End 6G Networks," https://desire6g.eu/, 2024, [Accessed 04-10-2024].

[67] REGOROUS, "RIGOROUS-6G: Project Home," https://rigourous.eu/, 2025, [Accessed 04-10-2024].

[68] PREDICT-6G, "PREDICT-6G: Towards a deterministic 6G network: reliable,time sensitive and predictable — predict-6g.eu," https://predict-6g.eu/, 2024, [Accessed 04-10-2024].

[69] ACROSS Consortium, "Automated zero-touch cross-layer provisioning framework for 5g and beyond vertical services (across)," https://cordis.europa.eu/project/id/101097122, 2023, funded by the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101097122.

[70] D. Gkounis, N. Uniyal, A. S. Muqaddas, R. Nejabati, and D. Simeonidou, "Demonstration of the 5guk exchange: A lightweight platform for dynamic end-to-end orchestration of softwarized 5g networks," in *2018 European Conference on Optical Communication (ECOC)*. IEEE, 2018, pp. 1–3.

[71] S. Sharma, N. Uniyal, B. Tola, and Y. Jiang, "On monolithic and microservice deployment of network functions," in *2019 IEEE Conference on Network Softwarization (NetSoft)*. IEEE, 2019, pp. 387–395.

[72] A. Bravalheri, A. S. Muqaddas, N. Uniyal, R. Casellas, R. Nejabati, and D. Simeonidou, "Vnf chaining across multi-pops in osm using transport api," in *2019 Optical Fiber Communications Conference and Exhibition (OFC)*. IEEE, 2019, pp. 1–3.

[73] X. Vasilakos, W. Featherstone, N. Uniyal, A. Bravalheri, A. S. Muqaddas, N. Solhjoo, D. Warren, S. Moazzeni, R. Nejabati, and D. Simeonidou, "Towards zero downtime edge application mobility for ultra-low latency 5g streaming," in *2020 IEEE Cloud Summit*. IEEE, 2020, pp. 25–32.

[74] M. Bunyakitanon, X. Vasilakos, R. Nejabati, and D. Simeonidou, "End-to-end performance-based autonomous vnf placement with adopted reinforcement learning," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 534–547, 2020.

[75] M. Bunyakitanon, A. P. Da Silva, X. Vasilakos, R. Nejabati, and D. Simeonidou, "Auto-3p: An autonomous vnf performance prediction & placement framework based on machine learning," *Computer Networks*, vol. 181, p. 107433, 2020.

[76] S. Moazzeni, P. Jaisudthi, A. Bravalheri, N. Uniyal, X. Vasilakos, R. Nejabati, and D. Simeonidou, "A novel autonomous profiling method for the next-generation nfv orchestrators," *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 642–655, 2020.

[77] X. Vasilakos, S. Moazzeni, A. Bravalheri, P. Jaisudthi, R. Nejabati, and D. Simeonidou, "ion-profiler: Intelligent online multi-objective vnf profiling with reinforcement learning," *IEEE Transactions on Network and Service Management*, 2024.

[78] J. Gallego-Madrid, R. Sanchez-Iborra, P. M. Ruiz, and A. F. Skarmeta, "Machine learning-based zero-touch network and service management: A survey," *Digital Communications and Networks*, vol. 8, no. 2, pp. 105–123, 2022.

[79] J. A. Hawkinson and T. J. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)," RFC 1930, Mar. 1996. [Online]. Available: https://www.rfc-editor.org/info/rfc1930

[80] E. C. Strinati and S. Barbarossa, "6g networks: Beyond shannon towards semantic and goal-oriented communications," *Computer Networks*, vol. 190, p. 107930, 2021.

[81] J. Liu, X. Du, J. Cui, M. Pan, and D. Wei, "Task-oriented intelligent networking architecture for the space–air–ground–aqua integrated network," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5345–5358, 2020.

[82] A. Mostaani, T. X. Vu, S. K. Sharma, V.-D. Nguyen, Q. Liao, and S. Chatzinotas, "Task-oriented communication design in cyber-physical systems: A survey on theory and applications," *IEEE Access*, vol. 10, pp. 133 842–133 868, 2022.

[83] ETSI, "Network functions virtualisation (nfv) release 2; management and orchestration; architectural framework specification," European Telecommunications Standards Institute (ETSI), Group Specification GS NFV 006 V2.1.1, Jan. 2021, accessed: 2025-04-22. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/nfv/001_099/006/02.01.01_60/gs_nfv006v020101p.pdf

[84] D. Goderis, D. Griffin, C. Jacquenet, and G. Pavlou, "Attributes of a service level specification (sls) template," https://www.ietf.org/archive/id/draft-tequila-sls-03.txt, 2003, [Accessed 27-11-2024].

[85] C. Pedrosa-Ortega, M. J. Hernández-Ortiz, E. García-Martí, and M. C. Vallejo-Martos, "The stakeholder salience model revisited: Evidence from agri-food cooperatives in spain," *Sustainability*, vol. 11, no. 3, p. 574, 2019.

[86] A. G. Papidas and G. C. Polyzos, "Self-organizing networks for 5g and beyond: A view from the top," *Future Internet*, vol. 14, no. 3, p. 95, 2022.

[87] M. Beshley, M. Klymash, I. Scherm, H. Beshley, and Y. Shkoropad, "Emerging network technologies for digital transformation: 5g/6g, iot, sdn/ibn, cloud computing, and blockchain," in *IEEE International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering*. Springer, 2022, pp. 1–20.

[88] J. Niemöller, R. Szabó, A. Zahemszky, and D. Roeland, "Creating autonomous networks with intent-based closed loops," *Ericsson Technology Review*, vol. 2022, no. 4, pp. 2–11, 2022.

[89] P. Georgatsos, J. Spencer, D. Griffin, T. Damilatis, H. Asgari, J. Griem, G. Pavlou, and P. Morand, "Provider-level service agreements for inter-domain qos delivery," in *Quality of Service in the Emerging Networking Panorama*, J. Solé-Pareta, M. Smirnov, P. Van Mieghem, J. Domingo-Pascual, E. Monteiro, P. Reichl, B. Stiller, and R. J. Gibbens, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 368–377.

[90] P. Morand *et al.*, "Initial specification of protocols and algorithms for inter-domain sls management and traffic engineering for qos-based ip service delivery and their test requirements," *Deliverable D1*, vol. 2, 2004.

[91] M. Sloman, "Policy driven management for distributed systems," *Journal of network and Systems Management*, vol. 2, pp. 333–360, 1994.

[92] J. Strassner and J. S. Strassner, *Policy-based network management: solutions for the next generation*. Morgan Kaufmann, 2004.

[93] H.-W. Braun, "Models of policy based routing," RFC 1104, Jun. 1989. [Online]. Available: https://www.rfc-editor.org/info/rfc1104

[94] S. Ghosh, K. Antonakoglou, I. Mavromatis, and K. Katsaros, "Intelligent routing as a service (iraas) a flexible routing framework for knowledge-defined networks," in *2024 IFIP Networking Conference (IFIP Networking)*, 2024, pp. 5–13.

[95] International Telecommunication Union (ITU), "Security architecture for systems providing end-to-end communications," https://www.itu.int/rec/T-REC-X.805-200310-I/en, October 2003, iTU-T Recommendation X.805, [Accessed 2025-04-23].

[96] B. M. Khorsan, "Hexa-X architecture for B5G/6G networks – final release," https://hexa-x.eu/wp-content/uploads/2023/07/Hexa-X-D1.4-Final.pdf#page=115.09, 2023, [Accessed 02-10-2024].

[97] ETSI, "Zero-touch network and Service Management (ZSM); Enablers for Artificial Intelligence-based Network and Service Automation," chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/012/01.01.01_60/gs_ZSM012v010101p.pdf, [Accessed 08-11-2024].

[98] N. I. of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf, 2024, [Accessed 02-10-2024].

[99] P. Mell, J. Shook, and R. Harang, "Measuring and improving the effectiveness of defense-in-depth postures," in *Proceedings of the 2nd Annual Industrial Control System Security Workshop*, 2016, pp. 15–22.

[100] A. Asgari, R. Egan, P. Trimintzios, and G. Pavlou, "Scalable monitoring support for resource management and service assurance," *IEEE network*, vol. 18, no. 6, pp. 6–18, 2004.

[101] A. Tassi, D. Warren, Y. Wang, D. Bhamare, and R. Behravesh, "On optimization of next-generation microservice-based core networks," *IEEE Transactions on Vehicular Technology*, 2024.

[102] L. Parsons, "Ethical concerns mount as AI takes bigger decision-making role — news.harvard.edu," https://news.harvard.edu/gazette/story/2020/10/ethical-concerns-mount-as-ai-takes-bigger-decision-making-role/, 2020, [Accessed 02-10-2024].

[103] N. T. Lee, P. Resnick, , and G. Barton, "Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms — brookings.edu," https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/, 2019, [Accessed 02-10-2024].

[104] B. Brik, H. Chergui, L. Zanzi, F. Devoti, A. Ksentini, M. S. Siddiqui, X. Costa-Pérez, and C. Verikoukis, "A survey on explainable ai for 6g o-ran: Architecture, use cases, challenges and research directions," *arXiv preprint arXiv:2307.00319*, 2023.

[105] T. Shi, H. Ma, G. Chen, and S. Hartmann, "Location-aware and budget-constrained service brokering in multi-cloud via deep reinforcement learning," in *Service-Oriented Computing: 19th International Conference, ICSOC 2021, Virtual Event, November 22–25, 2021, Proceedings 19*. Springer, 2021, pp. 756–764.

[106] N. Toumi, M. Bagaa, and A. Ksentini, "Machine learning for service migration: a survey," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1991–2020, 2023.

[107] S. Wang, J. Xu, N. Zhang, and Y. Liu, "A survey on service migration in mobile edge computing," *IEEE Access*, vol. 6, pp. 23 511–23 528, 2018.

[108] T. Yu, H. Liu, L. Zhang, and H. Liu, "Msrdl: Deep learning framework for service recommendation in mashup creation," *Scientific Reports*, vol. 13, no. 1, p. 7641, 2023.

[109] O. A. Wahab, A. Mourad, H. Otrok, and T. Taleb, "Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1342–1397, 2021.

[110] M. R. TF, P. SivaPragasam, R. BalaKrishnan, G. Lalithambal, and S. Ragasubha, "Qos based classification using k-nearest neighbor algorithm for effective web service selection," in *2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. IEEE, 2015, pp. 1–4.

[111] C. Yin, R. Yang, W. Zhu, X. Zou, and J. Zhang, "Optimal planning of emergency communication network using deep reinforcement learning," *IEICE Transactions on Communications*, vol. 104, no. 1, pp. 20–26, 2021.

[112] J. Boyan and M. Littman, "Packet routing in dynamically changing networks: A reinforcement learning approach," *Advances in neural information processing systems*, vol. 6, 1993.

[113] Y.-H. Hsu, J.-I. Lee, and F.-M. Xu, "A deep reinforcement learning based routing scheme for leo satellite networks in 6g," in *2023 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2023, pp. 1–6.

[114] J. Nan, M. Ai, A. Liu, and X. Duan, "Regional-union based federated learning for wireless traffic prediction in 5g-advanced/6g network," in *2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*. IEEE, 2022, pp. 423–427.

[115] C. Zhang and P. Patras, "Long-term mobile traffic forecasting using deep spatio-temporal neural networks," in *Proceedings of the Eighteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2018, pp. 231–240.

[116] G. O. Ferreira, C. Ravazzi, F. Dabbene, G. C. Calafiore, and M. Fiore, "Forecasting network traffic: A survey and tutorial with open-source comparative evaluation," *IEEE Access*, vol. 11, pp. 6018–6044, 2023.

[117] M. Abbasi, A. Shahraki, and A. Taherkordi, "Deep learning for network traffic monitoring and analysis (ntma): A survey," *Computer Communications*, vol. 170, pp. 19–41, 2021.

[118] R. A. Addad, D. L. C. Dutra, T. Taleb, and H. Flinck, "Ai-based network-aware service function chain migration in 5g and beyond networks," *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, pp. 472–484, 2021.

[119] Y. Liu, C. Zhang, H. Yang, S. Zhang, X. Wang, and F. Li, "Deep reinforcement learning based reliability aware sfc placement in multi-domain networks," in *2023 15th International Conference on Communication Software and Networks (ICCSN)*. IEEE, 2023, pp. 215–219.

[120] V. B. Souza, M. H. Pereira, L. H. Lelis, and X. Masip-Bruin, "Enhancing resource availability in vehicular fog computing through smart inter-domain handover," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*. IEEE, 2020, pp. 1–6.

[121] M. I. Khan, M. M. Alam, Y. L. Moullec, and E. Yaacoub, "Throughput-aware cooperative reinforcement learning for adaptive resource allocation in device-to-device communication," *Future Internet*, vol. 9, no. 4, p. 72, 2017.

[122] J. Hu, S. Guo, X. Kuang, F. Meng, D. Hu, and Z. Shi, "I-hmm-based multidimensional network security risk assessment," *IEEE Access*, vol. 8, pp. 1431–1442, 2019.

[123] K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5g/6g networks: Principles," *Challenges, and the Role of Machine Learning in the context of O-RAN. arXiv*, 2021.

[124] H. N. Fakhouri, S. Alawadi, F. M. Awaysheh, I. B. Hani, M. Alkhalaileh, and F. Hamad, "A comprehensive study on the role of machine learning in 5g security: challenges, technologies, and solutions," *Electronics*, vol. 12, no. 22, p. 4604, 2023.

[125] Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When machine learning meets privacy in 6g: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2694–2724, 2020.

[126] S. Sagar, A. Mahmood, Q. Z. Sheng, and W. E. Zhang, "Trust computational heuristic for social internet of things: A machine learning-based approach," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–6.

[127] A. M. Konsta, A. L. Lafuente, and N. Dragoni, "A survey of trust management for internet of things," *IEEE Access*, 2023.

[128] S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki, and W. Ni, "Towards a machine learning driven trust management heuristic for the internet of vehicles," *Sensors*, vol. 23, no. 4, p. 2325, 2023.

[129] J. Wang, X. Jing, Z. Yan, Y. Fu, W. Pedrycz, and L. T. Yang, "A survey on trust evaluation based on machine learning," *ACM Computing Surveys (CSUR)*, vol. 53, no. 5, pp. 1–36, 2020.

[130] J. Wang, Z. Yan, H. Wang, T. Li, and W. Pedrycz, "A survey on trust models in heterogeneous networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2127–2162, 2022.

[131] Y. He, G. Han, J. Jiang, H. Wang, and M. Martinez-Garcia, "A trust update mechanism based on reinforcement learning in underwater acoustic sensor networks," *IEEE Transactions on Mobile Computing*, vol. 21, no. 3, pp. 811–821, 2020.

[132] N. Çevik and S. Akleylek, "Sok of machine learning and deep learning based anomaly detection methods for automatic dependent surveillance-broadcast," *Ieee Access*, 2024.

[133] M. Sarhan, S. Layeghy, and M. Portmann, "Evaluating standard feature sets towards increased generalisability and explainability of ml-based network intrusion detection," *Big Data Research*, vol. 30, p. 100359, 2022.

[134] F. B. Saghezchi, G. Mantas, M. A. Violas, A. M. de Oliveira Duarte, and J. Rodriguez, "Machine learning for ddos attack detection in industry 4.0 cppss," *Electronics*, vol. 11, no. 4, p. 602, 2022.

[135] N. M. Hijazi, M. Aloqaily, M. Guizani, B. Ouni, and F. Karray, "Secure federated learning with fully homomorphic encryption for iot communications," *IEEE Internet of Things Journal*, 2023.

[136] A. F. Diallo and P. Patras, "Adaptive clustering-based malicious traffic classification at the network edge," in *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*. IEEE, 2021, pp. 1–10.

[137] H. Asgari, S. Haines, and O. Rysavy, "Identification of threats and security risk assessments for recursive internet architecture," *IEEE Systems Journal*, vol. 12, no. 3, pp. 2437–2448, 2017.

[138] Cloud Native Computing Foundation, "Kubernetes," https://kubernetes.io/, 2025, accessed: 2025-04-22.

[139] The Helm Authors, "Helm: The package manager for kubernetes," https://helm.sh/, 2025, accessed: 2025-04-22.

[140] Istio Authors, "Istio: Open source service mesh for cloud-native applications," https://istio.io/, 2025, accessed: 2025-04-22.

[141] Linux Foundation, "Nephio: Cloud native network automation," https://nephio.org/, 2025, accessed: 2025-04-22.

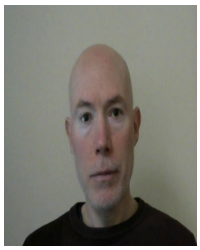
[142] Cisco Systems, "Dynamic multipoint vpn (dmvpn)," https://www.cisco.com/c/en/us/support/security/dynamic-multipoint-vpn-dmvpn/series.html, 2025, accessed: 2025-04-22.

[143] "Generic routing encapsulation (gre)," https://www.rfc-editor.org/rfc/rfc2784.html, 2000, rFC 2784, Internet Engineering Task Force.

[144] S. Kent and K. Seo, "Security architecture for the internet protocol," https://www.rfc-editor.org/rfc/rfc4301.html, 2005, rFC 4301, Internet Engineering Task Force.
[145] PostgreSQL Global Development Group, "Postgresql: The world's most advanced open source relational database," https://www.postgresql.org/, 2025, accessed: 2025-04-22.
[146] IETF OAuth Working Group, "Oauth 2.0 authorization framework," https://oauth.net/2/, 2025, accessed: 2025-04-22.
[147] Grafana Labs, "Grafana: The open and composable observability platform," https://grafana.com/, 2025, accessed: 2025-04-22.
[148] InfluxData, "Influxdb: Time series data platform," https://www.influxdata.com/, 2025, accessed: 2025-04-22.
[149] Sebastián Ramírez, "Fastapi: Modern, fast (high-performance) web framework for building apis with python," https://fastapi.tiangolo.com/, 2025, accessed: 2025-04-22.
[150] NetworkX Developers, "Networkx: Python package for the creation, manipulation, and study of the structure, dynamics, and functions of complex networks," https://networkx.org/, 2025, accessed: 2025-04-22.

SAPTARSHI GHOSH is a Future Networks Technologist in Orchestration at Digital Catapult with over five years of experience in B5G technologies. He received his M.E. in Software Engineering from Jadavpur University, India (2016), M.Sc. in Smart Networks from the University of the West of Scotland, UK (2017) and PhD in Cognitive Routing for Self-Organised Knowledge-Defined Networking in 5G from London South Bank University, UK (2021) with GATE, Erasmus-Mundus and Marie Skłodowska-Curie Fellowships respectively. Saptarshi has contributed to the knowledge focusing on network softwarisation, automation, orchestration and intelligence through several EU/UK projects funded by Horizon, Innovate-UK, Erasmus+, DST-DASA, EPSRC, and DSIT and has obtained industrial certifications including JNCIA-DevOps and CCNP-EI. Formerly, he was associated with London South Bank University as a sessional lecturer and Senior Research Fellow. His research domain includes network orchestration, knowledge-defined networking, IP routing, 6G Self-Organised-Networking and Graph Theory.

HAMID ASGARI has been with Thales UK Research, Technology, Solution & Innovation (RTSI) since 1996 and is a Thales Expert. He is also a Visiting Professor at King's College London since 2013. He is currently leading both Future Network and Verification &Validation research activities at RTSI. Hamid in highly experienced and has been directing research, leading R&D teams internally at Thales and externally in national and European collaborative projects since year 2000. Hamid has also been liaising and coordinating external collaborations with industry and academia. He has been very active in transferring technology resulted from R&D, linking the technologies with application areas, and contributing towards their use. He has a proven track record of publications in highly-valued journals and peer-reviewed conferences. He is a senior member of IEEE and has been involved in Technical Committees and standardisation Working Groups.



DARRYL HOND is a member of Thales UK Research, Technology & Solution Innovation and is a Thales Specialist in computer vision and image processing. He has a PhD in automatic face recognition, and has been conducting research for over 25 years into object classification, face analysis, motion detection and stereovision. This work has required the use of a range of pattern recognition and machine learning techniques, including the application of deep learning. His more recent research has concentrated on the development of algorithms for establishing the trustworthiness of artificial neural networks. During the REASON project, he has been investigating how machine learning models can support network management and orchestration, and how those models can be rendered trustworthy.

KOSTANTINOS ANTONAKOGLOU is a Senior Future Networks Technologist at Digital Catapult where he contributes in research and development of 5G and beyond 5G systems focusing on network service orchestration. In the past he has worked as a Research Associate at King's College London at the Centre for Telecommunications Research after completing a PhD there. Overall, he has worked on EU and EPSRC-funded projects such as 5GVICTORI, INITIATE, 5G-CAR and Primo-5G and is interested in a variety of topics including haptics and bilateral teleoperation over networks, inter-domain management and orchestration of network services as well as quantum communication and clock synchronisation.

IOANNIS MAVROMATIS is a Lead 5G/Future Networks Technologist at Digital Catapult, London, UK. He has extensive experience in 5G-and-beyond technologies, cloud-native computing, testbed deployments, wireless networking, software architecture and development. Dr Mavromatis received his PhD in "5G Connected and Automated Vehicles" in 2018 from the University of Bristol. He was the lead backend architect of the award-winning UMBRELLA framework, and, in the past, while working at Bristol Research and Innovation Laboratory of Toshiba Europe Ltd. and the University of Bristol, he was involved in several publicly and privately funded projects (SYNERGIA, CAVShield, BEACON-5G, FLOURISH, VENTURER, etc.). His research interests span the areas of 5G-and-beyond Communications, Cloud-native Computing, Cybersecurity, Machine Learning & Federated Learning, and Sustainability. Dr Mavromatis received the IEEE Popularity Award from IEEE VNC 2018 and the IEEE Best Paper Award from VTC-Spring 2019.

NOEL BUTLER is a Cybersecurity Specialist working in Thales's Research, Technology, Strategy, & Innovation (RTSI) team. He has 20+ years of experience in software development and is a cybersecurity subject matter expert, with particular interest in security threat and risk assessment methodologies, information security concepts and security architecture design.

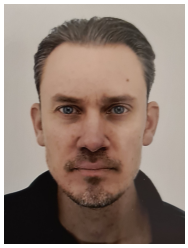
RASHEED HUSSAIN (Senior member, IEEE) is a Senior Lecturer with the Smart Internet Lab and Bristol Digital Futures Institute (BDFI), Department of Electrical and Electronic Engineering at the University of Bristol, UK. Before, he was with the Innopolis University, Russia, University of Amsterdam, Netherlands, and Hanyang University, South Korea. He also served as an ACM Distinguished Speaker (2018-2021) and currently serving another term as ACM Distinguished Speaker (2022-2026). To date, he has delivered around 20 invited and keynote talks (including ACM DSP lectures) and serves as Associate Editor in many journals including IEEE Communications Surveys and Tutorials. His research interests include Information, network, and cyber security, Future Networks (6G) security, Digital Twins security, Responsible AI, Explainable AI, and Fairness in AI.

SHASH ZEB (Member, IEEE) is a Postdoctoral Research Associate with the University of Bristol, Bristol, UK, where he is a member of the Smart Internet Lab and the High-Performance Networks research group. He received the B.E. degree in Electrical Engineering (EE) from the University of Engineering and Technology, Peshawar, Pakistan, in 2016, and the M.S. degree in Electrical Engineering from the National University of Sciences and Technology (NUST), Pakistan, in 2019. He completed his Ph.D. degree in Electrical Engineering in 2023 at NUST, where he served as a Research Associate with the Information Processing and Transmission (IPT) Lab, School of Electrical Engineering and Computer Science (SEECS). During his Ph.D., he was a visiting researcher at the CONNECT Research Center, Trinity College Dublin, under the Erasmus+ International Mobility Program, and a Ph.D. student Fellow with the Networked Intelligence Lab at the AI Graduate School, Gwangju Institute of Science and Technology. His research interests include emerging technological enablers and techniques, both theoretical and applied, for the design and implementation of Beyond-5G/6G networks and industrial communication..

KONSTANTINOS KATSAROS has 14+ years of experience in wireless communications across industry and academia. At Digital Catapult, he provides oversight for 5G and beyond 5G system architecture and subsystem implementations. Specializing in new architectures using virtualisation and edge computing across industrial sectors. Has led research into the use of mobile edge computing to assist immersive applications and connected vehicles. He has co-authored more than 20 peer-reviewed technical articles and conference papers and has two patents on vehicular communication systems.

SHADI MOAZZENI is a Lecturer in Networks at the University of Bristol, Bristol, UK, and a member of the Smart Internet Lab and Bristol Digital Futures Institute (BDFI). She previously served as a Senior Research Associate and later as a Research Fellow at the University of Bristol. She is the project investigator for the Innovate-UK funded nCOMM+ project and has collaborated as Co-Investigator on various UK projects such as TITAN, REASON, and UK-TIN. Additionally, she was the cluster lead researcher for the EU Horizon 2020 5G-VICTORI project. She received her M.Sc. degree in Computer Architecture Engineering from Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in 2010, and her PhD in Computer Architecture Engineering from the University of Isfahan, Iran, in 2018. From July 2016 to February 2017, she was a visiting PhD researcher at the University of Bologna, Italy.

She specialises in AI-Native 6G networks, focusing on the orchestration and optimisation of next-generation intelligent networks, multi-access edge computing, and intelligent multi-objective profiling towards zero-touch network and service management. Her work aims to enhance future network performance and develop innovative, human-centric networking solutions.



DAVID TEE (BEng, Electronic Engineering, Reading, MIET) has over 26 years' experience with Thales in the UK. His wide range of experience includes RF hardware design, simulation and prototyping, systems engineering test procedure design, verification and validation processes, and RF cosite analysis and propagation calculations. He has performed MATLAB data acquisition and analysis of Atomic Optical Magnetometer data for a project with UCL, been involved in low-TRL studies of quantum clock and quantum navigation devices. Java software developed to parse and translate from a domain specific language (DSL) to executable test cases for a connected autonomous vehicle project. More recently he has worked Simulink projects, delivery of a Python code base for an AI run-time dissimilarity algorithm demo, and a project manager role on a study of CHERI memory safety, and a data-driven detection, classification and identification project developing ML Operations concepts for deploying toolbox capabilities at the edge.

GABRIELE INCORVAIA is a member of Thales UK - Research, Technology & Solution Innovation, where he works as a Principal AI Research Engineer. He has experience in developing and implementing AI-based solutions for practical problems and has an interest in AI trustworthiness and verification. Before joining Thales UK, Gabriele completed a PhD in Mathematical Sciences at The University of Manchester.

DIMITRA SIMEONIDOU is a Full Professor at the University of Bristol, the Co-Director of the Bristol Digital Futures Institute and the Director of Smart Internet Lab. Her research is focusing on the fields of high-performance networks, programmable networks, Future Internet, wireless-optical convergence, 5G/6G and smart city infrastructures. In the past few years, she is increasingly working with Social Sciences and Humanities on topics of climate change and digital transformation for society and businesses. Dimitra has been the Technical Architect and the CTO of the smart city project Bristol Is Open. She is currently leading the Bristol City/Region 5G and Open RAN pilots. Dimitra is a member of the UK Government Supply Chain Diversification Advisory Council, a founding member of the UK Telecoms Innovation Network and member of the OFCOM Spectrum Advisory Board. She has led major research projects funded by UK Government and the EC. She is currently coordinating the DSIT REASON project developing blueprint architectures and technologies for 6G and the EPSRC JOINER project, aiming to establish a UK-wide experimentation platform for 6G research and innovation. She is the author and co-author of over 700 publications, numerous patents and several contributions to standards. She has been co-founder of three spin-out companies developing solutions for connected smart infrastructures. Dimitra is a Fellow of the Royal Academy of Engineering (FREng), a Fellow of the IEEE (FIEEE), Fellow of WWRF and member of UKCRC.