UKTIN

Future Capability Paper

Network Management

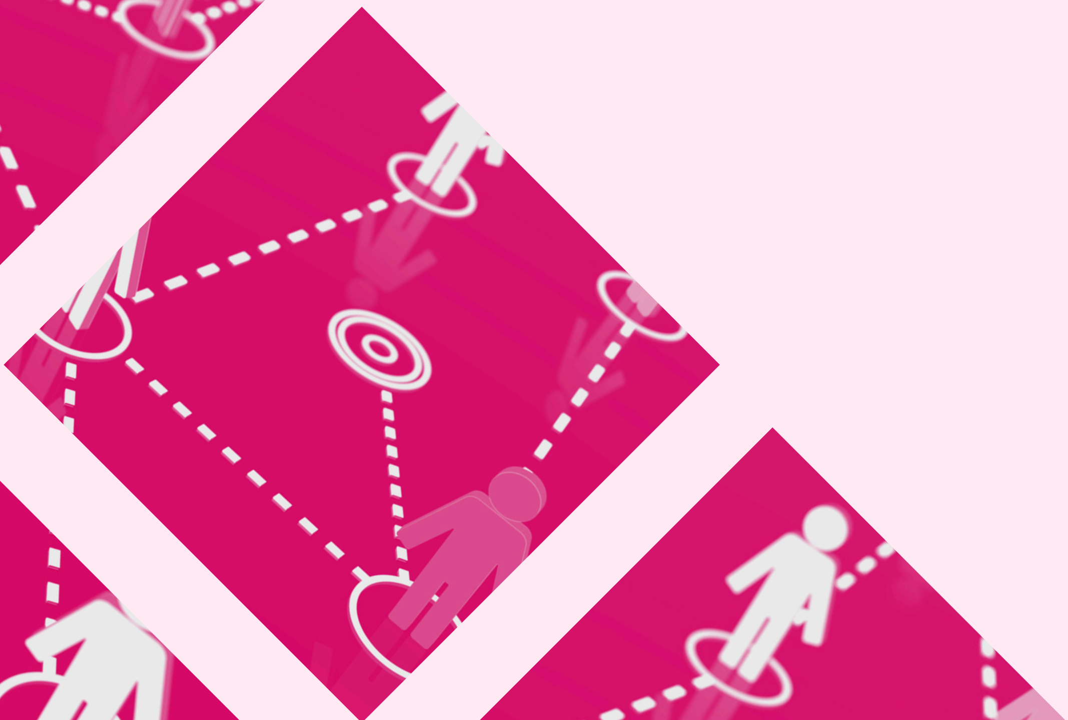


Table of Contents

Executive Summary

What is Network Management?

Network Management refers to the administration, monitoring, and maintenance of networks, ensuring that networks operate efficiently, securely, and reliably for customers whilst continually evolving to maintain performance, reduce risk of security attacks and introduce new and optimised services and features.

This task has gradually become harder over the decades with networks increasing in size, complexity, encumbered with legacy components, consolidation, competition, and budgetary pressures.

Ultimately, Network Management assures the trust a customer has in their provider, guaranteeing the service they're paying for will work.

Networks are and will be increasingly important to all aspects of the UK economy including:

- The drive to Net Zero, where the UK energy supply will be reliant on a robust digital backbone to support the integration and control of renewable energy onto the National Grid.
- Automations and robotics across heavy and light industry, warehouses, and distribution.
- Transport networks and autonomous vehicles (whether train, buses, trams, or cars).
- Heath services and especially remote health monitoring and intervention technologies.
- Finance and payment systems.
- Blue Light, legal and regulatory 'chain of evidence' industries requiring ubiquitous coverage and trusted identity.

Great Expectations

Up until now telecommunications networks have delivered a best-effort service satisfying consumer demand. Now they will need to transform to meet commercial, regulatory, and technical requirements necessitating fundamental changes to today's telecoms networks.

For example, 99.99% network availability is not good enough if assessed according to aviation or railway industry safety requirements. This 0.01% unavailability would translate to approximately a major communication incident each a day at Waterloo or Heathrow. By comparison, contemporary mobile telecommunications provide outdoor service around the 99.6% ballpark.

Network Management is fundamental to the provision of secure and reliable networks, from configuration, implementation of security policies, through monitoring, fault detection and resolution. As networks continue to sharply scale to support ever increasing data growth whilst managing more sophisticated security threats, the world of Network Management is and will continue to become more and more complex. In fact, it is now predicted that humans alone will soon not be able to effectively manage networks, and that automated software solutions will be essential to the delivery of future networks, we see this today in cyber security defence industries.

Our Objective

This paper, along with the other Future Capability Papers will elaborate on the ever-increasing complexity of the technical, commercial, and regulatory aspects affecting the management of contemporary and future telecoms networks, and then make recommendations to address these challenges, to assure the continuity of telecommunication services in the UK, and how the UK can return to be a global leader in this industry.

It should be noted that ultimately, exact measures will come down to why a customer pays for a telecoms service and the telecoms industry assures that service. Our recommendations as a team are all based on facilitating this future. We believe that the challenges our industry and our customers face, will be met through trust and collaboration, enabled by a truly long term, sustainable UK cross-industry telecommunications vision and strategy.

UK Telecoms Commercial Landscape

The telecommunications ecosystem and UK commercial landscape is unrecognisable from 50 years ago, even from 25 years ago. In part, this is due to the phenomenal growth the industry has undergone, and acceleration in growth in traffic volume, demand for ubiquitous coverage “absolutely everywhere” for consumers, enterprises, and machines. In turn this has led to increased expectations for guaranteed quality of service and assured reliability, and trust for industry and public services.

Today the UK telecoms landscape can be characterised as follows:

- Commercial complexity, no single provider can guarantee they provide the entire physical or logical service truly end to end for their customers.
    - Telecoms providers outsourcing non-core functions
    - All UK mobile network operators have placed their physical infrastructure assets into joint venture “Towercos”
    - The growth of the enterprise market served through neutral host and private network providers.
- Technological complexity, across multiple access and device-based technologies.
- Regulatory complexity, as above and across any industry telecommunications serve.

- Responsibility towards the environment and social concerns and ensuring appropriate governance.
- Pressure on every commercial enterprise to return shareholder value has driven off-shoring
- Demographically a shortage of qualified STEM skills, this skills deficit is serious. Demographically the telecommunications industry is in the main older than 40 not younger, and therefore we need to ensure that what we recommend will support the telecoms engineers, IT teams and technicians of the future to be far more productive than any previous generation.

Over the last 40 years, the UK has lost its leading edge in network technology and management. Mainly driven by globalisation and outsourcing, the UK is now over reliant on technology that is designed and manufactured abroad, and networks that are managed in outsource centres across the globe. As the world moves into a more unstable period, this leaves the UK in a vulnerable position which needs to be addressed. The UK is a service-based economy, its research base is still excellent, however translating research into home-based product development and a 'UK telecoms champion' hasn't happened (the closest is Arm).

Challenges & Opportunities

This future capability paper describes the technical and economic challenges facing network operators and providers with the management of their contemporary and future networks. Technology innovation must consider these to ensure that they are operated in an efficient and secure way whilst maintaining experience and benefits to customers as well as revenue for operators & and providers.

- Network of networks
  - Coverage, scale, complexity, heterogeneity, multiplexity, 5G, 6G and beyond...
    - Both contemporary Environmental Social and Governance requirements and the economic viability of providing ubiquitous coverage and capacity solutions of multiple technologies will lead to more collaborative models, sharing of infrastructure and active equipment.
    - This growth in relationships across physical, logical and commercial boundaries will lead to a significant permutation challenge to successfully assure & maintain customer service across all involved agencies.
    - Involved agencies will need a guaranteed way of ‘sharing’ and ‘trusting’ each other in real-time.
- Customer experience management
  - Self-orchestration in the future assured services in critical industries will expect far better service availability than currently offered by the operators. It won’t be acceptable to react to faults, but instead pre-empt issues and route around faults, and repair services.
  - This will obviously require an AI led approach, necessitating significant data capture and analysis from multiple sources to proactively predict and prevent faults affecting service.
  - Fault management and recovery automated by AI.
  - Customer perception, reporting and visibility.
    - Providing customers a real time view of their service and performance
    - Automated real time traffic management, routing and optimised traffic shaping based on usage type and patterns.

- Secured network topology discovery and control
    - Elasticity and interoperability, modern networks are extremely dynamic with (physical and virtual) connectivity to serve customers formed and dismantled on a continuous basis across many interconnected networks, nodes, cloud, and applications layers.
    - Network change today is driven by the constant need for software, firmware, and configuration updates. This will need to be coordinated across these layers.
    - Autonomous security, patch and software updates are becoming more critical for customers to continue to trust telecoms, even in Zero Trust Networks.
    - These interacting layers must be observable, discoverable to each other, ultimately controllable with aligned security, ensuring all changes are authorised correctly.
    - AI driven APIs & digital security are critical to underpin this complexity in a trusted manner.

These examples illustrate the importance of AI and introducing new ways of ingesting and processing huge amounts of data, to uncover inter-dependencies between an ever-increasing number of devices, servers, software etc and feeding into processes such as anomaly detection, traffic engineering, topology discover.

Recommendations

With networks moving towards software running either in the cloud or on specialised edge microprocessors close to the end users, there is an opportunity for the UK to build upon its:

- Leadership in software development, AI and microprocessor design;
- Strong academic research within our universities;
- Strongly competitive mobile and fixed networks; and
- leading edge service, finance and Net Zero industries.

not only to address the UK current vulnerable position, but also to enable the UK to regain leadership in Network Management and drive economic growth in this sector. In conclusion, we ask that Government in conjunction with wider sector/ other actors (industry, academia etc) :

1/ Facilitate a UK long term Vision to develop and leverage AI/ Automation technologies to improve and facilitate the management of highly complex networks

Back a truly long term (20 year) strategy of how telecommunications enable the modern economy, not just the automation of itself, but also the facilitation and automation of all industries that will require telecommunications [1].

[1] UK Government's Wireless Infrastructure Strategy

2/ Facilitate the creation of a set of industry specific requirements (connectivity, key value indicators etc.) including standards coordination.

Industry specific targeting. Creation of a cross industries & universities collaboration forum, to enable the sharing of Network Management knowledge, ideas, problems, and goals, to influence or create development and research areas. Where representatives from telecom networks, technology companies, universities, and other industries (Energy, Health, Logistics, Transport, Finance etc.) can work together to develop ideas and concepts that will develop Network Management capabilities for the wider benefit.

3/ Fund research focussed on scalable & robust Network Management tools & datasets

Including real world datasets for AI training, with associated development and test platforms. Government specific assistance, to incentivise and sponsor the creation of a sharing platform (or platforms) for time series data and large language model datasets for training new AI services from real-world network data. This recommendation will require the appropriate sponsorship from UK operators, both the academic and non-academic world should promote this.

4/ Support & Facilities for NM R&D and training of researchers, engineers in AI systems for NM automation.

UK based skills development. Government to invest in UK NM skills development to increase UK Security, Resilience, Reliability & Scale. A long-term investment in home grown skills pipelines to address the demographic challenge. Renewing this workforce and skill set is akin to training more doctors and nurses since Network Management pervades every part of our telecoms economy.

5/ Provide financial and other incentives to support investment in home grown NM capabilities and supply.

For example, with the provision of brokerage & Services, where bilateral agreements across all these agencies will not be feasible. Is there an opportunity for the UK to create companies as trusted telecoms service brokers? For example, for data exchange between telcos & techcos domestically and internationally for data insight services based on AI and experience operating networks, or for systems integration services based on open APIs and complexity management. We should aim to facilitate best practice from UK parallel industries e.g. London exchange, other Financial Services, Pharma, & Legal to support these brokerage services.

1/ Introduction

The experience demonstrated that a new mobile or fibre network technology is standardised approximately every 10 years. According to the TeleManagement Forum (TM Forum [2]), Network Operations costs form an average of 27% of the overall operational spend (Opex) by telecoms operators. This Opex spend is dependent on network management costs related to people and the system, among other component costs, and hence has a significant impact on the overall profitability of a telecoms operator.

This caused operators a huge challenge to their ability to manage new technologies and the co-existence between the networks. The ability to manage multiple networks directly effects the ability to grow an operator's revenue and customer satisfaction, and to control the underlying cost base. The complexity increases significantly as the networks and the interfaces become more open, e.g. through Open APIs and Open Networks (such as ORAN and CAMARA [3] (Open Gateway) which opens fixed networks and other elements). Automation will be the main contributor to reduce the cost in the network management towards "zero touch" [4] networks especially with multiple vendors, technologies, and standards.

One of the main objectives of this Future Capability Paper is to propose to the government actions to take to fill gaps in network management.

A large global ecosystem of system suppliers, integrators, and managed service suppliers (both insourced and outsourced) has developed to deliver network management. This ecosystem is valued at $9.5B in 2022 [5], and is supported by 10 major systems and component suppliers [6], and a large number [7] of providers (e.g. integrators, service providers).

This illustrates a level of diversity already, but the development of open interfaces and networks is seen as a key strategic step towards a level playing field. The UK Government, through DSIT, formerly DCMS, has supported this strongly for 5G [8]. In industry, or example, the Open RAN Alliance [9] has been standardising new interfaces to enable multiple vendors to interoperate to deliver services over 4G and 5G.

[2] Telemanagement Forum, 2024
[3] GSMA Open Gateway
[4] "Zero touch" management minimises operator intervention in network and service management processes, see e.g. ETSI's Industry Specification Group
[5] There are many inconsistent estimates published by industry analysts. PRNewsWire.com example
[6] Quote from PRNewsWire.com
[7] The number is not easy to find because the sector is so diverse. Example from LinkedIN
[8] UK Government, "5G Supply Chain Diversification Strategy", 7th December 2020
[9] Open RAN Alliance

Introduction

This Future Capability Paper reflects the preliminary discussions within the UKTIN NM EWG. The EWG members followed the following process which is reflected in the following sections:

1. Define the scope of Network Management.
2. Determine the major challenges impacting Network Management systems, processes, and skills over the coming 10-year period.
3. Determine the specific strengths, weaknesses, and gaps for the UK in Network Management.
4. Make initial recommendations for R&D focus and other areas to leverage the UK strengths, fill UK gaps and exploit any identified opportunities.

2/ What is Network Management (NM)?

The International Organisation for Standardisation (ISO) released the “FCAPS model” in the early 1980s. This traditional view of Network Management refers to the administration, monitoring, and maintenance of computer networks with FCAPS standing for Fault, Configuration, Accounting, Performance and Security. This definition has extended to also encompass planning, design, dimensioning and orchestration aspects of the plan-build-operate network lifecycle. It involves a set of activities and processes aimed at ensuring that a network operates efficiently, securely, and reliably. Network Management needs to evolve to provide service assurance and the guaranteeing of customer experience.

Network management encompasses various tasks and responsibilities, including:

- Configuration Management: This involves setting up and maintaining network devices (routers, switches, firewalls, servers, etc.) to ensure they function as intended. Configuration management also includes defining and implementing network policies and rules. Configuration management also now includes Orchestration of network functions, increasingly supported on cloud-based infrastructure.
- Performance Monitoring: Continuous monitoring of network performance to identify and address issues that can impact network efficiency, such as bottlenecks, latency, and packet loss.
- Security Management: Implementing security measures to protect the network from unauthorised access, data breaches, and other cyber threats. This includes setting up firewalls, intrusion detection systems, access control lists, and encryption protocols.
- Fault Management: Fault management can be Reactive or Predictive. Detecting and responding to network faults, such as device failures or communication errors, or predicting when they may occur in the future. Fault management aims to minimise network downtime by quickly identifying and resolving issues.
- Accounting and Billing: In some cases, network management may involve tracking resource usage and generating billing information for clients or internal departments. This is common in-service provider environments.
- Change Management: Managing changes to the network, such as adding new devices, updating configurations, and implementing new services. Proper change management practices help prevent disruptions and ensure that changes are well-documented.
- Topology Discovery: Mapping and documenting the network's physical and logical layout, including the connections between devices and the structure of subnets and VLANs.
- Traffic Analysis: Analysing network traffic patterns to understand user behaviour, application performance, and potential issues. This data can be used to optimise network resources and plan for capacity expansion.

- Bandwidth Management: Managing and optimising the allocation of network bandwidth (and wireless spectrum) to ensure that critical applications and services have the necessary resources, and that non-critical traffic doesn't degrade network performance. Scaling of the network up and down to meet current and predicted usage.
- Inventory Management: Maintaining an inventory of all network devices, software licenses, and configurations to facilitate troubleshooting and planning for network upgrades.
- Backup and Recovery: Implementing backup and recovery strategies for network configurations and data to ensure data can be restored in case of failure or data loss.
- Compliance and Documentation: Ensuring that the network complies with industry standards and regulations and maintaining comprehensive documentation for audits and troubleshooting.
- User Access Control: Managing user access to the network, including assigning user privileges, enforcing security policies, and ensuring that only authorised users can access specific resources.
- Remote Monitoring and Management: Utilising remote management tools to monitor and manage network devices, cloud infrastructure, applications, and configurations, which is especially important for geographically dispersed networks.

Automation in network management is crucial for maintaining a stable and secure network that meets the needs of organisations and users. It often involves the use of network management software and tools to automate and streamline many of these tasks, reducing manual effort and potential errors.

One aspect of automation is the capability to predict emerging impacts upon many of these processes, e.g. degradations leading to a solid fault or the need for more capacity to respond to increasing demand. Another is to protect human decision makers from an avalanche of alarms and statistics, many of which are routine. Artificial Intelligence (AI) is seen as an enabler of prediction through Machine Learning.

Network Management functions are usually enacted in a set in of software functions distributed between those built into individual network elements (e.g. switches, routers, and mobile core elements) and software in the Operational Support Systems (OSS) that an operator has in their IT stack. Generally, individual NM functions are exposed via APIs or other standardised interfaces such as SNMP for integration into the overall NM system. The trend is to adopt cloud-based technologies and the associated agile development techniques associated with them for OSS system development and network virtualisation. This is severely hindered in non-greenfield operators by the need to integrate with the legacy systems that have evolved over 20+ years.

3/ Current Technical Challenges & Trends

Managing networks has never been trivial, but it has historically focussed on the management of a single network, usually within one organisation, where each network component was physically managed by the organisation within its own physical sites, network equipment and data centres. This was true for both corporations and network operators. In that world, network management and analytic software and network topology were usually provided by the same organisation, who with a single ownership structure would be responsible for the whole product development, integration, and introduction into the network. Networks were traditionally deployed and configured manually onto each physical component with simplistic alarms that could be sent to the control room when issues occurred. These would then be manually analysed to resolution.

Today we can see technology and commercial trends that present increasingly complex technology and operational challenges right now with the existing state of the art:

- Diversity of technology, e.g. SDWAN, MetroEthernet operated over fibre delivering connectivity to consumers and enterprises using a variety of media on premises – WiFi, Ethernet, industrial Operational Technologies (OT); various mobile communications platforms – 4G, 5G, and variants for railways and vehicles; and eventual non-terrestrial networks.
- Diversity of service, e.g. legacy voice, voice over Internet, enterprise VPNs, private networks (Non-Public Networks), broadband Internet access, virtual networks in a multi-tenanted infrastructure.
- Moving to a cloud-first infrastructure and the rise of hyperscalers as CSPs to facilitate virtualisation of core delivery and management functions. The 5G Service Based Architecture is a topical example.
- Outsourcing, to specialist organisation in all aspects of the supply chain from app development, security, design, build and operation. Corporates often no longer own the physical networks, and in many circumstances do not have visibility or knowledge of the end-to-end supply chain of the network. This may apply to service providers as well, e.g. MVNOs.
- Sharing of technology and infrastructure such as Neutral Host networks.
- Federation of networks and services, requiring common service level specifications and open interoperable interfaces.
- Building and integrating the most cost-effective regional networks, such as Alternative Networks [10], rather than utilising a single country wide network.
- Splitting operators into “Servcos” and “Netcos” to optimise ROI. Here the Netco has the operator’s infrastructure and may offer wholesale services to multiple Servcos.
- Sustainability and efficiency, e.g. minimising energy costs and maintaining the corporate ESG agenda.

[10] Otherwise known as “Altnets” but also including Neutral Host and Tower operators in this category

- Creating diversity in the supply chain and competition from a macro level down to a component level, such as Open RAN initiatives.
- Moving to alternative business models and the evolution of some Telcos to Techcos, e.g. where the organisation who receives the most benefit pays (e.g. the drive from networks for the OTT service providers to pay or, in the mobile world, enterprises or cities paying for mobile coverage).
- Sweat existing assets and sunk costs by integrating legacy networks and systems into future systems.
- Organisational focus has moved to providing the best end user experience, through aggregation of best-in-class services to meet the organisations' bespoke needs.

To consolidate this fragmented collection, the technological challenges to be faced today fall broadly into 4 categories -- scale, multiplexity, dynamicity/elasticity and heterogeneity/interoperability -- which we detail below. It is imperative that research and innovation be directed at tackling them so that contemporary and future networks are operated in an efficient [11] and secure way.

- Scale of network and service infrastructure: The most obvious challenge in managing today's networks and services is their sheer scale. For example, in the past decades, we have seen hyper-scale data centres being deployed, supporting link speeds of 100Gbps and 400Gbps, thousands of network switching devices and interconnected servers, and providing core services to businesses and end-users. IoT deployments are forecasted to scale to billions of devices and supporting networks will need to provide efficient and secure managements. Low-earth orbit satellite networks will consist of tens of thousands of orbiting routing devices providing global network coverage and feature an aggregate bandwidth in the order of hundreds of Tbps, comparable to today's aggregate fibre capacity.

  A direct consequence of the ever-increasing scale of the underlying systems is the explosion in the data that one can extract from a network deployment to support its management. Data itself can be raw metrics, aggregated information, or higher-level events/alerts. At a typical large enterprise network, the event rate is 135 million events a day, whereas there are just a few hundred 'actionable incidents' [12] . This, of course, poses a substantial strain in management systems, in terms of the required processing power, storage space and energy required to monitor, store and transform those into actionable insights for a network or service provider. Moreover, it also adds multiple layers of complexity in terms of navigating data and insights into the day-to-day operation of networks rendering networks and services much less observable than in the past.

[11] Here, efficiency is defined in a multi-faceted way, encompassing resource utilisation, cost, and energy.
[12] IEEE Document, Vertex Entropy As a Critical Node Measure in Network Monitoring

- Multiplexity: Modern network deployments are very much in line with the 'multiplex' definition in network science where the same set of nodes are linked by different types of interaction.

  In practice, this means that there are both known and latent interdependencies amongst network devices, protocols and running services that commonly form different 'network' topologies; examples of such topologies include ones directly linked to a network layer and respective protocols (e.g., a layer-3 topology [13], or a call graph of microservice instances [14]), all running as applications.

  Importantly, multiplexity in topologies could include latent interdependencies amongst different component types in a network (e.g., hardware, protocols, running services, load balancers and in-network middlebox functionality) which, at first sight, are not part of a coherent structure and as such might not be naturally subject to monitoring, but may interact when specific conditions are met (e.g., failure/error, malicious attack, software bug) with potentially catastrophic results [15].

- Dynamicity/Elasticity: With the advent of software defined networking (SDN) and network function virtualisation (NFV), often based on cloud based micro-services, that are self-scaling and based upon containerisation technology (such as Kubernetes), resulting in the fact that the network and its underlying components are no longer static. Networks themselves have changing configurations, adding and removing paths and components as the traffic, security and protection demands change.

  This results in networks being extremely dynamic with (physical and virtual) connectivity formed and dismantled at different timescales; examples of such dynamicity include mobile devices connecting to different Wi-Fi and cellular base stations, forwarding paths being setup by OpenFlow [16] and P4 [17] programs in response to dynamic policies or, at the extreme, TCP connections, micro service deployments being reconfigured. Virtual network functions and any other services supported by a network can be scaled up or down, in an elastic, on-demand fashion, according to current load and user preferences (e.g., to support anomaly/intrusion detection, or load balancing).

[13] The paths that information will take (a routing topology) created by routing protocols that discover the optimum connectivity between interconnected neighbouring switching nodes)
[14] Determining the connectivity and information flow relationships between microservice instances is a topic for research, e.g. https://www.computer.org/csdl/journal/td/2022/12/09774016/1DjDsGch5a8, as well as an immediate practical problem to be solved, e.g. https://codescene.com/blog/visualize-microservice-dependencies-in-team-context/ or https://neo4j.com/blog/fixing-microservices-architecture-graphconnect/.
[15] USENIX.org Presentation, Metastable Failures in the Wild
[16] OpenFlow is a network communication protocol used between controllers and forwarders in an SDN architecture, see for example:
[17] Programming Protocol-independent Packet Processors (P4) is an open source, domain-specific programming language for network devices, promoted by the Open Networking Foundation.

Network Management will therefore need to adapt to configuring and managing ever changing networks in real-time.

- Heterogeneity and Interoperability: Contemporary network deployments can be seen as a collection of interconnected hardware, firmware, and software, all working together to provide connectivity and services to end-users. For example, a network may span and need to support legacy and current technologies seamlessly. This diversity of technologies is likely to include:
  - Mobile (2G, 3G, 4G, 5G and soon 6G)
  - Open Networks and interfaces as standardised by ORAN Alliance
  - Corporate office LANs and Wide Area Networks
  - Fixed line fibre, copper services delivered through multiple ISPs
  - Cloud based networks and network elements (e.g. firewalls, policy, load balancing, DoS and security protection, and identity management).
  - Edge and distributed compute
  - Public and Private Networks

Heterogeneity is inherent to networks not only because of the diversity of the components comprising a network, but also because of the plethora of manufacturers of hardware, software and service providers and the fact that networks have been running (and still do) many generations of hardware, firmware, and software.

Contributing to this, there has been a multitude of monitoring and management systems (standardised and proprietary, general-purpose, and deployment-specific), operating in parallel and in tandem to provide management services to network and service operators. The most significant development was the standardisation of RAN Intelligent Controller (RIC) by the ORAN Alliance to manage multiple vendors with standard interfaces. Interoperability is a key challenge that is directly related to heterogeneity; specifically, devices, firmware, software, and management systems from different manufacturers/providers, standardised or proprietary, legacy or contemporary must all work together to support efficient and secure operation of a network deployment. On top of that, interoperability is also particularly challenging in relation to the diversity in the network and service provision ecosystem. More specifically, network management should be operational in environments where multiple stakeholders operate network devices and services and where full observability may not be inherently possible.

In summary, networks are now, and will continue to become highly complex and dynamic across multi-network and technology environments. The future of Network Management will be characterised by increased automation, software-defined approaches and scalability whilst addressing security concerns.

4/ Future Telecom Trends

The response to the challenges and trends outlined in Section 3 is already creating the key technology trends that will influence network management over the next 10 years. Some are already mature and will lead to significant innovation. Others are the subject of continuing research and development. These include:

- Open Networks/APIs: will introduce new infrastructure suppliers into the eco-system which will require a centralised platform to manage multiple technologies and suppliers' equipment. APIs come with multiple areas of application e.g. for service application development to expose Network-as-a-Service (NaaS) functions, inter-operator or inter-domain and intra-operator.
- Multi-Cloud Environments: As more organisations embrace multi-cloud strategies, network management will become more challenging. Coordinating and optimising network traffic across different cloud providers and on-premises infrastructure will be essential.
- Edge Computing: With the rise of edge computing, network management will extend to edge devices and edge data centres. This requires new approaches to ensure low latency, reliability, and security at the edge.
- Security and Compliance: Security will remain a top concern in network management. As networks become more complex and distributed, ensuring the security and compliance of data and applications will be a constant challenge.
- Zero Trust Network Access (ZTNA): ZTNA is an evolving security model that assumes no trust within the network and enforces strict access controls. Implementing ZTNA will be crucial in securing complex network environments.
- 5G, 6G and IoT: The rollout of 5G and the proliferation of IoT devices will introduce new requirements for network management. These networks will need to support massive numbers of connected devices and ultra-low latency applications.
- Network Slicing: Network slicing is a technology that assists operators in building and manage a network, that meets and exceeds the emerging requirements from a wide range of users. The way to achieve a sliced network is to transform it into a set of logical networks on top of a shared infrastructure. Each logical network is designed to serve a defined business purpose and comprises of all the required network resources, configured and connected end-to-end.
- Neutral Hosts: Shared infrastructure utilised by more than one network operators;
- Alt Nets: An alt-net is a company that builds its own independent telecommunications network an alternative network to the national incumbents. Often on a regional basis.
- Containerization and Microservices: With the adoption of containerization and microservices architecture, network management will need to adapt to support dynamic and ephemeral workloads.
- Hybrid and Multi-Network Environments: Organisations will increasingly rely on a combination of public and private networks, creating a need for effective management across multiple network types.

- Hybrid and Multi-Network Environments: Organisations will increasingly rely on a combination of public and private networks, creating a need for effective management across multiple network types.
- Supply Chain Security: Organisations (and countries) will demand multi-vendor approach, to ensure that vendor lock-in is avoided and that as the world destabilises no country is dependent upon technology from a single country or organisation. In addition, supply chain security could be extended to also take into consideration the risk of opensource or 3rd party software libraries incorporated into network equipment being insecure/compromised as was the case in the "SolarWinds incident" [19].
- "Network Softwarisation" is a network architecture that separates the software implementing network functions, protocols and services from the hardware running them. It has been motivated by technologies like network function virtualisation and software-defined networking, which is radically changing the way communication infrastructures are designed, programmed, integrated and operated, enabling rapid and innovative service creation with easy deployment and opening the door to a faster pace of innovation, particularly for application of Artificial Intelligence in the design of Autonomous Networks. This builds on the existing Software Defined Network (SDN) functionality.
- Network Automation & Zero Touch Network Management is a hot topic in telecoms networks, driven by the need to lower operational costs, make up for skills shortages and deal with the customer expectations in an environment of increasing service and network complexity. Automation is a progressive objective with certain priority processes and procedures being implemented first and others added once confidence is built. Extensive automation is only now possible because of the softwarisation, AI and OpenAPIs along with the development of standardisation frameworks such as ETSI ZSM - zero touch network management.

  Another challenge is the complexity of integration of open networks. No single vendor may feel responsible for performance – the burden will be on a systems integration to make sure system is meeting expectation.

  The TM Forum [20] has produced an autonomous network maturity. This model defines six levels of autonomous networks:
  - L0 – Manual management: The system delivers assisted monitoring capabilities, which means all dynamic tasks must be executed manually.
  - L1 – Assisted management: The system executes a certain prefigured repetitive sub-task to increase efficiency.
  - L2 – Partial autonomous network: The system enables closed-loop operations and maintenance (O&M) based on an artificial intelligence (AI) model for certain units in certain environments.

[19] WIRED Article by Kim Zetter, The Untold Story of the Boldest Supply-Chain Hack Ever
[20] TMForum.org

- L3 – Conditional autonomous network: Building on L2 capabilities, the system can sense real-time environmental changes, and, in certain network domains, optimise and adjust its operation to the external environment to enable intent-based closed-loop management.
- L4 – Highly autonomous network: Building on L3 capabilities, in a more complicated cross domain environment, conducts analysis and makes decisions based on predictive or active closed-loop management of service- and customer-experience-driven networks.
- L5 – Fully autonomous network: The goal for telco network evolution. The system possesses closed-loop automation capabilities across multiple services, multiple domains, and the entire life cycle.

- Artificial Intelligence (AI): is a vital and promising technology that can optimise performance in a dynamic environment in the field of mobile communication systems. With the increasing inefficiency and cost of traditional techniques of operation and administration in complex network infrastructures, a change towards more intelligent ways is necessary. The primary objective is to develop a comprehensive framework for the integration of Artificial Intelligence (AI) into mobile communications, with a focus on achieving total autonomy in the context of 5G and 6G networks. The means by which this can be achieved is by applying OAI, FlexRIC, xApps and rApps using Containers managed by Kubernetes [21]

Most operators are currently either at L2 or L3 on this model for Network Management. An example is Orange which considers itself to be at "L2 on average" [22].

A more detailed discussion of future network technological trends, discussed in the group, is contained in Annex A of this document.

[21] Kubernetes: is a portable, extensible, open-source platform for managing containers and services, that facilitates both declarative configuration and automation. It has a large, rapidly growing ecosystem. Kubernetes services, support, and tools are widely available.
[22] TM Forum Article by Michelle Donegan, Orange sizes up the network automation and monetization challenge

5/ The Challenge of Customer Experience Management

Customer Experience Management (CEM) in network management refers to the practice of monitoring, analysing and optimising the customer experience as it relates to network services and connectivity. It is a critical aspect of telecommunications and network service providers operations. Operators who successfully manage their networks for a customer experience viewpoint will be the most successful in the future and hence techniques and tooling to provide a Quality of Experience (QoE) / Quality of Service (Qos) view are becoming critical to an operator's profitability.

According to a recent McKinsey report [23] "Within six months of the first successful pilots of proactive and preventive interventions, customer satisfaction scores rose 15 points and churn fell 40 percent". Many of these interventions are likely driven from analysis of CRM systems and Network Management derived data.

The quality of the customer experience is fundamental to business success. It will directly impact that business's ability to deliver services to its own customer base meaning that customer satisfaction, loyalty and overall accessibility and connectivity at point of need are items that transcend all supplier and customer layers in network management.

By contrast, poor quality of customer experience will lead to customers finding work arounds to network issues, often creating operational inefficiencies which can result in poor onward customer service, ultimately leading to business failures and higher dissatisfaction rates.

As the number of technologies and vendors increases in a network, the interoperability between them becomes more challenging. As a result, the network performance will suffer, especially along the network boundaries, unless a centralised network management system is deployed. There are systems available such as Customer Experience Management (CEM) and Network Automation using AI to improve the network performance.

[23] McKinsey and Company – Winning in Customer CX - April 2023

Customer Experience Management

The key aspects of CEM in network management are:

- Monitoring Network Performance: Monitoring tools and software are used to ensure that the network is performing at an optimal level. These tools will track metrics such as network latency, packet loss, bandwidth, and availability.
- CEM Driven Network Optimisation: CEM involves optimising the network to meet a business intent which focussed on the needs of the customer e.g. a specific QoS/QoE. This can involve re-configuration expansion, capacity or upgrades and deploying new technologies.
- Real Time Monitoring: Monitoring needs to be real time, to identify and repair issues as quickly as possible.
- Proactive Issue Resolution: CEM focuses on resolving issues before they impact the customer, including identifying problems before they become critical and using analytics to identify maintenance and upgrade requirements.
- End to End Visibility: CEM emphasises the need for end-to-end visibility into the network, understanding how service, access and data flows from the service providers network to the customers devices.
- Quality of Service (QoS) Management: Quality of service parameters will ensure applications and services are given appropriate resources and priority within the network. It's important to understand both the customers mission statement and their prioritisation schedule for applications and services, knowing these will aid with other aspects of CEM as detailed above for example video streaming, VoIP telephony. Specific service models evolving from Network Digital Twins can be used to model and evaluate the customer service, and these can evolve to model the customer's perception of the service being received.
- Service Level Agreements (SLA's): These outline the expected level of service quality to customers and stakeholders. These metrics are monitored to ensure the network is behaving in line with customers' expectations.
- Customer Feedback, Support and Complaint Resolution: These functions are intrinsically linked and analysing complaints, concerns, together with data analytics can lead to improvements and improved customer experiences.

Improvements in Automation and AI mean that vast volumes of network performance data can identify trends and patterns in network performance. RPA, AI in Network Management: Service providers can now utilise these tools to make data driven decisions and improve the customer experience. This is therefore an ever increasingly important part of CEM.

[23] McKinsey and Company – Winning in Customer CX - April 2023

5.1/ CEM Factors Driving Network Management Evolution?

CEM needs to adapt from managing the boxes of the singular organisational type network to managing the experience in the evolving models of network management. The adaptations will enable the following question to be answered: “What does the customer need to manage their experience?”

It must focus too on minimising the gap between quality of service versus the quality of experience, with potentially a key question becoming “What does the customer need to manage their experience?”

The current market position:

- UK Network Providers continue to embrace outsourcing and service models, service desks, planning and management teams are often based abroad. UK customers then feel the impact of language barriers and other nuances which lead to delays in responding to network incidents. the effect is lower quality customer experience for UK based customers and lack of access to the required skill set at the required moment in time.
- Security, theft of intellectual property rights and technology is a risk, with so much network management performed overseas unauthorised access and its effects becomes a clear concern for key network infrastructure in the UK.

As Networks move away from being independent, singularly organisational in nature towards interoperable cloud based and highly complex structures, the role of the customer is also changing:

- End User: Often the primary customer who relies on the network to access services, applications and data to perform required business functions and processes.
- Network Administrators and IT Services: This customer’s objective is maintaining network availability and connectivity to end users. This function is often duplicated across both customer and supplier functions.
- Third Party Vendors and Supply Chain: Network management invariably relies on relationships with third party vendors and supply chain to supply services and components of the network. These services can be operational in nature such as service desks for escalation of network issues, network engineering resources, software, hardware, environment, power.
- Regulatory Authorities: Enforcement bodies and ultimately the Government are also customers since they can set legal requirements and enforce rules and standards in network management. There will invariably be an overriding concern for security and integrity of the networks of UK plc.

The line between a customer and network services provider (supplier) is blurring constantly and potentially only defined now by contractual arrangements rather than technical restrictions. A supplier can be both a customer and consumer at the same time in the ever more complex network management space.

The future evolution requirements to achieve the required changes include:

- Integration of Real-Time Data: Using data analytics and AI to process and analyse vast amounts of data in real time can help predict and address issues before they impact customer experience. The evolution of the "Network Digital Twin" models to include other factors and data inputs such as social media or behavioural data elements plus the addition of AI-based analyses is one way to more accurately evaluate real-time QoS / QoE in a network management system.
- Proactive issue resolution: Resolving issues before an impact is felt will greatly enhance overall customer satisfaction. Here use of AI is central to the move from predictive to pro-active resolution.
- Customer education: Educating customers and proactive communication about changes in the network can empower customer decision making for their own business processes.
- Personalisation and environment: Take into account individual customer preferences, behaviours and historical interactions. Some customers will simply want access on demand and have no desire to understand any of the mechanics of how the network works, others will want visibility of the network and an input into decision making.
  It will also be crucial to understand the customers environment, network conditions at the time, end point devices to deliver tailored experiences and manage the experience.
- Multichannel Support, Agility and Responsiveness: Support experience should be seamless across multiple channels and will play an important role in ensuring customer satisfaction with their experience.

This will go hand in hand with the requirement to be agile and responsive building in change management processes that are fit for purpose, while keeping customer experience at its centre.

6/ The Open Network Management Opportunity

The topic of Open Network Management spans Open-Source Software, Open Standards and Interfaces (protocols or Application Programming Interfaces (APIs)), through to the Automation and Orchestration of a multi-vendor network. Although a degree of standardisation exists, each equipment supplier has its own network management solution. If a network operator has multiple equipment suppliers, multiple technologies and multiple networks, network management complexity increases exponentially. The volume of data that is generated cannot be processed by people.

Open Network Management platforms address the issues by centralising and automating control of network components using AI/ML, reducing complexity and delivering cost efficiencies which will reduce the chance of human errors through data overload. Open Interfaces play a significant role in this transformation by enabling networks with all kinds of different technologies, standards and vendor equipment to easily connect to the centralised management system.

Benefits include:

- Increased Innovation: Open interfaces and communities encourage agile development, enabling the quick adaptation of mobile networks to the evolving application and user demands.
- No Vendor Lock-In: Breaking free from proprietary solutions allows operators to mix and match components, choosing best of breed and avoiding vendor lock-in or bespoke solutions.
- Operational Efficiency: Automation tools, built on Open APIs, streamline network operations, reducing costs and minimising manual configuration or optimisation
- Better Network Insight: Open Interfaces and Orchestration tools empower operators with deeper insights into network performance and resource allocation.
- Encouraging convergence with other future networks: Supports the de-layering of telecoms network provision e.g. the Servco/Netco/Infrastructure-co/Neutral host split and the APIs in the open ran approach should mean simpler future integration with NTNs.

The Open API/Network Specifications define standards which allow developers to build applications without accessing to the source code such as Open RAN, Open API. The specifications define the interactions between the use cases and the API i.e. requested and returned information. Several industry bodies are addressing the need for Open management systems; OSI, Open RAN Alliance [24], TM Forum, Open API [25], GSMA Open Gateway [x], Linux Foundation CAMARA [x], ETSI MANO [x], 3GPP [26] etc. The standards bodies are also collaborating for alignment [27].

[24] OpenRAN.org
[25] CSPs see CAMARA collaboration as a model for standards (tmforum.org)
[26] 3GPP.org article by Lionel Morand, OpenAPIs for the Service-Based Architecture
[27] Open API v3.1.0

Open Network Management

Open Networks/APIs will play a significant role in diversifying the composition of telecommunication networks.

Adopting Open Interfaces can introduce new security challenges in comparison with closed systems. There is, however, a trade-off. While openness can expose vulnerabilities, it also fosters transparency, quicker patching, and strong community support, all of which can enhance security. Ultimately, the security of an open interface depends on its implementation, including adherence to standards, best practices operationally, and commitment of its users and their organisations. Regardless of whether an interface is open or closed, a comprehensive approach to security is always crucial.

Another challenge of Open Network Management platforms can be the perceived lack of features and maturity versus traditional closed or single-vendor platforms. While this may have been relevant in the early stages, industry adoption of initiatives such as Open-Source MANO, Open RAN , ONAP and Open APIs has resulted in a strong and active community developing these solutions. This openness fosters a collaborative and innovation culture, which accelerates development and feature parity. Efforts such as the Telecom Infra Project (TIP) bring vendors and operators together to further develop standards and promote interoperability.

There are currently a large number of ORAN interoperability testing projects taking place globally. For example, recently, DSIT funded projects [28] to stimulate the ORAN eco-system. Some of them could be summarised as follows:

- SCONDA, will deploy Mavenir's ORAN equipment in Three's commercial network in Glasgow. P.I.Works' RIC will manage the interoperability, mobility between legacy and ORAN hybrid networks to demonstrate that both networks can co-exist by use of a RIC based centralised network management.
- With Open RAN (Radio Access Network), Navigate (London), the project seeks to validate that the chosen blueprint is technically and operationally viable, demonstrably more cost-effective and energy efficient compared to legacy Single Operator RAN Macrocell approaches. NEC Europe Ltd. is a lead partner to provide Open RAN solution while Freshwave Services Ltd. is the neutral host partner in this project.
- Cambridgeshire Open RAN Ecosystem (CORE) seeks to stimulate innovation and encourage new players to enter the UK market by proving Open RAN in a real-world HDD test environment.
- The 'Sunderland Open Network EcosysTem' (SONET) Project is poised to transform the way we engage with live sports and esports. the project will showcase a highly efficient, state-of-the art High-Density Demand (HDD) Open RAN solution at the Stadium of Light and the new British Esports Arena, part of the National Esports Performance Campus in Sunderland.

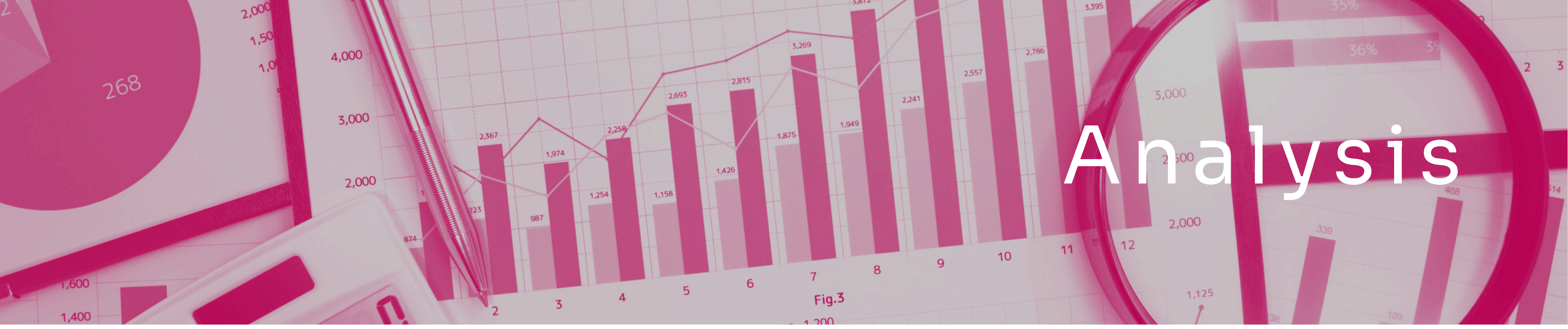
[28] Successfully funded Department of Culture, Media & Sport (now DSIT) Projects

- 5G MoDE (Mobile oRAN for highly Dense Environments), seeks to revolutionise how we manage dense mobile network traffic using Open RAN. This provides a robust, high-capacity connectivity without the need for permanent infrastructure. Mavenir, VMware and University of Surrey are working with lead partner VMO2 to deliver this.
- SmartRAN Open Network Interoperability Centre (SONIC) Labs initiative already delivered end-to-end testing with a number of telecom equipment vendors and their products in various ways to better understand the challenges and possibilities of Open Radio Access Network (Open RAN). The continuing project includes several cohorts to demonstrate the ability to interchange Open RAN vendors in RAN, RIC and network management areas.
- There are also other projects like the FONRC (REASON, TUDOR) that are looking into NM for multi-domain environment, NTN etc.

In summary, Open Network Management has the potential to revolutionise the way networks are designed, built and operated. As the industry continues to adopt these technologies, their maturity increases, and the eco-system grows. Open Network Management platforms empower operators to unlock intelligent network operations and fuel unprecedented business agility. This key technology paves the way for:

- Enhanced Network Performance: Optimised resource allocation by using real-time network data and AI-powered algorithms to efficiently distribute resources, dynamically adjusting to traffic demands and user needs. This translates to improved network performance, reduced congestion, and lower latency.
- Automated network healing: Granular visibility into network performance, allows operators to pinpoint and resolve issues proactively, minimising downtime and disruptions. Self-healing mechanisms ensure ongoing optimal operation, dramatically reducing manual intervention and maintenance costs.
- Streamlined network operations: automating manual tasks, simplifying network management and orchestration. Thus, reducing operational expenses while freeing up valuable resources for strategic initiatives.

And, importantly for network operators in the current commercial climate, Open Network Management platforms enable new revenue streams. They allow operators to deliver innovative service offerings, allowing them to create and offer customised connectivity solutions for enterprises, verticals like automotive and healthcare, and emerging applications like AR/VR. Also, there is the opportunity for (ethical) data monetization. The wealth of network data collected by the management platform and available via Open APIs can be analysed and turned into valuable insights, which can be m through targeted advertising, personalized service recommendations, and Network As A Service (NaaS) offerings.



7/ Analysis of UK Network Management Position

This section discusses the current capability for Network Management (NM) in the UK and potential opportunities that may be apparent based on the discussion and challenges discussed earlier in this Future Capability Paper.

It should be clear by now that the scope of NM is wide and there are many future technical, operational, and commercial challenges in the next 5–10-year period. Telecoms infrastructure cannot operate without NM, so nearly every new telecoms initiative or project needs a NM element as part of it.

The challenge for the UK is to focus on those projects which leverage or develop specific NM competencies or solutions which exploit specific UK capabilities or strengths.

A key question to be asked across all the identified opportunities described below is:

- Are we exploiting/using R&D outcomes in the right way? E.g. is all this research effort going to be translated into specific monetised UK benefits or be lost, maybe with some knock-on to international standards or open-source projects that benefit all?

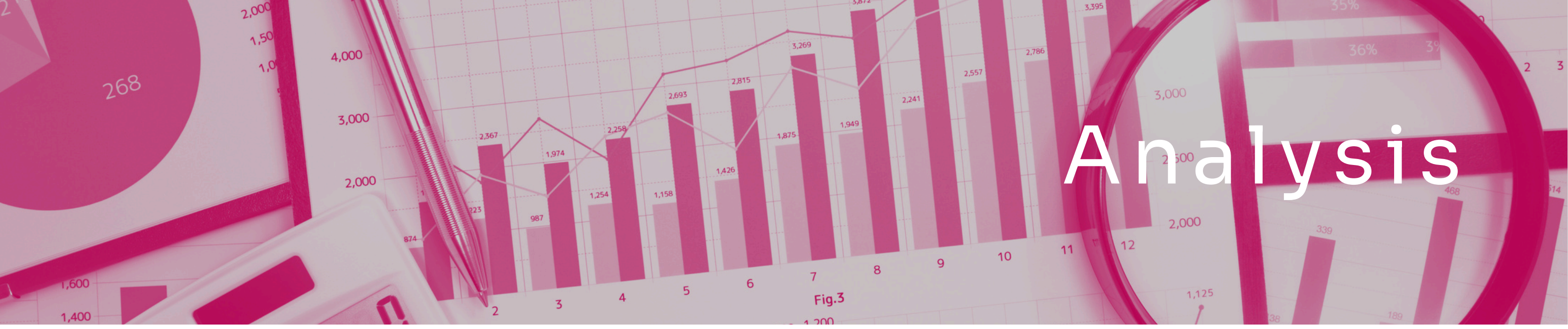
7.1/ Research & Innovation

7.1.1/ Current Situation

The UK is a centre for advanced telecoms research focussed on a core of universities but less so in the commercial sector. Notable universities involved in telecoms research include Bristol, Brunel, Surrey, Strathclyde, Glasgow, Sussex and UCL. Many of the research projects involve NM as part of the solution although arguably few are primarily focussed on NM as the main objective.

Many R&D projects involving ORAN, many funded from government initiatives, tend to include NM elements in the form of the RIC integrations, and many are including AI and automation as part of the solutions. The DSIT sponsored Open Networks Ecosystem (ONE) set of projects and ESPRC projects (TITAN, JOINER and HASC) has significant content for the deployment of AI and Apps for the ORAN environment. Also, the DSIT funded REASON project, which includes Universities of Bristol, Belfast, KCL, Southampton, and Strathclyde, together with others including Digital Catapult and Real Wireless as a consortium, seeks to develop multi-domain orchestration across multiple network domains. The same can be said for TUDOR including Non-terrestrial Networks, led by University of Surrey.

Of other notable academic research, “Rethinking large-scale network management through the lens of neuroscience - University of Sussex” covers the application of neuroscience to the management of telecoms networks.



The UK's recent re-joining of the EU Horizon R&D initiative may open the opportunity for more NM focussed NM R&D particularly centred on the application of E2E orchestration/APIs and AI assisted automation, as well as vertical integration, ie customer experience evaluations in large scale trials.

One specific gap in R&D is in the development of digital twins for the translation of network telemetry information into a true representation of the customer experience for the service being delivered. A good example outside the UK is Japan's IOWN [29] programme which has digital twins at its core. Also UK R&D platforms such as the University of Bristol Reality Emulator [30] could play a part.

From a commercial aspect the level of NM R&D activity is patchy and reflects the decline in telecoms suppliers in the UK over the last 20 years. This activity can be broken down into three areas:

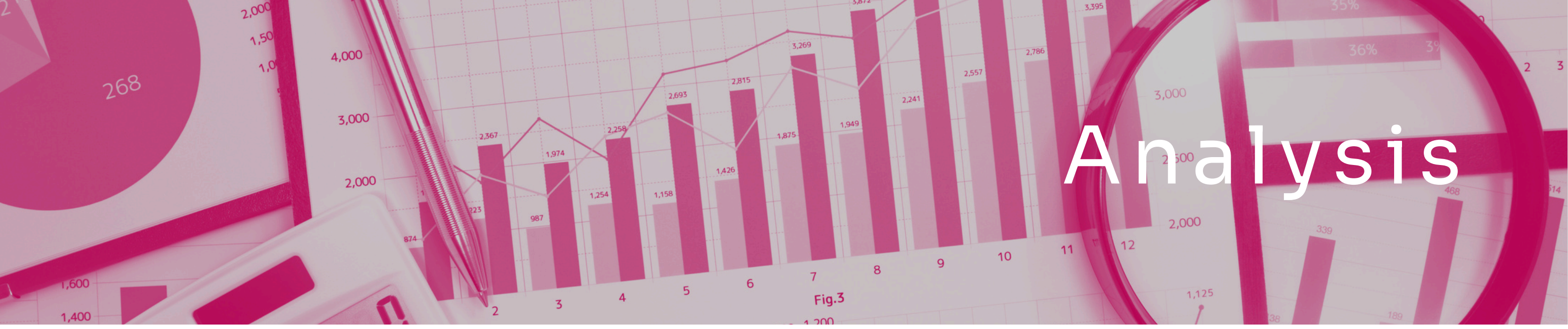
- Telecoms Operators.
- Large Multinational Technology Companies In UK.
- Small Number of SME Software Suppliers

Although, historically, the UK has strong initiatives for setting up SMEs, there is more focus required to encourage and help the transition from research into successful SME. Comprehensive academic research stays at universities which do not translate into commercial products.

Over the last 30 years the UK has created notable start-ups delivering solutions in the NM space –Micromuse (Fault Management), Orchestream (Provisioning), Cramer (Inventory) to name three. These are all now absorbed into large, foreign-owned, companies, respectively IBM, Oracle, and Amdocs. There is still a residual development presence in the UK from this, though the trend is to move software development to Asia where development costs are lower. Several large multinationals have large R&D facilities in the UK (for example IBM and Microsoft) where some AI related R&D work is carried out, but telecoms is not the prime focus of these sites. Moogsoft, a medium-sized NM supplier, which is now part of Dell, has been funding R&D in UK universities, which sets a great precedent for other similarly sized companies.

As a 3rd party independent Centralised Self Organising Network (cSON) automation tool vendor, P.I. Works has large number of cSON deployments in the UK networks and globally. The tool collects measurement data from the network with multiple vendors and using sophisticated algorithms self-heals the issues in the network. cSON with the introduction of RIC is currently available today to manage both hybrid, legacy and ORAN networks seamlessly.

[29] DTC White Paper
[30] Bristol Digital Futures Institute, Reality Emulator



A few niche NM suppliers are emerging with development focussed on areas such as analytics, network slicing management and physical inventory, but these are very small on a global basis (even when compared to NM only suppliers). Examples here are ORI [31] -- for Hybrid Cloud / Service Orchestration and Zeetta Networks for network Slicing and private networks management.

Telecom Operators have some residual R&D in UK, e.g. BT, but, for most of the others, any research is carried out outside the UK and most of the innovation carried out by third-party suppliers or systems integrators mainly overseas.

7.1.2/ Opportunities

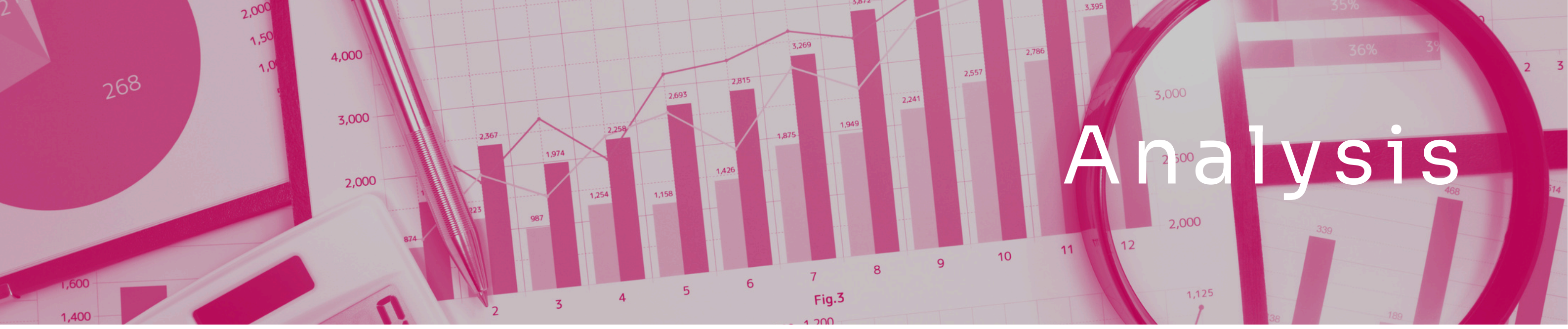
Despite the patchy picture presented in the previous section there are many opportunities for the UK to make a beneficial contribution to the NM R&D space over the next 5-10 years.

Some UK opportunities in NM or adjacent technology R&D are:

- Highly qualified engineers, innovative thinking, entrepreneurs pushing boundaries; large profitable operators (group argue that they might not be profitable) that are respected both globally, and for their leadership in research. We can utilise this power in influencing standards.
- The UK is one of the leading nations in emerging technology research. DSIT is funding technology trials and innovation such as security, AI, the ONE competition, and historically 5G testbeds and trials to improve the eco-system and accelerate UK based companies.
- The UK has many research centres capable of developing centralised AI driven automated open network management systems using Big Data collected from multiple networks with different standards and technologies. They can be used subsequently to influence standards bodies
- The UK is the leading country in network security and well-established practices to protect networks and critical services. This know-how is crucial to protect open networks.
- Furthermore, UK has strong and influential network operators, which can help collaboratively develop Open Network Management systems with the research centres.

From the above the Expert Working Group has identified the following more specific opportunities for UK research into NM that should be prioritised. Annex A describes several topics that expose R&D challenges for NM in more technical detail.

[31] ORI.co



7.1.2.1/ Automation & AI

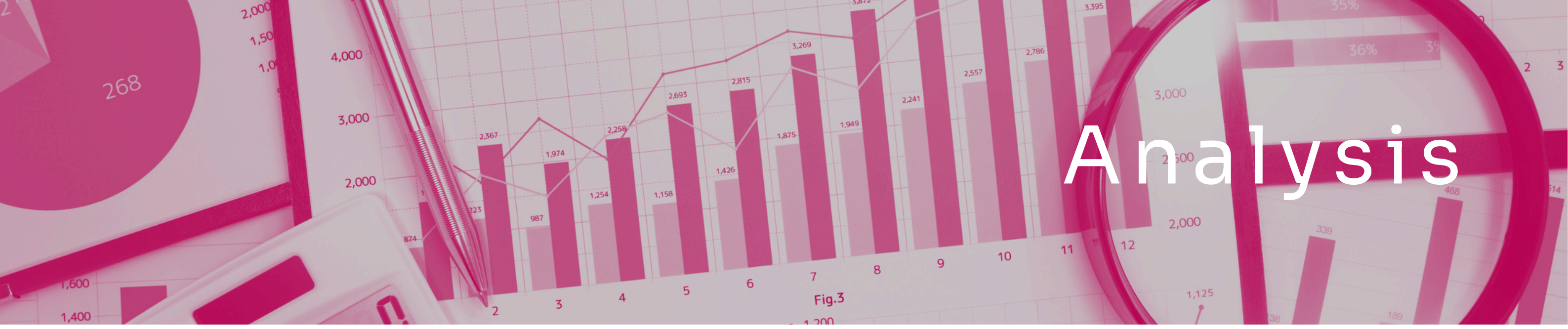
Automation will play a crucial role in network management. Self Organising Network (SON) is operational today in various networks in the UK and globally. Some of the automation use cases for SON are:

- Code and RAN parameter Optimisation;
- Capacity and Coverage Optimisation;
- Load Balancing;
- Energy Saving;
- Network configuration; and
- Slice Management.

The SON uses the network measurements 24/7 from the OSS. SON's complex algorithms identify problems and resolve them automatically. This is the first step towards 'Zero Touch Networks' eliminating human interventions. As a result of automation, problems could be resolved faster more correctly reducing the cost for the operators. Automation is one of the most important element of 'intend-driven' networks to enable automated orchestration of services. A centralised SON plays a crucial role in multi-vendor networks today by transforming multiple network management systems into an equivalent single network management system. cSON collects measurements from each vendor's OSSs 24/7 and takes necessary actions to resolve problems by considering inter-vendor relationships in the whole network. Centralised solution is important in the introduction of ORAN technology with multiple vendors.

Today, Three UK and P.I. Works are working with other partners funded by DSIT, to deploy a centralised RIC solution to automate network management of Three's legacy network with multiple vendors (Samsung, Huawei, Ericsson) and the new ORAN vendor Mavenir in Glasgow. There will be live customers in the network during the project which will represent a real use case for other operators to realise the viability of ORAN technology deployment over their existing commercial networks.

With the advent of AI and ML, networks will become more self-healing, self-optimising, and self-configuring. AI algorithms can predict and proactively address issues, further reducing manual intervention.



AI will be key to developing automated processes such as:

- Forecasting traffic and high traffic, hot-spots in the network to take actions before congestion occurs;
- Network discovery, design and auto-configuration;
- Capacity management, self-scaling and maximising the efficient use of resources;
- Anomaly detection and diagnosis, to monitor customer experience and drive incremental improvements;
- Automated fault diagnosis and self-healing, with the optimal focus on pro-active pre-healing; and power and cost management. (please see the UKTIN NM EWG Future Capability Paper Appendix A/2 for more information on use cases)
- Development of Retrievable Augmented Generation (RAG) methods to enable NM specific large language models to be continuously updated for better accuracy and support cost effectiveness.

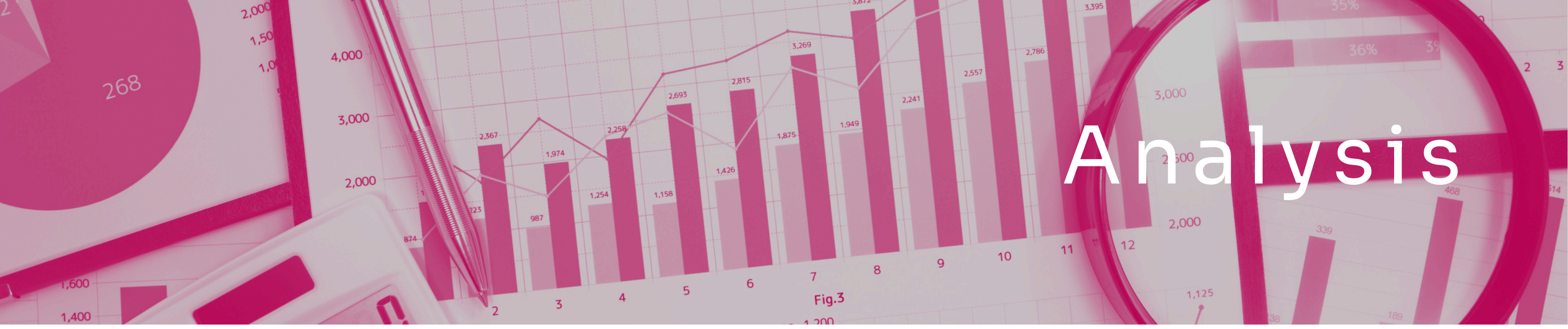
According to a recent study by CapGemini [32] "The majority of telcos (61%) aspire to reach at least Level 3 autonomy by 2028. The journey will be long and complex, however, as only 1% expect to attain Level 5 and 16% to attain Level 4 overall (including operations)." Therefore, there is a large opportunity here to use R&D to help achieve the higher levels of automation.

7.1.2.2/ Network & Customer Experience Analytics

Advanced analytics tools will be critical for understanding network performance, identifying anomalies, and optimising resources. Real-time monitoring and analytics will be integral to network management.

- Understanding the layers and suppliers of the network (physical, virtual, cloud and the various technology elements), and determine the performance of each.
- Integration of feedback from customer experience management and feedback tools to correlate experience perception to the actual network performance.
- Advanced machine learning and predictive techniques driving proactive network operations e.g. the use of GenAI and digital twins focussed on specific scenarios e.g. very high-density mobile networks.

[32] CapGemini Research Institute - Networks with intelligence, Why and how the telecom sector should accelerate its autonomous networks journeys



7.1.2.3/ Observability

Observability takes root from control theory, relies on collecting and analysing this rich dataset that enables the capability to infer the internal state of a system merely based on its external outputs. For instance, it uses telemetry, taps into diverse data points, such as logs, metrics, and traces, generated by every component, from software and hardware to containers and microservices, across hybrid network infrastructure and connectivity environments. At its core, the observability aims at decoding the complex interactions among these components in time and location, to seamlessly determine, predict and rectify anomalies, ensuring optimal system performance, reliability, hence most efficient user experience for any given set of network resources.

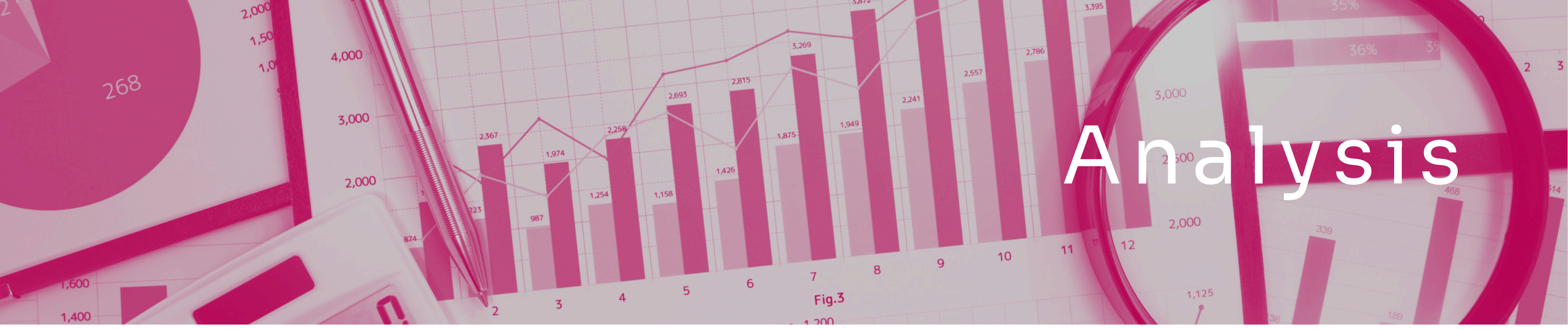
7.1.2.4/ Intent-based networking (IBN)

IBN is a network management approach that aims to make network configuration and operation more intuitive, automated, and responsive to the needs of users and applications. IBN systems are designed to simplify the management of complex networks by aligning network behaviour with the intended business objectives and policies, which are expressed as high-level "intents”. As an example to help meet the “Challenge of Customer Experience Management” the question “What does the customer need to manage their experience?” needs to be defined as an Intent and mechanisms need to be defined to link to automated changes in the network to meet that intent.

7.1.2.5/ Change Management/Control

Because networks change continually in an organic way, it is essential to manage this process. This breaks down into several component activities:

- Managing processes for controlled and managed change, as systems develop and learn through ML before auto-action is taken.
- Record keeping enabling analytics and feedback of changes implemented.
- Interoperability, backward) compatibility and Standards:
    - Network management tools and protocols will need to evolve to ensure interoperability across diverse environments, reducing vendor lock-in.
- Human Resource Challenges:
    - The complexity of managing multiple networks will require network administrators and IT professionals to gain new skills and certifications to keep up with the changing landscape.



7.1.2.6/ Open NM, Trust & "Brokerage"

As the nature of Open Networks and interfaces, the opportunity is to develop new APIs, trust and security mechanisms that enable complex multi-domain networks to:

- To manage multiple vendors, multiple technologies and standards under one centralised network management umbrella
- Exchange data between networks to enable end-to-end customer service experience improved across those networks.
- Support the full range of Network Management functions across multiple systems.
- Secure data from each operator in the E2E service chain so that only designated and secured information is available to 3rd parties in a controlled way.
- Act as a trusted data mediation party between operators for NM data.
- Expose AI-as-a-Service (AIaaS) APIs to enable collaborative AI between network domains and operators.

This leverages the UKs strength in AI, Security, trusted intermediary status in the worldwide ecosystem and could be delivered via opensource or standards organisation driven mechanisms.

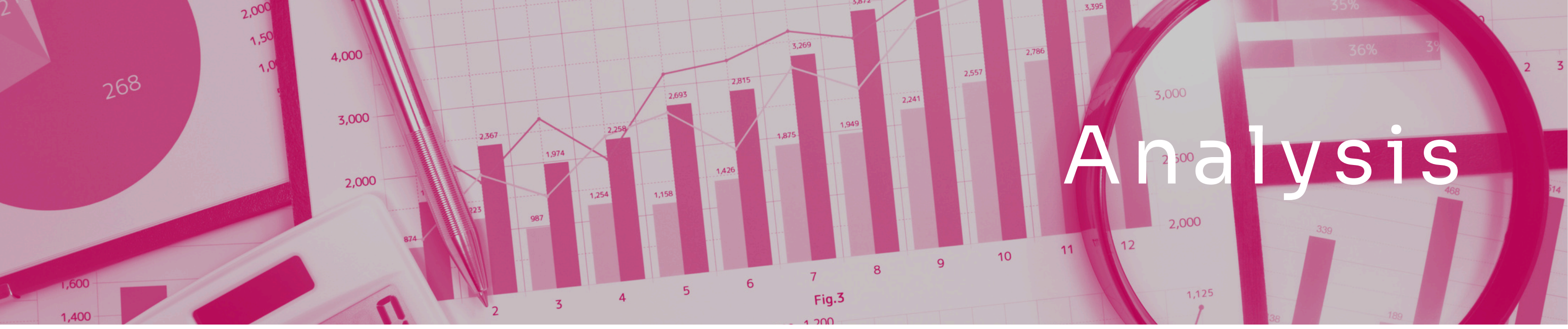
7.1.2.7/ AI Based Automation Across "Complex" Networks

The opportunity here is to develop AI tooling to automate delivery and experience-based assurance across network domains based on multiple telecoms technologies e.g. a mobile broadband service roaming between a high density in building network delivered via a neutral host operator, an external mobile operator, and a satellite-based operator. Alternatively business critical E2E broadband service delivered across WiFi, alt-net fibre, and fixed operator networks. The use of collaborative AI between operators could bring major advantages in offered service quality and operational cost reduction.

This leverages the UKs strength in AI and Alt-net type network operations and links to potential aspects of future 6G functionality.

7.1.2.8/ Customer Experience Drivers & Digital Twins

The opportunity here is to develop digital-twin models that reflect and predict customer behaviour based on the processing of real-time network events and maybe, other inputs e.g. social media or sensor-based data. Essentially this enables the real-time translation of resource-based network performance data, sensor data and social media data into service quality data and the into customer experience data to be used by the operator's OSS and BSS systems to manage and maximise the customer experience. And service-level agreements (SLAs) This could involve machine-learning, forms of large-language models and other AI tooling.



7.1.2.6/ Open NM, Trust & "Brokerage"

As the nature of Open Networks and interfaces, the opportunity is to develop new APIs, trust and security mechanisms that enable complex multi-domain networks to:

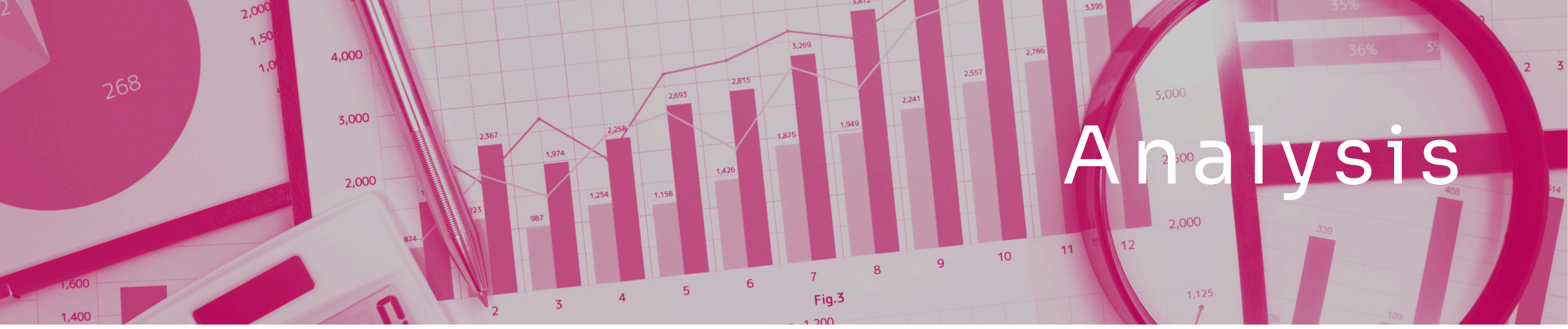
- To manage multiple vendors, multiple technologies and standards under one centralised network management umbrella
- Exchange data between networks to enable end-to-end customer service experience improved across those networks.
- Support the full range of Network Management functions across multiple systems.
- Secure data from each operator in the E2E service chain so that only designated and secured information is available to 3rd parties in a controlled way.
- Act as a trusted data mediation party between operators for NM data.
- Expose AI-as-a-Service (AIaaS) APIs to enable collaborative AI between network domains and operators.

This leverages the UKs strength in AI, Security, trusted intermediary status in the worldwide ecosystem and could be delivered via opensource or standards organisation driven mechanisms.

7.1.2.7/ AI Based Automation Across "Complex" Networks

The opportunity here is to develop AI tooling to automate delivery and experience-based assurance across network domains based on multiple telecoms technologies e.g. a mobile broadband service roaming between a high density in building network delivered via a neutral host operator, an external mobile operator, and a satellite-based operator. Alternatively business critical E2E broadband service delivered across WiFi, alt-net fibre, and fixed operator networks. The use of collaborative AI between operators could bring major advantages in offered service quality and operational cost reduction.

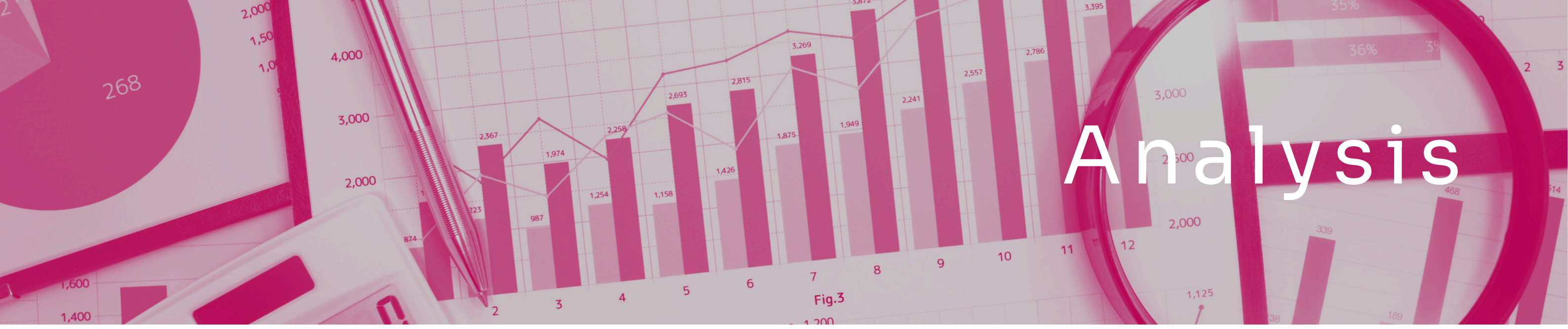
This leverages the UKs strength in AI and Alt-net type network operations and links to potential aspects of future 6G functionality.



7.1.2.8/ Customer Experience Drivers & Digital Twins

The opportunity here is to develop digital-twin models that reflect and predict customer behaviour based on the processing of real-time network events and maybe, other inputs e.g. social media or sensor-based data. Essentially this enables the real-time translation of resource-based network performance data, sensor data and social media data into service quality data and the into customer experience data to be used by the operator's OSS and BSS systems to manage and maximise the customer experience. And service-level agreements (SLAs) This could involve machine-learning, forms of large-language models and other AI tooling.

This leverages the UK's experience with operating large private, business-critical networks e.g. NHS and similar large customers along with strengths in behavioural research and AI. Investment in this area can directly impact UK's competitiveness and opens opportunities to grow revenues in outsourced, cost-effective network operation particularly at scale.



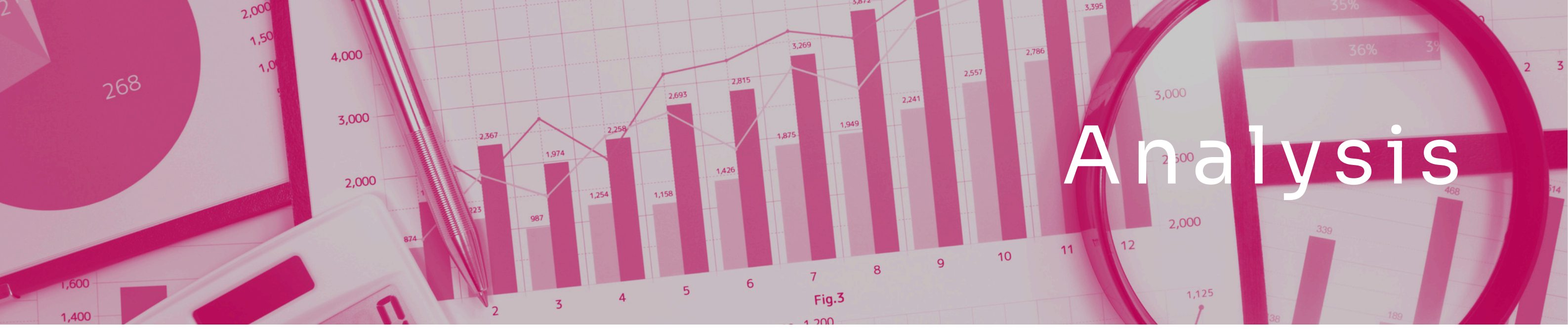
7.2/ Skills

A key part of strengthening the UK's ability to compete in the NM space is to have sufficient skills available to deploy in operators, product developers and R&D activities. Also, there needs to be a well-developed process to bring new people into the world of NM and continuously refresh the skills pool, including new approaches to the skill area. NM skills are wide-ranging and this causes a problem in developing some key specialist people in this area. NM skills can be broadly broken down into the following categories:

- Software Development.
- Telecom Network.
- AI tooling and familiarity with essential ML algorithms and toolkits.
- Network Operations.
- Commercial, Economic & Behavioural.

These are summarised in the following table:

Software Development	Telecom Networking	AI Tooling	Network Operational	Commercial, Economic, Behavioural
Network programmability (P4, OpenFlow)	IP Networking	Machine Learning	ITIL/TMF ODA	Opex/Capex
Systems (C, C++, Go)	Cloud IT Networking	Deep learning	Field Force Mgmt.	Business Cases / Telecom Finance
ML and Data analysis-focussed (Python)	Mobile	Reinforcement Learning	NOC	Customer/ User Behaviour
CI/CD	Optical	Generative AI	Automation	Evolving Procurement processes
Agile Software Development	Wireless	Large Language Models (LLM)	Continuous Improvement	Evolving Accounting processes, (SaaS, Non-Capitalisable etc.)
API Development	Satellite (+NTNs)	Prediction mechanisms	IT Operations	
Opensource Tooling	Positioning, Timing (PNT)	AI Governance	Power Management and Optimisation	
Matlab	Software Define Radio	Federated Learning		
Real-time systems	Software Defined Network			
System Integration	Orchestration			
Microservice Development				



7.2.1/ Current Situation

The present situation is poor, characterised by deficiencies in three areas.

7.2.1.1/ Education

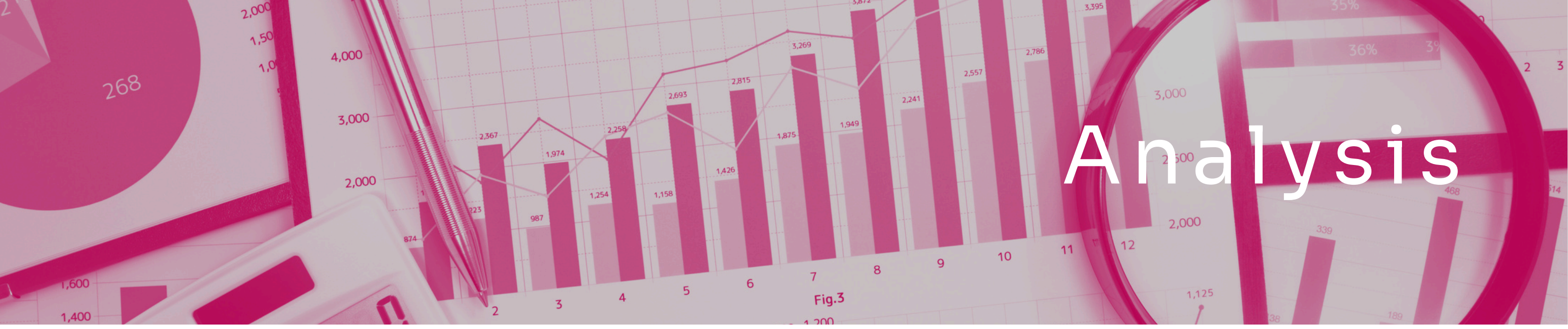
We have identified specific issues relating to recruitment of students for telecoms subjects in general. :

- There is a lack of focus on NM in telecoms education at undergraduate or postgraduate level.
- A low level of interest from UK youth compared to national aspirations.
- But a high level of interest from overseas youth, namely: China, India and Middle East, but this comes with challenges in getting VISAs.
- Lack of NM specific content in telecoms training.

There are also practical concerns to address, particularly related to computer communications security and more specifically in a laboratory practice situation beyond the classroom for NM which explicitly seeks to monitor and control network elements and traffic. Some University IT services may restrict computer communication network training practice to Windows workstations, where students have access to a predefined range of software development environments, such as network simulators, and tools managed by the IT service.

Other operating systems such as Apple IoS or some varieties of Linux may also be supported where there is confidence in their security and skills and effort to do so. Others may require a segregated lab network firewalled or disconnected from other IT services. If security concerns are satisfied, then such networks can be connected to the main network and traffic can be routed between them. This is improving WLAN networking skills of students by allowing them to apply tools such as Wireshark, x2go, Openstack etc, whilst becoming familiar with practical IP networking concepts. On Linux Raspberry Pi (RPi) workstations students are free to explore, access and install Python program packages including AI / ML packages such as TensorFlow, Keras, PyTorch etc, to develop intelligent portable Wireless network systems that can be attached to AGVs, Drones etc. even though they have been able to perform this on their desktop Windows workstations using Python on Anaconda.

Self-help skilling between universities and companies can also play a key role. The existing industrial placement system, which provides university students with one-year industrial experience after their second year in university in companies such as BT, Interoute Viavi, Motorola, L3-TRL Technology, Johnson Controls, Inmarsat etc, has proven to be a very effective way to capture the interest of students in a career in NM. Professional social networks such as LinkedIn will provide continuity post graduation, by allowing educators to track the career progress of their protegees.



7.2.1.2/ Operators

There is a shortage of skills in NM with a worsening position looming unless action is taken. The remaining resource in some sectors, for example radio, is ageing with no pipeline to replace lost talent, knowledge, and skills.

Demographics is a strong influencer with most of the highest skill people located in the South East of England.

Most operators have succumbed to the cost-driven trend to outsource large parts of their organisations to third-party companies with skills located in Easter Europe or Asia.

7.2.1.3/ Suppliers/Systems Integrators

Suppliers and systems integrators have a mix of “on-the-job” training and professional training and certification delivered by a mix of in-house and third parties.

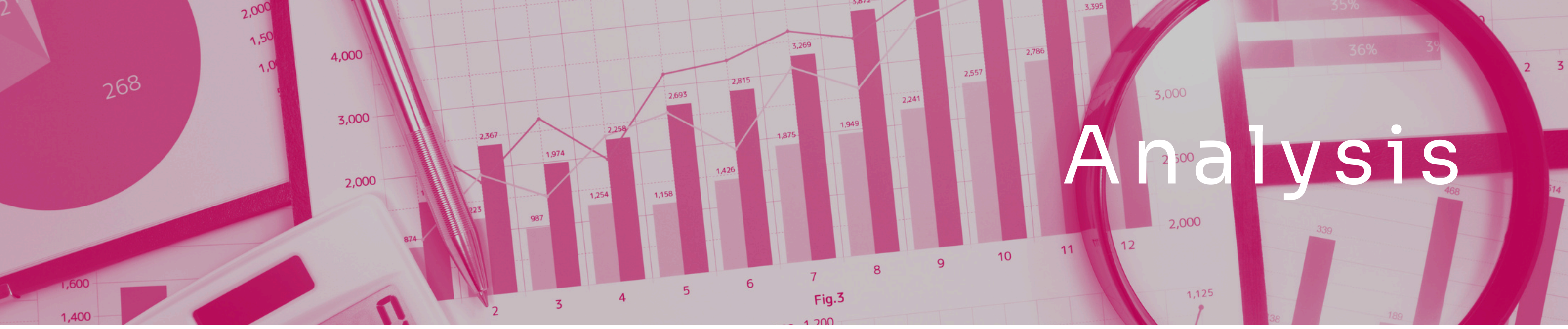
7.2.2/ Opportunities

NM and related operational skills take many years to develop. A major effort needs to be taken to develop and retain such skills in the UK. This is currently made easier by the explosion in the number and types of network operators in the UK – mobile, service providers, alt-nets, neutral hosts etc. However, the shortage of skilled engineers in network operations could also be partly addressed by automation of network management.

Some areas of good practice that could be leveraged to improve the situation are:
IET/BCS/NCSC Certification as a means of promoting technology priorities:

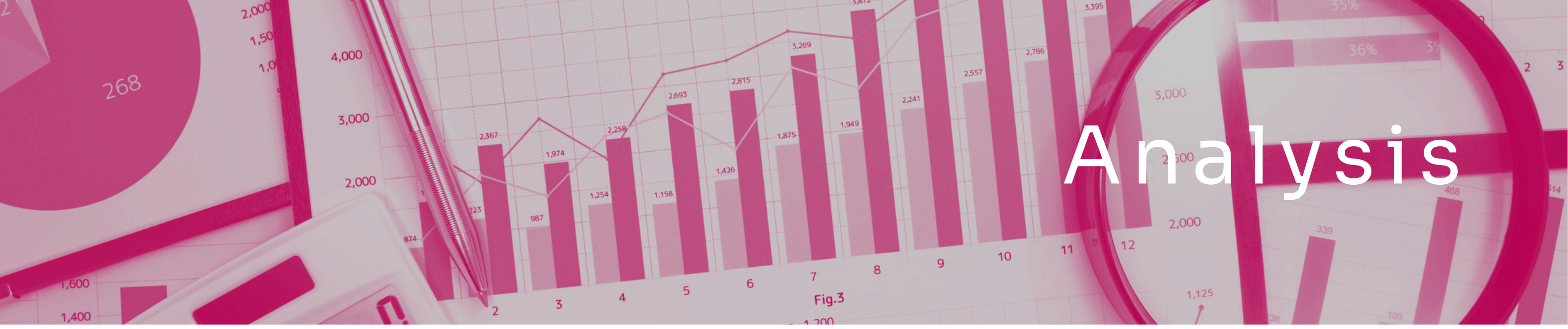
- BEng, BSc, MEng, MSc degree programs in Electronic and Electrical Engineering, Computer Science and Cybersecurity Departments of universities regularly have their degree programs scrutinised by the IET, BCS and NCSC professional organisations to obtain accreditation. Often this is accompanied by stringent skills, knowledge and understanding requirements to be provided by modules in their degree programs and recommendations of enhancements to the degree program structure for those with particular titles. All universities in UK seek this degree program accreditation as students tend to only choose to join courses that are accredited. A dialog must be established between UK Catapults and professional organisations to promote a particular national technology priority (e.g. Communication Network Management, Artificial Intelligence, cyber security etc.) to ensure that degree programs meet industry requirements.
  See references [33][34][35]

[33] IET, Academic Accreditation
[34] Academic accreditation - BCS accredited degree programmes | BCS
[35] Higher education - NCSC.GOV.UK



- Degree Apprenticeships Company as a means of focused training:
  An alternative to university but still gaining a degree in engineering, software, data, UX, business or management etc., is a degree apprenticeship offered by companies in collaboration with universities. The student receives a salary and benefits while learning on-the-job and taking time off to study block taught modules for a degree with an associated university(s) over the course of 3-4 years. The degree is awarded by the participating university. This is popular with companies because it reduces junior staff churn due to commitment to a 4-year duration of employment to obtain a degree and produces a technologist with exactly the skills required for its operations. This is less popular with universities because the numbers of students involved are in the 10s whereas viable courses require numbers of students in 100s and block teaching is not a usual form of delivery of modules. What is needed is more incentives for both companies and universities for this to succeed. See references [36]&[37].
- Knowledge Transfer Partnership (KTP) scheme.
  KTP is part of Innovate UK, which is helping innovation by creating and supporting and collaboration environment between universities and research centres, businesses, and graduated students to work on solving problems. Such a scheme is helping both academics and industry experts to work and solve real problem that faces businesses in innovations. See Ref [38].
- Use projects and programmes led by universities and supported by UK Research and Innovation Council (UKRI) which could be used to test some Network Management tools and systems. For example, the new Convergent Screen Technologies and Performance in Realtime (CoSTAR) networks, which has 5 different labs across the UK (National Lab, Realtime Lab, Live Lab, Screen lab and Forsight lab). See Ref [39]. JOINER project, funded by the DSIT Open Networks R&D fund [40] will interconnect multiple existing 5G testbed in many universities and has a NM “brain”component.
- Extend the self-help skilling between universities and companies to technical colleges. One of the most important tasks is extend capture the interest and imagination of potential students to interest them towards a career in communications network management and AI earlier in their career between Technical College and University. A university placement system, which provides technical college students with two weeks of followed by 6 months day release industrial educational experience in universities such as Brunel University, where the student is loaned an IoT toolbox and performs RPi and Linux networking labs under the supervision of university 2nd and 3rd year students who are paid by the university to provide this technical support. This is proving to be a very effective way to capture the interest of students to pursue a career in Electronic and Communications within universities and subsequently in network management within industry.

[36] Level 6 | BBC Early Careers.
[37] Graduates & Apprentices - Early careers - Careers | BT Plc.
[38] Knowledge Transfer Partnerships (ktp-uk.org)
[39] Convergent screen technologies and performance in realtime (CoSTAR) – UKRI
[40] UKTIN, Government Funded Projects



7.3/ R&D Infrastructure & Facilities

7.3.1/ Current Situation

R&D into telecommunications and NM will often involve the development of new protocols and ways of interacting between networked computer systems. Research teams doing such work must do so within the constraints of academic institution or corporate security requirements, processes, and other best practices.

If there are no real operational networks to work with in research projects, including MSc, PhD studies as well as industrial labs, NM research can be done using Network Simulators (e.g. NS-3, OPNET, OMNET, Matlab 5G Toolbox, etc.) on which network and user traffic are modelled and then network management algorithms are developed.

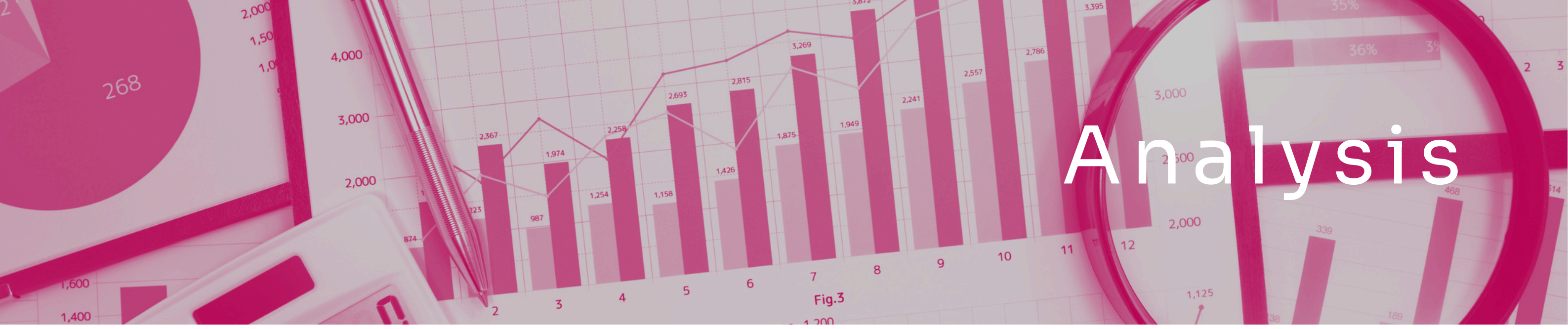
Connected systems containing many computers can be easily constructed as a local private (i.e. segregated) network from commodity off the shelf products, such as the RPi running Linux and small routers. There are various ways such private networks can be connected to each other and to corporate networks, e.g. using Virtual Private Networks or local portals, as mentioned in section 7.2.1 above.

Network Management infrastructure facilities are not only needed for mobile networks. General access to network/switching fabric, for complex next generation internet research is important. Network Management infrastructure facilities are not only needed for mobile networks. General access to network/switching fabric, for complex next generation internet research is key.

There are also facilities dedicated to network and telecommunications R&D, such as the National Dark Fibre Facility [41] (NDFF), to interoperability testing of ORAN equipment, such as SONIC Labs [42], and many purpose-built University laboratory networks, such as the Smart Internet Laboratory at the University of Bristol [43], which recognises the broad multidisciplinary nature of distributed systems R&D. The JOINER project, funded by the DSIT Open Networks R&D fund [44] will extend the NDFF concept by interconnecting multiple existing 5G testbeds, e.g. between the Digital Catapult SONIC Lab and Bristol University's R&D platforms.

Outside the academic hubs, the UK Catapults have built private 5G networks, some supported by wide-area interconnecting infrastructure; and many projects from the DCMS (now DSIT) 5G Testbeds and Trials Programme are maintaining their testbeds for further R&D. Opportunities.

[41] NDFF
[42] SONIC Labs
[43] Smart Internet Laboratory at the University of Bristol
[44] UKTIN, Navigate Government Funded Projects



Analysis

The current situation described above in section 7.3.1 indicates various ways of establishing networked system platforms that can be developed further to support NM R&D and innovation. They provide a route towards exploitation of R&D results that might otherwise remain in the academic domain. In addition, they provide a facility for extending the student learning and practical training experience to development of NM functionality, particularly the use of AI/ML in NM applications as discussed extensively elsewhere in this report.

When R&D results are at a high enough level of TRL to be exploitable, or new techniques and algorithms will be tested, the next innovation steps must overcome several challenges:

- Scaling up – NM systems manage large numbers of network elements. We have often mentioned the large amount of data that AI/ML analytics require. If it does not work at scale, then the new capability is both unusable and useless.
- Security – While it is essential that the development environment is protected, it will be necessary to disrupt the availability, integrity and confidentiality of the NM system being tested, attempt to undermine its authentication, authorisation, and access control, and subvert its accountability mechanisms. This must be done in a secure way, e.g. so that coexisting systems are not collaterally damaged (even though this may be a useful lesson) and the attacks must be realistic and repeatable.
- Optimisation – the new capability must perform at scale and there will undoubtedly be opportunities to improve it, e.g. to alter it to integrate with existing NM facilities and tools.
- Implementation – a R&D outcome will not have been developed to any quality standards that would be expected of a commercial product. However, open-source, often licence-free implementations are used in operational systems (FlexRIC, OpenAirInterface, Open5Gs, Open5GCore) and the risks of using them must be assessed and evaluated in the context of lifetime cost of support among other criteria.

These establish that the R&D results are usable and deployable and further experimentation will say whether they are likely to be useful in commercial situations.

This pre-exploitation evaluation and testing cannot be done unless there is a systematic managed framework. It must be funded properly. The EWG strongly suggests that there should be an umbrella project for telecommunications with different contributing projects to aim at the best outcome for the UK. These funded projects would be a new technology, AI, network management automation or customer experience, all under the same umbrella project. The umbrella project must be managed by only one organisation such as UKTIN.

8/ Recommendations

To illustrate the complexity of the future evolution of NM, we have many detailed recommendations that could take advantage of opportunities available to the UK, strengthen areas of weakness, and counter emerging threats.

Rec 1 - UK long term Vision to develop and leverage AI/ Automation technologies to improve and facilitate the management of highly complex networks.

Back a truly long term (20 year) strategy of how telecommunications enable the modern economy, not just the automation of itself, but also the facilitation and automation of all industries that will require telecommunications. (reference HM Gov Wireless Infrastructure strategy here).

We believe we need a long-term (10 year+) strategy for improving the NM ecosystem in the UK covering development of homegrown NM specific skills, establishment of trusted methods for data exchange, open network management APIs and targeted investment in R&D and revenue growth facilitation measures.

To support this strategy for the future evolution of NM, we have detailed recommendations that could take advantage of opportunities available to the UK, strengthen areas of weakness, and counter emerging threats.

Rec 2 - Create a set of industry specific requirements

We are asking the government to facilitate the creation of a cross industry and research forum, to enable the sharing of knowledge, ideas, problems, and goals, to influence or create development and research areas. For example, a forum where representatives from telecom networks, technology companies, universities, and other industries (Energy, Health, Logistics, Transport, Finance etc.) work together to develop ideas and concepts that will develop Network Management capabilities for the wider benefit. Examples of the scope could include:

- co-creation of requirements from Health and Energy industries, maybe smart cities and network densification
- understanding the absolute requirements from customers and translate into specifications for telcos
- output form this is set of binding requirements e.g. for robotic surgery or driverless cars.

Rec 3 – Real World Datasets

We are asking the government to facilitate the creation of a NM data repository, containing real network-based data, to use as a for testbed for development of NM AI-based automation tools. The main objectives of this would be to enable students to train on NM technology without the need for a "real-world" network and, to train and test AI new systems to aid R&D on NM automation.
For example:

- To produce localised/use-case/scenario specific large-language models (LLMs)to drive network automation systems possibly involving RAG (retrieval, augmented, generation)
- To support AI assisted digital-twin application development such as geo-location using wireless derived data
- To test neural-network based fault management systems as part of a network automation/orchestration system

Because most networks are commercial enterprises, access to this data is extremely difficult and beset with confidentiality and IP issues. The measures necessary to overcome the barrier of the extreme difficulty in obtaining real network-based data need to be determined. This includes:

- How to incentivise operators to provide data, how to make disclosure trusted.?
- Create the correctly skilled and resourced Data analyst team - to get or generate the data.
- Find the appropriate Security body and resources within the data suppliers – to approve the accessing of the data in a way to prevent the "reverse engineering" of infrastructure architectures from the data. This "trust environment" may require the universities to sign up to GDPR and appropriate regulations.
- Create the infrastructure for accessing, localising and using the data for testing.

This recommendation will require the appropriate sponsorship from UK operators, both the academic and non-academic world should promote this.

Similar sharing models from parallel industries may provide good practice to help e.g. sharing of medical information examples are Paddington Life Sciences iCare Trust innovation [45] (recognised at Patient Experience Network National Awards) or UKbiobank [46].

[45] imperial.nhs.uk
[46] UK Bio Bank

Rec 4 - R&D Co-ordination

(Based on 6GStart ‹ 5G-PPP) [47]

An umbrella activity is required to orchestrate, capture, and promote the achievements of UK research projects by facilitating activities in the inter-project working groups and maintaining membership links to the standardisation community. This could be led by UK Catapults This is partially the role of UKTIN -- both promoting activities and bring the ecosystem together, now with activities around standards etc. In the past (5GTT programme) projects were 'forced' to collaborate/exchange info etc. This can be put in the GFA/CA for all DSIT and similar projects.

It is required to:

- Extract strategic R&I orientations from the UK community of projects.
- Coordinate with 5G/6G R&I results/initiatives at UK level.
- Establish and maintaining dissemination structures and web presence for the UK research initiatives.
- There are well established academic conferences for NM (CNSM, IM, NOMS). Build a NM community across the UK and internationally (e.g., by seed funding NM projects), organising workshops on strength areas for UK NM research and, when applicable, attach these workshops to the established international conferences..
- Orchestrate and track UK projects and programmes contribution to emerging standards.
- Facilitate international cooperation across key regions based on promoting UK priorities.
- Develop methodologies for collecting metrics data for technology solutions.

[47] Following the lines of https://www.ukri.org/news/6m-boost-for-the-communications-technologies-of-tomorrow/ specifically for NM could be accelerating most of what we suggest in this paper

Rec 5- Fund research focussed on scalable R&D Platforms for NM e.g. Network "Manageability"

Create a cross industry and university technology collaboration environment that enables the R&D and development of new ideas, services, and technologies. This would enable small to large technology organisations and universities to work together on "real data and systems" to understand, develop and prove new network management ideas, that without real data or platforms are prohibitive for small and medium organisations or universities research.

The goal would be that research would be focussed on scalable and robust Network Management (Software Defined Configuration, Automation, Fault Detection and Observability); Secure Networks; Data Brokerage (sharing data across industries to drive improved customer experiences and performance); AI within Networks.

Research and consult on the facilities needed to create a representative development and verification network for NM research including those necessary for:

- inter-operator network interconnection
- orchestration across multiple network domains
- NM in shared infrastructure and neutral host networks,

Make UK telecom 5G/6G labs more nationally available (beyond JOINER network) across more research institutions and universities in UK, who can exchange knowledge and learn from each other. Objective is to make AI applied to mobile communication network management more generally available across more research institutes and universities with the objective of training more students more widely. These can also be used as a source of service NM data specific for the types of leading-edge services carried over those platforms.

Establish funding for selected academic research to become successful SMEs.

Rec 6 – Skills

We are asking the government to invest in UK NM skills development to increase UK Security, Resilience, Reliability & Scale and bring NM skills back to UK.
UK telecoms has suffered from short-termism and needs the long-term strategy. This will include the development of a home-grown NM skills base. This in-turn will allow for network management tasks to be carried out in the UK not overseas. The use of AI based automation will bring down UK costs so that operational cost drives for offshoring are negated.

Rec 7

We are asking the government to invest in this. To counteract the shortage of skills described earlier, we recommend:

- A long-term investment in home grown skills pipelines to replace aging and outgoing network management resources. Renewing this workforce and skill set is akin to training more doctors and nurses since Network Management pervades every part of our telecoms economy.
- To recruit outstanding talent from abroad as required while we grow and invest in the home skills described above.
- Maximising the availability and quality by utilising the people from diverse backgrounds.
- Provide tax incentives to incentivise investment in Level 1 NM staff development.
- This should ideally include strategy, development and tax incentives.

Network Management roles and skills to focus on are:

- Field Technician Level – address the shortages by:
    - Building on existing successful apprentice and Knowledge Transfer Partnership schemes
- Network Operations
    - These roles are fundamental to the development of AI driven automation. There is a 5-10 year lead time, need to recruit talent externally to fill short and medium term gaps
    - IP skills /virtualisation/AI. Without skills already in the UK we cannot develop our own skills
    - Skills development in this category should focus on a “4 eyes on” approach to change – resilience and reliability management leading to the ability to “co-pilot” AI driven automation system. This will be human led for the next 5-10 years focused on determining the appropriate level of human intervention needed in AI NM systems.
- NM Developers.
    - This is focussed on software and AI driven skills development as described in the earlier section.

Rec 8 – Provide tax incentives to incentivise investment, AI & NM related IP

As described earlier we need to grow the telco NM business in the face of ever-increasing network complexity. How to deal with growth without growing cost base in-line.

Leveraging AI and Automation goes hand in hand with training Network engineering and management resources so we can build those AI models in the future:
- Develop AI/ Automation technologies to improve and facilitate the management of highly complex networks.
- Promote network management and network manageability as a specific research area and focus for existing AI/ML developers.
- Research and develop CEM based digital twin models for telecoms with R&D leveraging experience of large customers e.g. NHS & Finance.
- Provide financial incentives for NM IP commercialisation
- Expand Seed funding opportunities for NM start-ups.
- Build on best-practice spin out/in university schemes.

Rec 9 - Provide financial and other incentives to support investment in home grown NM capabilities and supply.

For example, the provision of brokerage & Services. Bilateral agreements across all these agencies will not be feasible, is there an opportunity for the UK to create companies as trusted telecoms service brokers e.g. for data exchange between telcos & techcos domestically and internationally, for data insight services based on AI and experience operating networks or for systems integration services based on open APIs and complexity management. Leveraging best practice from UK parallel industries e.g. London exchange, other Financial Services, Pharma, & Legal. In the case of recommendation 5 around a brokerage platform for telco data to facilitate analysis and modelling an alternate approach given the personal and commercial sensitivities of telco data might be to facilitate a protected sandpit within each telco that enables modelling against the data but with the telco remaining the 'data controller' as per GDPR.

Look for opportunities to establish UK as a telecoms service broker e.g.
- For data exchange between telcos domestically and internationally
- For data insight services based on AI and experience operating networks
- For systems integration services based on open APIs and complexity management
- Leverage Best practice from UK parallel industries 2T/1T London exchange, other Financial Services, Pharma, & Legal

9/ Conclusions

Data networks whether fixed or mobile are critical infrastructure within the UK and for the UK to thrive in the future digital world it is essential that networks are performant, robust and secure.

Data networks are and will be ever increasingly important to all aspects of the UK economy including the foundation of services critical to the functioning of society:

- Automations and robotics in across heavy and light industry, warehouses and distribution.
- Transport networks and autonomous vehicles (whether train, buses, trans or cars).
- Heath services and especially remote health monitoring and intervention technologies.
- Finance and payment systems.
- Entertainment from streaming television services, gaming, and social media.

Network Management is fundamental to the provision of secure reliable networks, from configuration, implementation of security policies, through monitoring, fault detection and resolution. As networks continue to sharply scale to support ever increasing data growth whilst managing more and more sophisticated security threats, the world of Network Management is and will continue to become more and more complex. In fact, it is now perceived that humans will not be able to effectively manage networks soon, and that automated software driven network management solutions will be essential to the delivery of future networks.

Over the last 40 years the UK has lost its leading edge in network technology and the management of networks. Mainly driven by globalisation and outsourcing, the UK is now over reliant on technology that is designed and manufactured abroad and networks that are managed in outsource centres across the globe. As the world moves into a more unstable period, this leaves the UK in a vulnerable position which needs to be addressed.

The fact that networks are moving towards software running either in the cloud or on specialised edge microprocessor close to the end users, there is an opportunity for the UK to build upon its:

- Leadership software development, AI and microprocessor design.
- Strong academic research within our universities.
- Strongly competitive mobile and fixed networks; and
- leading edge service, finance and Net Zero industries.

Not only to address the UK current vulnerable position, but also to enable the UK to regain leadership in Network Management and drive economic growth in this sector.

A/ Future Technology Trends & The Implications For Network Management

This is a repository of the discussion points in the group on future network technology trends that affect the complexity of future network management systems and processes.

Note: The text in this Annex is still being curated in the first version of the NM EWG's report.

A.1/ Open RAN As An Example Of Open Network Management For Mobile Networks

e-CPRI defines the possible split between the hardware (FPGA, DSP, SoC) and the software multiaccess edge computing (MEC) parts. Most 5G/6G implementations include Central Unit-Distributed Unit (CU-DU) split, with some going further to also include exposure of Enhanced Common Public Radio Interface (e-CPRI) creating a split in the radio equipment between a Remote Unit (RU), Distributed Unit (DU) and Centralized Unit (CU). The motivation for e-CPRI is to make it easier for Mobile Network Operators (MNOs) to mix and match vendor equipment for their 5G/6G network. A 5G RAN PHY Split (ORAN) at option 7.2, which is currently the industry favourite for RU-DU functional splits for traditional cell sites, enables maximum virtualisation of the base station functions for realisation on a local MEC cloud that facilitates the advantages of centralized computing and keeps the fronthaul connection with the edge using limited data overhead and low delay (less than microsecond), whilst exposing the software interfaces for maximum application of Artificial Intelligent applications to the 5G/6G protocol stack functions in order to automate them. The benefit of hardware (FPGA) PHY is that not only does in reduce delay but also it operates fast enough to perform the signal processing required to measure Time Difference of Arrival delays which can be used for obtaining distance measurements, which with further trilateration processing obtains location.

OpenAirInterface (OAI) implements 3GPP stack: The radio access network (eNB, gNB and 4G, 5G UE) as well as the core network (EPC and 5G-CN). Source code is split into two projects:(1) OAI Radio Access Network (OAI-RAN); (2) OAI Core Network (OAI-CN).

FlexRIC "Flexible RAN Intelligent Controller" is a software suite that interfaces with the Open-Air Interface (OAI) radio stack over the O-RAN-defined E2-interface to monitor and control the RAN in real-time. It contains (1) RAN agent that allows for interfacing with the radio stack, (2) Real-time (RT) controller.

xApps and rApps are network automation tools. They maximise the radio network's operational efficiency. rApps are specialised microservices operating on the non-RT RIC. xApps and rApps provide essential control and management features and functionality. xApps are hosted on the near RT RIC and optimise radio spectrum efficiency.

rApps: Non-real time network automation (non-RT RIC) operates from within the RIC's Service Management and Orchestration (SMO) framework. This software functions centrally on the operator's network. The non-RT RIC communicates with the near-RT RIC's counterpart applications, called xApps, to provide policy-based guidance.

xApps are used by the near-RT RIC to handle those events requiring action work in near-real time from 10 milliseconds (ms) to 1 second. The near-RT RC operates as a cloud-based process on the network edge. Within the structure of the near-RT RIC itself, xApps communicate via defined interface channels. There is an internal messaging infrastructure, which provides the framework to handle conflict mitigation, subscription management, app lifecycle management functions and security. Data flows via the RIC's E2 interface for other network automation policy functions.

Understanding and applying these computerization technologies are critical to realising the O-RAN ALLIANCE's mission to re-shape the RAN industry by the redesign and implementation of an intelligently autonomous, open, virtualised and interoperable 5G/6G Radio Access Network [48]. The main drawback of Artificial Intelligence and Reinforcement Learning solutions is the high number of interactions with environment required to explore all possible actions and its possible outcomes to train it, which is a big price to pay when models are to be deployed in an operational environment. Research is needed to overcome this limitation [49].

Current discussion suggests that there could be an option to extend the existing RIC network scope to become an open NM platform for the wider access network. Above the RIC sits the SMO NM layer. These tend to be based on more general orchestration platforms such as ONAP and hence could also be extended to form a more E2E management & automation platform.

[48] O-RAN Alliance "Overview of Open Testing and Integration Centre (OTIC) and O-RAN Certification and Badging Program" White Paper, April 2023
[49 Daniel Camps, Anastasius Gavras, Mir Ghoraishi, Halid Hrasnica, Alexandros Kaloxylos, John Cosmas et al. "AI/ML – Enablers for Beyond 5G Networks" 2021-05-11 Version: 1.0, DOI 10.5281/zenodo.4299895,

A.2/ 5G/6G Communications – Measurement, Decision Making, Acting-Out Decision

A.2.1/ Intent Based Network Management Programmability Technology Enablers

The plurality of Public and Non-Public Networks, the plurality of services with the plurality autonomous network functions means that it is increasingly complex to manage the mobile network. Intent Based Network Management (IBM) aims to simplify establishing, maintaining, and implementing network policies and eliminate unnecessary expert labour associated with traditional network configuration management particularly since it is increasingly difficult to train experts with the required expertise to manage networks in a timely manner. The advantage of using an intent-driven approach lies in the abstractness that can be achieved with the provided intents and letting the intent translation, evaluation and verification modules decide about the actual deployment policy. The system converts the high-level language, from the intent, into a language that can be interpreted by the controller so that it is then possible to install them.

A.2.2/ Autonomous Network Management

Since network and service management is now a complex task beyond the capabilities of a network management team on its own it requires the aid of Artificial Intelligence /Machine Learning (AI/ML). AI/ML methods for network optimisation can be categorised into Neural networks, Reinforcement learning, Hybrid solutions and ML techniques for networking problems [1]. These have been applied to Network planning, Network diagnostics and insights, Network optimisation and control, slice management and service orchestration, cross layer and optimisation, routing and scheduling [1].

Here the challenge is standardisation toward enabling AI/ML in networks, Trust in AI/ML-based networks and AI/ML-based KPI validation and system troubleshooting for 5G/6G.

[1] Daniel Camps, Anastasius Gavras, Mir Ghoraishi, Halid Hrasnica, Alexandros Kaloxylos, John Cosmas et al. "AI/ML – Enablers for Beyond 5G Networks" 2021-05-11 Version: 1.0, DOI 10.5281/zenodo.4299895

A.2.3/ Autonomous Network Functions

In the context of the move to 6G based mobile networks over the next 5-10 years, the following functions are likely to need management by automated NM systems. For ease of categorisation, we have grouped these based on the OSI network model.

A.2.3.1/ Future Physical Layer Functions Needing Management

The coexistence of myriad of new services requires much larger amounts of network capacity, which cannot be solely supported by the sub 6GHz frequency bands that are currently being used for 4G, so mobile network operators have been considering using mm-Wave, sub-THz and IR bands which can be used in a multicomponent carrier networks that simultaneously allows the use of these bands. At these frequency bands there is much larger bandwidths available to support much larger amounts of network capacity for a much larger number of devices required by the eco-system of mobile network users. Operating at these higher frequencies comes with consequences. The propagation of EM waves at higher radio frequencies suffers from much larger pathloss, does not exhibit so much multipath reflection from the scatterers in its environment, and does not exhibit so much refraction around objects or penetration through objects such as windows, doors and walls. To overcome these limitations in propagation characteristics, beamforming using antenna arrays is used, which concentrates the EM energy in the desired direction of transmission so that it can propagate further but in general it has the characteristics of a binary channel, namely: either there is a direct line of sight path between transmitter and receiver or there is not.

Here the challenge is to autonomously steer the beams from RUs towards the UE and track the moving UE and vice versa without the beams intersecting with each other.

A.2.3.2/ Intelligent Beamforming & Beamsteering

The machine-learning model proposed in [50] learns about beamforming antenna environment i.e. its main path and its contrived multipaths between the transmitter and receiver by using the uplink pilot signal received at the terminal BSs with only omni or quasi-omni beam patterns to learn and predict the best RF beamforming vectors. Note that these received pilot signals at the BSs are the results of the interaction between the transmitted signal from the user and the different scatterers in the environment through propagation, reflection, and diffraction. Therefore, these pilots, which are received jointly at the different BSs, draw an RF signature of the environment and the user/BS locations — the signature we need to learn the beamforming directions. This proposed coordinated deep learning solution operates in two phases. In the first phase (learning), the deep learning model monitors the beam training operations and learns the mapping from the omni-received pilots to the beam training results. In the second phase (prediction), the

[50] Ahmed Al Khateeb, Sam Alex, Paul Varkey, Ying Li, Qi Qu, Djordje Tujovic "Deep Learning Coordinated Beamforming for Highly-Mobile Millimeter Wave Systems" IEEE Access, Vol. 6, 2018

system relies on the developed deep learning model to predict the best RF beamforming using only the omni-received pilots, eliminating the need for beam training.

Here the challenge is to continuously learn about the changing environment.

A.2.3.1.2/ Grant-Free NOMA for Massive Machine Type Communications

Non-orthogonal Multiple Access (NOMA) is identified as a promising technology to provide massive connectivity, where multiple users can simultaneously transmit their data over the same radio resource block (RB) by employing user-specific MA signature sequences, which can be exploited by the receiver for efficient data recovery. Various NOMA schemes can be categorized based on MA signatures such as spreading, scrambling, interleaving, and power domain. In grant-free access, the active users directly transmit data using the available channel resources that the Base Station broadcasts periodically, without needing the signalling required for complicated channel access request and granting process [51] [1].

Reinforcement Learning (RL) can be a promising tool to deal with dynamic resource configuration optimisation. [52]

A.2.3.1.2/ Legacy IoT Networks

There is a large variety of short-range, peer-to-peer wireless technologies such as Bluetooth, NeoCortec, Zigbee, Z-Wave, and 6LoWPAN., mMTC, NFC, RFID, LoRa, NB-IoT, WiFi Direct which have been developed to meet specific requirements on functionality, energy consumption, data speed, and operating range.

AI could be used to consolidate all these peer-to-peer wireless technologies into a single generic wireless system.

[51] Muhammad Basit Shahab, Mahyar Shirvanimoghaddam, Rana Abbas, Sarah J. Johnson “Grant-Free Non-Orthogonal Multiple Access for IoT: A Survey” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 22, NO. 3, THIRD QUARTER 2020
[52] Y. Liu, Y. Deng, M. Elkashlan and A. Nallanathan, "Cooperative Deep Reinforcement Learning based Grant-Free NOMA Optimisation for mURLLC," ICC 2022 - IEEE International Conference on Communications, Seoul, Korea, Republic of, 2022, pp. 1-6, doi: 10.1109/ICC45855.2022.9882276

A.2.3.2/ Future Data Link Layer Functions Needing Management

A.2.3.2.1/ Radio Link Control

In a practical OFDM system, Adaptive Modulation and Coding (AMC) is not performed on a per sub-carrier basis because of its significant feedback and control signalling overhead. Instead, the same MCS is used on all the subcarriers assigned to a user equipment. The frequency selective nature of the wideband channel means that the signal to noise ratios (SNRs) of these subcarriers can be different. The MCS chosen is a function of a vector of subcarrier SNRs. In principle, this requires an unwieldy multi-dimensional lookup table to map the vector of SNRs to the MCS, which is cumbersome to generate and store and is seldom used.

Link quality metrics (LQMs) have been proposed to simplify this problem and make it similar to AMC over narrowband channels, in which a simple, one-dimensional lookup table suffices. Exponential Effective Signal to Noise Ratio Mapping (EESM) maps the vector of subcarrier SNRs seen by codeword into an effective AGWN SNR [53].

Current 4G/5G Mobile system use fixed tables constructed (as shown in figure 1b in reference [54]) and used by UEs that map ESNR with CQI that is then reported back to the RAN scheduler. These tables are constructed from the BLER curves for AGWN (as shown in figure 1a in reference [55]) obtained from network simulations. Then of course accurately estimating the parameter β in the EESM mapping equation (in equation 1 in reference [56]) becomes important because it influences the mapping. BLER against SNR curves for given CQI values are obtained from simulations.

The current 4G BLER QoS is measured using Cyclic Redundancy Checking (CRC) to determine if there was an error on the transmitted MAC packet. The outcome of this is conveyed to the UE using HARQ. The capacity available for data transmission is obtained from Tables of code rate against CQI [57]. Further complications arise since, different UE receivers employ different channel estimation and equalisation algorithms, whose performance varies.

Here the challenge is to use Reinforcement Learning to dynamically learn the optimum CQI and MCS and integrate it into the 5G Architecture [58].

[53] Jobin Francis and Neelesh B. Mehta, "EESM - Based Link Adaptation in Point-to-Point and Multi-Cell OFDM Systems: Modelling and Analysis" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 13, NO. 1, JANUARY 2014
[54] Stefan Pratschner , Martin Klaus Muller, Fjolla Ademaj , Armand Nabavi, Bashar Tahir, Stefan Schwarz and Markus Rupp "Verification of the Vienna 5G Link and System Level Simulators and Their Interaction" Online publication seen on 31-10-2023
[55] As 29
[56] As 28
[57] "5G NR Physical layer procedures for data 3GPP TS 38.214 version 15.2.0 Release 15"
[58] Raffaele Bruno, Antonino Masaracchia, Andrea Passarella "Robust Adaptive Modulation and Coding (AMC) Selection in LTE Systems using Reinforcement Learning" 2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall), 14-17 September 2014. DOI: 10.1109/VTCFall.2014.6966162

A.2.3.2.2/ Radio Resource Allocation Control

Any one scheduler may not be suitable for all use cases. Different contexts need different solutions whether or not it is an adaptable single solution or three different solutions. A 4G like scheduler may be sufficient for smartphones (eMBB service), a quite different type of low latency scheduler is required for autonomous AGVs and drones (URLLC service) and yet another type of deterministic or AI based scheduler is required for the Internet of Things (IoT, mMTC service).

Low latencies can be obtained using small Transmission Time Interval (TTI) durations (set by selecting the Subcarrier Spacing (SCS)), minimising the iterations required for Channel coding (Turbo for 4G and LDPC for 5G) and depending on how much data is being transmitted restricting the temporal size (number of TTIs) of a 5G Resource Block (RB). The scheduler, which is capable of obtaining low packet latencies, needs not only to define whether to transmit from one UE or not but also define the size of the RB, which will define the type of channel estimation and equalisation algorithm that can be used.

The scheduling algorithm and time required to make the scheduling decision for providing fairness may restrict the ability to make quick scheduling decisions for low latency packets. A scheduling decision every 10ms would present a problem, if low latency in the order of 100ns is required. Certain very high priority low latency packets may require a snap decision to be transmitted within one 0.125ms slot. In this case a very simple Round Robin scheduler may be required. On the other hand, other use cases may require a balance between proportional fairness and throughput. Furthermore, when there is congestion then min-max or bottleneck scheduling may be required. For certain links where there is a high probability of link loss, then a scheduler which can incorporate a high degree of link redundancy may be required. Combining Traffic scheduling with CQI seems to be achievable but this needs to be able to deal with moving users i.e. non-stationary solution, and a cell free solution i.e. UE can transmit to two IABs. Scheduler to overcome the unreliability of a beamforming channel is also required. A list of different schedulers and their characteristics can be found in [59].

[59] Alexandre Kazmierowski & Victor Gabillo et al "Multi-agent Deep Reinforcement Learning Scheme Specifications" 6G BRAINS Deliverable D2.3, 30 September 2021

A.2.3.2.3/ Slicing

Currently 4G supports audio/video communication and downloading, Internet and messaging services. 5G/6G is to support innovative new services like autonomous vehicles and smart cities, and increase efficiency through smart agriculture, factory robotics and healthcare applications such as remote surgery, each with their own unique service requirements. The challenge is to manage the requirements of these services so that they can all simultaneously operate on a common 5G/6G mobile network infrastructure to take advantage the economies of scale in an eco-system of mobile network users. Slicing has been seen as a means for simplifying and optimising network and infrastructure sharing in different ways, along the three main class of services defined in 5G/6G, namely: eMBB (enhanced Mobile Broadband), URLLC (Ultra Reliable Low Latency Communications), mMTC (massive Machine Type Communications). Clearly there are many different ways that slicing can be used for segregating packets from each other.

Here the challenge is to manage the slicing of the mobile network end-to-end resources and to assign user's packet data to the appropriate slice of which four are listed as follows:

1. one slice per family of services: one for smartphones (eMBB service), one for autonomous driving (URLLC service) and one for the Internet of Things (IoT, mMTC service).
2. one slice per set of technical requirements: grouping services that belong to the same family of use-case requirements (bandwidth, latency, security, volume of messages, scalability, mobility, etc.).
3. one slice per vertical customer: business customer from Industry 4.0, within which several services with heterogeneous requirements can be identified, namely: (1) Streaming Training and Instructional AV (high throughput, close to eMBB); (2) Mission critical manufacturing control from edge/autonomous AGVs/Drones streaming video and control signals (low latency high availability close to URLLC); (3) IoT data retrieval for maintenance or tracking (low throughput, close to mMTC).
4. one slice defined per business customer and technical requirements: Three slices for business customer from Industry 4.0 three categories of services: (1) Streaming Training and Instructional AV (high throughput, close to eMBB); (2) Mission critical manufacturing control from edge/autonomous AGVs/Drones streaming video and control signals (low latency high availability close to URLLC); (3) IoT data retrieval for maintenance or tracking (low throughput, close to mMTC).

A.2.3.3/ Future Network Layer Functions Needing Management

A.2.3.3.1/ Network Planning

Base station planning has been a fundamental research area in mobile networks where the main objective is to design a base station topology that minimises system cost without compromising the experienced subscriber quality of service measured by network coverage and capacity [60][1]. 5G/6G mobile networks are expected to consist of significantly denser deployment of base stations than current mobile networks to provide high levels of data transfer capacity. This motivates the development/study of advanced and novel base station network heuristic NM planning tools for 5G mobile networks if mobile networks operators are to maximise the cost efficiency of 5G. Multiple types of base stations such as macro, pico, femto and Integrated Access and Backhaul, which have different characteristics should be exploited when formulating the base station planning problem for 5G.

A.2.3.3.2/ Joint Network, Compute, & Storage Resource Allocation in Virtual Elastic Infrastructures

The E2E path of the traffic should be jointly optimised with the network, compute, and storage resource allocation [61].

The 6G transport network interconnecting the computation and communication nodes will consist of front/mid/backhaul (X-haul) links of different technologies and capabilities (i.e., both fibre and wireless links), calling for joint consideration of the access network and transport in the modelling process, i.e., optimisation of both user association and traffic routing problems [62].

A.2.3.3.3/ Cell-Free Networks

Since it is envisaged that 5G/6G will require far more RU Integrated Acccess and Backhaul (IAB) access points (1 million per square Km or 1 per square meter) for mMTC small cells, then user equipment moving fast through the mobile network will incur an increasing large amount of signalling to perform inter cell handovers. A cell-free network does away with signalling for handover because the UE is accessing transmission from multiple access points at the same time. A cell free IAB network allows ease of installation of additional new access points because it does not require physical backhaul infrastructure but instead uses the wireless mesh IAB network.

Here the challenge is implementation complexity related to the need to synchronously combine the signals from the UEs received by multiple RU radio Access Points.

[60] David Tyona Aondoakaa “Cost Efficient 5G Heterogeneous Base Station Deployment Using Meta-heuristics" Brunel University PhD Thesis, December 2018
[61] A.Rovira-Sugranes, A. Razi, F. Afghah, and J. Chakareski, “A review of AI-enabled routing protocols for UAV networks: Trends, challenges, and future outlook,” Ad Hoc Networks, vol. 130, p. 102790, May 2022, doi: https://doi.org/10.1016/j.adhoc.2022.102790
[62] As 35

A.2.3.3.4/ Routing

Artificial intelligence (AI) driven routing algorithms dynamically choose the best path for every data packet by analysing a variety of network characteristics, including latency, available bandwidth, and network congestion [63].

In order to maximise network efficiency, guarantee dependable data delivery, and adjust to shifting network circumstances, autonomous routing is essential.

A.2.3.3.5/ Intelligent Reflective Surfaces versus Integrated Access & Backhaul

To overcome these limitations in multipath reflections, Intelligent Reflective Surfaces (IRS) have been proposed to produce a manmade multipath environment to circumvent obstructing obstacles in the radio coverage environment. An alternative solution that has been proposed is to increase the number of Remote Unit (RU) radio access points to increase the probability that a line-of-sight path will always exist between the transmitter and receiver. The issue now becomes that of providing a backhaul for many more RU access points to the gateway to the core network since an optical fibre backhaul for a very large number of RU radio access point, very quickly becomes impractical. Integrated Access and Backhaul (IAB) has been proposed as a solution, where the RU not only provides direct access to user equipment but also provides a network of backhaul nodes through which access to the core network can eventually be reached.

Here the challenge is to not only share radio resources between access and backhaul parts, which can be performed using slicing of radio resource, but also design Multi-Agent routing between network of distributed IABs to the gateway and the core network to meet the QoS requirements of the packet data particularly for reliable and delay sensitive services.

A.2.3.3.6/ Fault Management & Recovery

In autonomous network management, fault management refers to the proactive identification and fixing of abnormalities and failures in the network. AI-driven fault management systems keep an eye on the health of the network, spotting problems like equipment failures, lost connections, or security threats. Based on network behaviour and historical data, AI algorithms may forecast possible problems, enabling the implementation of preventive actions. When a malfunction occurs, self-governing systems have the capacity to identify the problem and take action on their own, reducing network downtime and improving network dependability.

In autonomous networks, fault management is essential to preserving network security and continuous connection.

[63] As 35

A.2.3.3.7/ Reconfigurable Intelligent Surfaces

Reconfigurable Intelligent Surfaces (RIS) represent an innovative approach to wireless communications by using intelligent reflectors to manipulate and enhance signal propagation. Autonomous network management in RIS environments involves the real-time adjustment of these intelligent surfaces to optimise coverage, reduce interference, and enhance signal quality. AI algorithms continuously analyse network conditions, user locations, and channel characteristics to make dynamic decisions on configuring RIS elements.

This autonomous management of RIS surfaces ensures that wireless communications benefit from improved coverage, capacity, and reliability, particularly in challenging indoor or urban environments. RIS technology in autonomous networks offers a revolutionary approach to wireless connectivity and network management.

A.2.3.3.8/ Sustainable Networks - Motivation & Management of Beamforming & Beamsteering

Isotropic antenna radiates its transmitted EM energy equally in all directions irrespective of desired direction of transmission whereas beamsteered mmWave and sub-THz antenna increases transmission efficiency of the transmitting base station by directing EM energy only in the desired direction of transmission.

Here the challenge is to identify the location or direction and distance of the User Equipment to power control and steer the beam towards it.

A.2.3.3.9/ Optical Wireless Communications (1550 nm IR)

Optical Wireless Communications (OWC) allows building owners to deploy their own license free Non-Public indoor 5G Network in their building without having to apply for a shared spectrum license from OFCOM. This means that there is no need for Mobile Network Operators (MNO) to extend their outdoor radio frequency coverage into smaller buildings and there is no need to perform an interference assessment since there is no interference with the outdoor radio frequency. Since OWC is only able to support 1 Gbps data rates up to 5 m over a field of emission of 25° or 3 Gbps with an angle of 15° up to 5 m, multiple access points (AP) installed at regular intervals on the ceiling is required to ensure complete coverage of the room and thus continuous connectivity for the user. This is not a problem because OWC access points are small and relatively cheap to produce, which also means that can be more easily integrated into smart phones. Furthermore, a cell free network inside buildings will obviate the need for subdividing the rooms of a building into cellular coverage areas.

It is likely that these private networks will be numerous and operated by 3rd party network operators, who will look to save on operational costs by managing their customer NPNs using autonomous network management solutions.

7.2.3.3.10/ Managing across licensed & license free networks

Non-Public (Private) Mobile Networks: Outside to indoor mobile solutions are trouble free for the consumer to set up but do not work for all locations inside a building because it is not so efficient to illuminate inside buildings from RU radio access points located outside. Therefore most mobile phone users tend to connect to mobile networks when roaming outside and Wireless LAN networks when roaming inside, if only they are able to obtain the building owner's wireless access password, which is not always the case.

Mobile service from Mobile Network Operators in indoor environments alone falls short since fewer than 2% of commercial and public buildings are currently covered by dedicated wireless indoor solutions. [64] Mobile Network Operators (MNOs) do not have the budget or a valid business case to cover the remaining 98% of pubic/commercial buildings, despite being the key stakeholders as they are the spectrum holders/owners. MNOs will not finance a building access network solution for public or commercial buildings unless there is exceptional number of end users such as in airports and train stations, which typically requires a multi-operator solution, or for a substantial corporate client, which typically requires a single operator solution. Therefore the introduction of a commercial and public buildings network solution for mobile networks could have an enormous impact on this market.

In the absence of an MNO led solution it is expected that there will be landlord owned and third-party neutral host building access non-public network solutions occurring.

Here the challenge is the management of NPNs by building owners or third-party neutral host and the interworking of the Public Network with the Non Public Network.

License Free Networks as Opposed to Shared License Spectrum: One of the growing problems in homes and businesses is interference between the range of different wireless systems in the home, namely: electronic equipment such as microwave ovens, cordless phones, wireless headsets, Zigbee, ZWave, Bluetooth devices, surveillance cameras and other wireless radio networks. Thus, the main motivation for homes and businesses has been to switch to home networks that use regulated spectrum such as from mobile networks to avoid interference problems. Furthermore, many modern buildings are built with thermal metal clad insulation that severely restricts the propagation of RF waves and with metallized windows, which restrict the propagation of RF waves within and to/from outside the building. In the extreme, some buildings are made from steel shipping containers such as the Starbucks building in Tukwila, Washington USA [65]. Therefore, the introduction of modern building materials is making it increasingly difficult for the radio signal from wireless transceivers to provide sufficient coverage inside buildings and so many organisations are attempting to deploy mobile networks on their premises.

[64] "In-Building Wireless", ABI Research, April 2014 / "Wireless in Buildings", Commscope, February 2016
[65] Starbucks Opens New Reclamation Drive Thru Made From Recycled Shipping Containers (inhabitat.com)

The deployment of small mobile network cells using shared public spectrum requires the permission of MNOs, due to their potential to interfere with the main outside transmitted signal, but the MNOs only have the resources to approve installation for their larger business clients (with 100 employees and above) and neglect their smaller clients, who are by far the largest group in the marketplace. These smaller clients then become frustrated and return to using WiFi! This trend is being experienced worldwide.

Furthermore, larger clients, who wish to use small mobile network cells in their premises, require separate infrastructure for every MNO that is providing coverage in a building, which is very costly and inconvenient to the client. This has led to the concept of the sharing of mobile network resources using slicing, such as with Multi Operator Radio Access Network (MORAN) systems, and the concept of improving the coverage within buildings such as with Distributed Antenna Systems (DAS), both of which continue to be costly options for the client.

The status quo between mobile network providers and wireless network providers has been that the former have operated their networks in licensed spectrum whereas the latter in unlicensed spectrum. However recently this status quo has been disturbed by the concept of LTE-Unlicensed, License Assisted Access (LAA) and LTE Supplemental DownLink (SDL), which enables network operators the use of the 4G carrier aggregated LTE radio communications in unlicensed spectrum used by Wi-Fi equipment as well as licensed spectrum.

Recently MuLTEfire has been proposed by Qualcomm, which uses LTE in unlicensed spectrum that does not require an anchor in licensed spectrum, so opening LTE to organisations that do not own licensed spectrum like ISPs and stadia or conference venue owners. Furthermore, the Spectrum Access System (SAS) has been proposed by Google, which uses both 802.11 WiFi and/or LTE in unlicensed 3.5 GHz spectrum for Internet of Things (IoT) devices, which need low latency, high-performance wireless networks typically over a very short range that can handle up to ten million devices under management.

Adopting a cell free Mobile Network solutions in license free spectrum will alleviate the competition for spectrum and accelerate the continued growth of hot spots. Here the challenge is the management of NPNs operating with unlicensed spectrum by building owners or third party neutral host and the interworking of the Public Network with the Non Public Network.

A.3/ Security Of Public / Private Interfaces

Management of user experience expectations from a host of private networks that can overlap with public network.

As private networks begin to take advantage of dedicated spectrum that allow operation of services in the public domain we will begin to see two major aspects that begin to effect user experience.

Public networks are also known as “open” networks since they’re open for connections. These networks are accessible to anyone, regardless of device type, purpose, or function. However, they are usually less secure than private networks due to their open nature.

Private networks are typically used within a home or business. These networks are restricted to authorised users and are typically more secure than public networks. Hackers can compromise your network or devices that are connected to your network and can access to sensitive data. They can also install or inject malicious software on your devices, which may be used to compromise your personal information or take controlling your network or devices.

The question from the network management system point of view, is how to make your network more secure in both public and private networks and what is the secure way to share data between networks to maximise networks performance?

The other issue with private networks, is how the operators are dealing with customers data, is it similar to what have been applied for public network or different.

However, it’s important to note that the specifics of how customer data is handled can vary depending on the operator’s policies, the jurisdiction in which they operate, and the specific agreements they have with their customers. <u>Therefore a resulting question is, is it better to have different policies for public and private network when dealing with customer data or have one policy for both networks?</u>

A.3.1/ Trust Management (Blockchain and Federated Learning Solutions)

There is a growing movement towards decentralisation, with technologies like blockchain and peer-to-peer networks offering potential ways to build a more decentralised internet.

Blockchain technology can be a powerful tool for securing data sharing between different networks. Blockchain features that can help with creating a secure environment for data sharing can be summarised as below:

Decentralisation of Data Sharing: The decentralised features of blockchain eliminates the need for intermediates in the processes of sharing the data. Companies can exchange data with trusted groups by creating a network (peer-to-peer) which can reduces costs and enhances efficiency.

Enhancing Data Security and Integrity: As it employs advanced cryptographic methods to create a decentralised system that cannot be tampered with.
Selective Trust Between Sets: It permits selective trust between sets. For example, in a private blockchain, only a limited set of partners can share and add data, whereas in the case of public one, anyone can add or share into the blockchain.
Transparent and Immutable Records of Data: All data transaction recorded is transparent and can be accessed by all authorised members. These fosters trust between stakeholders, providing a permanent and auditable record of the exchanges of data.

While blockchain offers significant advantages for data-sharing, there are some challenges that need to be considered like, scalability, system integrations, regulations, standardisation, and power consumptions.

For the Federated Learning, often abbreviated as FL and some call it as collaborative learning. It is basically a machine learning (ML) approach where the learning algorithm is trained across multiple decentralised edge devices or servers holding local data samples, without exchanging them. The key features of FL include decentralised learning, collaborative model training, and enhanced data privacy. This is feasible as each device will use it is own data to train an AI model then shares only model updates, (not raw data). This approach has been applied in various fields including IoT devices which produce massive amounts of data, healthcare, where the privacy of patient data is very critical, and finance, where sensitive data and information is regularly complicated.

A.4/ 6G Localisation & Sensing

Localisation and Sensing the environment is important for Network Management because it can be used to plan the positioning of isotropic antennas in an intended coverage area for conventional wireless communication networks as well as plan the direction of beamsteering antenna arrays in future Space Division Multiplexing (SDS) communication networks.

A.4.1/ Localisation Technologies – ToA, RSS, AoA

Localisation of user equipment (UE) in mobile communication networks has been supported from the early stages of 3rd generation partnership project (3GPP). With 5th Generation (5G) and its target indoor and outdoor use cases [66][1], localisation is increasingly gaining importance. 5G localisation systems can utilise received signal strength (RSS), time-of-arrival (ToA), and angle-of-arrival (AoA) technologies with sub-6 GHz and mmWave (24.25 GHz – 52.6 GHz) for estimating position of UE The plurality of multiple-sensing technologies and multiple-sensing nodes ensures the continued ability to obtain localisation of UE despite the occurrence of any obstructions to block line-of-sight access.

A.4.2/ Environment Sensing – location from Landmarks

When all other conventional localisation technologies have not proved effective to estimate distance and position, particularly in urban canyons and indoor environments where direct line of sight path to GPS satellites and Mobile Communication access points are not available, then using the environmental sensing part of a 6G Communications and Sensing system can be used to establish localisation from landmarks such as buildings, street signs and geological features. The motivation for using 6G mobile networks for localisation as opposed to a dedicated RADAR/LIDAR system is the pervasiveness of mobile networks means that they can be applied universally and can employ the economies of scale to produce new and cheaper pervasive services that use high accuracy localisation. It is expected that the environmental sensing part of a 6G communications performs in a similar way to LIDAR or RADAR, by actively sensing its environment to produce a point cloud of the physical objects within it, which can be used to recognise objects and determine the coordinates and direction of object within a map. The best LIDAR systems can obtain a precision from between 0.5 cm over 200 m (Ouster OS1) to 2 cm over 400 m (Ouster OS2) accuracy, which is an indication of what accuracy can be expected from a 6G communication and sensing system. It has been shown that LIDAR can be used to estimate location to sub cm accuracy.

A.4.3/ Simultaneous Localisation & Mapping (SLAM)

6G SLAM combines multiple localisation technologies from mobile access points, such as sub-6 GHz, mmWave, sub-THz for RSS, Time Difference of Arrival (TDoA), and AoA localisation with sub THz environment sensing to produce a point cloud for producing and updating a digital twin for obtaining location from changing environmental landmarks.

[66] Alexandros Kaloxylos et al "Empowering Vertical Industries through 5G Networks - Current Status and Future Trends" EU 5G PPP Technology Board & 5G IA Verticals Task ForceWhite paper 20-08-2020, DOI 10.5281/zenodo.3698113, Version: 1.0, URL http://doi.org/10.5281/zenodo.3698113

A.4.4/ Location Data Fusion

Localisation of UEs using received signal strength (RSS), time-of-arrival (ToA), and angle-of-arrival (AoA) technologies with sub-6 GHz, mmWave (24.25 GHz – 52.6 GHz) and sub THz (90 GHz - 300 GHz) is highly dependent on the continuous direct line of sight access between the gNB access points (APs) and the UE. If there is no direct line of sight access to four or more gNB APs, then location ambiguity is introduced, and so other techniques can be used to maintain localisation such as dead reckoning from inertial measurement unit (IMU), AoA from received radio signatures, iterative multilateration, or position from landmarks. The received radio signatures estimate AoA from more than two APs or AoA and distance from one AP, so that some form of interim measures for obtaining location can continue to be made. Distance and speed of UE can be estimated using OTFS modulation from one AP due to its operation in the delay and Doppler domain as opposed to using OFDM, which operates in the time and frequency domains. If there is no direct line of sight access to any 6gNB APs, then position from landmarks calculates position from at least four landmarks or distance and direction from a single landmark identified from within point cloud data of a sensed environment obtained, for example, from a 6Gsensing/LIDAR system and/or 360-degree image.

A.4.5/ Millimetre-wave (mmWave) & terahertz (THz) bands combined with the beamforming technology

Millimetre-wave (mmWave) and terahertz (THz) bands combined with the beamforming technology offer significant performance enhancements for ultra-dense networks (UDNs).

Unfortunately, shrinking cell coverage and severe propagation path loss experienced at higher frequencies renders mobility management a critical issue in UDNs, especially optimising beam blockages and frequent handover (HO) if cell free networks are not employed.

To avoid this, dynamically updated digital twin systems produced from environment sensing systems can be used to intelligently predict possible blockages in advance and perform beamsteering for a space division multiplexing that avoids both obstruction with other beams and obstacles in environment.

Acknowledgements

UKTIN would like to thank the following for their contributions to this paper:

Tom Bennett (Chair)
Laith Al-Jobouri
Soufiane Ayed
Luc Berthouze
Tom Boyle
John Cosmas
Erol Hepsaydir
Bryn Jones
Michael McGroarty
George Parisis
Nazirali Rajvani
John Wintour-Pittom

UKTIN Secretariat:
Nick Coombes
Alistair Munro