RESEARCH

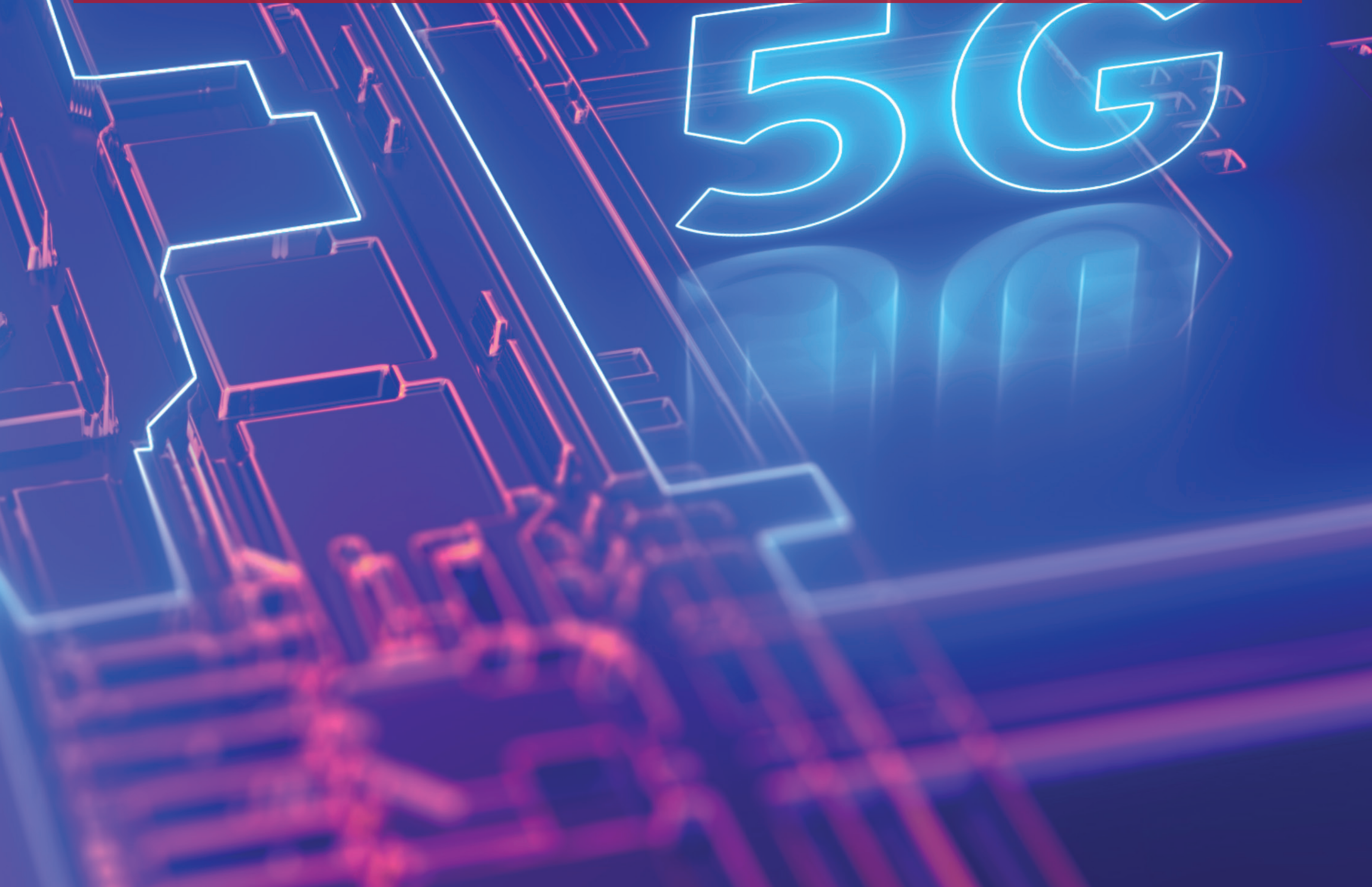
analysys mason

WHITE PAPER

BUILDING AUTONOMOUS NETWORKS FOR THE 5G ERA: A REFERENCE FRAMEWORK TO DELIVER BUSINESS OUTCOMES

Anil Rao, Gorkem Yigit and William Nagy

OCTOBER 2020



Contents

1. Executive summary 3

2. Autonomous networks enable CSPs to operate next-generation services 4

2.1 The introduction of new services and technologies increases the operational complexities of the network 4

2.2 Autonomous networks will dramatically change the operational economics and improve environmental sustainability 4

2.3 ML/AI-driven autonomous networks will transform the CSP operations framework 5

3. Autonomous networks will enable key business value outcomes 6

3.1 TM Forum provides a framework for achieving autonomous networks 6

3.2 Service providers will adopt different identities as they automate their networks; the scale and scope of automation will vary for each role 7

3.3 Increasing network automation and migrating from one identity to the next will enable service providers to achieve key business outcomes 8

4. Building autonomous networks 9

4.1 A common industry framework for achieving the autonomous network vision is emerging 9

4.2 CSPs should build hierarchical autonomous network architecture using a stepwise approach 10

4.3 CSPs should collapse network siloes into autonomous domains with cloud-native, software- and AI-driven digital infrastructure 11

4.4 The cross-domain service automation layer stitches autonomous domains together for end-to-end service orchestration 12

4.5 AI/ML will be essential in all layers of autonomous networks 12

5. Preparing the organization for autonomous networks 15

6. Conclusion and recommendations 17

7. About the authors 18

1 Executive summary

Communications service providers (CSPs) are introducing network function virtualization (NFV), cloud-native computing (CNC) and software-defined networking (SDN) technologies into 5G networks, even as they continue to operate legacy physical networks. This mix of legacy and new networks increases the operational complexity that cannot be managed using traditional operational approaches.

The legacy operational systems and processes were predominantly designed as siloed software solutions for various individual network domains and required significant manual effort and intervention. This approach is not economically and operationally viable for complex 5G networks and services. Autonomous networks will be critical to make legacy operations lean and to make 5G successful.

However, the journey to fully autonomous networks will be gradual; CSPs need to put strategies in place to carefully manage the transition. The TM Forum model for autonomous networks uses levels (0–5) to assess the maturity based on a set of conditions.[1] According to the research conducted for this study,[2] many CSPs are at level 2 (partially autonomous networks with limited autonomous capabilities), and some advanced CSPs are operating some network domains at level 3 (conditionally autonomous networks: intent-based automation based on real-time network changes).

To achieve the vision of autonomous networks, CSPs need to adopt an intent-driven automation approach. CSPs must first define the business intent; this could be an enterprise wanting to automate their WAN or the CSP wanting to fully automate its mobile broadband operations. The business intent is then translated into service intent (encapsulating the service design and service orchestration processes) and network intent (network resource and service orchestration), supported by assurance systems to monitor the state of the network and services. Together, the service design and orchestration, network orchestration and automated assurance systems, supported by AI/ML capabilities, enable an intent-driven, fully closed-loop autonomous network.

CSPs need to implement a hierarchical cross-domain automation architecture that collapses network siloes, simplifies network domains and transforms the underlying network into a platform by abstracting the underlying complexity. The use of industry-standard open APIs allows CSPs to achieve this by enabling adjunct applications such as SDN controllers and other OSS applications to access the network in a standardised way. A unified AI/ML and network analytics platform can further accelerate the journey to level-5 multi-domain autonomous networks.

It is critical that CSPs prepare their organizations for operations based on autonomous networks. A handful of CSPs will execute the transformation themselves, but the majority will require support from partners. CSPs should choose vendor partners that are deeply committed to the vision of autonomous networks and offer state-of-the-art network and operations platforms built for automation. Vendors should also offer a wide range of engagement models including software-as-a-service (SaaS), advisory services, managed services and outcome-based outsourcing to alleviate CSPs' business risks and increase the chances of transformation success.

[1] TM Forum (2020), Autonomous Networks: Empowering Digital Transformation For The Telecoms Industry. Available at: https://www.tmforum.org/resources/whitepapers/autonomous-networks-empowering-digital-transformation-for-smart-societies-and-industries/

[2] We interviewed four CSP executives in Western Europe whose organisations have either started to or are about to transform their networks to become autonomous.

2 Autonomous networks enable CSPs to operate next-generation services

Communications networks are becoming increasingly complex due to the introduction of new dynamic networking techniques such as NFV, SDN and cloud-native architecture. These foundational technologies, which form the basis for 5G, are rendering traditional operational approaches obsolete. CSPs will be unable to maintain competitiveness and provide a high-quality service if they continue to use the manual and labour-intensive methods of operating and maintaining their networks and services as they migrate to 5G.

2.1 The introduction of new services and technologies increases the operational complexities of the network

The implementation of 5G standalone (SA) calls for cloud-native networks that are based on virtualization and containers. The network stack will consist of virtualized and microservices-based cloud-native network functions and applications built on top of containers, which must fulfill the end-to-end service requirements. 5G-enabled digital services will provide CSPs with a new channel of revenue. Network slicing will allow CSPs to offer enterprise services that are differentiated by their use case, quality of service, and service level agreements to meet a particular enterprise's unique connectivity requirements. Network slicing will also allow CSPs to create logically isolated virtual end-to-end networks from the RAN to the core, and it is possible for CSPs to have hundreds of active slices at any time. The enterprise services will be ordered and customized by the customer through self-service portals and will be activated, altered and, eventually, deactivated on-demand.

New technologies and services are being introduced while the existing physical networks are supporting revenue-generating services, and it is expected that these physical networks will continue to exist for many years. This will result in a mix of coexisting legacy and new networks, thereby significantly increasing the level of operational complexity because the operations and management systems that are associated with the legacy networks must perpetually coexist with the new management systems. The introduction of newer technologies such as containers and microservices will only exacerbate the problem further.

CSPs have to carefully manage the transition from the existing operations model to the new model with minimal business disruption. One way to do this is to deploy an abstraction layer over the existing legacy networks and the new SDN and NFV-based networks using a common set of open APIs for both southbound and northbound integration. This provides the critical foundation upon which the journey to autonomous networks can progress. CSPs can then supplement it with additional capabilities such as ML/AI-based automation to ensure that the network can self-optimise based on service intent.

2.2 Autonomous networks will dramatically change the operational economics and improve environmental sustainability

High levels of automation will result in an opex transformation for CSPs. Opex reduction is a key issue for CSPs, particularly when organic revenue growth is difficult to achieve. The time and costs associated with manual processes such as network fault management, planning and design and report generation are variables that CSPs seek to minimise with their current networks. These processes will only become more time- and cost-intensive as network and service complexity increases. Automation is a critical factor in reducing time and labour requirements and enables a more efficient network. This will lead to large opex savings for CSPs as they operate their next-generation 5G networks.

CSPs must also consider the sustainability of their networks as they introduce new technologies. 5G new radio (NR) and other networking technologies such as mobile edge computing (MEC) increase the physical scale of the network. 5G NR requires cell site densification to provide comprehensive service coverage, which means that more radio units, base band units and centralised units must be deployed across roll-out zones. Likewise, as the adoption of edge computing becomes widespread, edge cloud locations will proliferate to maintain optimal service in a range of geographical locations.

The increased scale of the network means that there are greater sustainability concerns because the energy usage of the network is higher in order to keep the distributed sites operational. Power capacity, air conditioning requirements and coverage redundancy considerations are factors that CSPs must consider when operating the network. Automations powered by ML/AI can be implemented to manage these considerations without human intervention. They will monitor power consumption against service requirements and adjust site capacity, regulate internal site temperatures and dynamically alter cell site coverage to remove redundancies.

2.3 ML/AI-driven autonomous networks will transform the CSP operations framework

Autonomous networks are the key to operating complex and dynamic cloud-native networks efficiently and to ensuring that CSPs keep pace with their customers' requirements. Autonomous networks will enable CSPs to handle the complexities of orchestrating network resources to enable rapid service innovation. Autonomous networks can also orchestrate the assurance and fulfillment resources so that the whole network is unified and synchronized in its autonomy through closed-loop automation.

Machine learning and artificial intelligence are key enablers of the closed-loop automation vision of autonomous networks. These intelligent algorithms can handle the complex decision making required to configure and optimize network resources and to orchestrate services such as network slicing in an end-to-end fashion. ML/AI will also enable predictive operations: the algorithms will learn to spot patterns in network/service degradation and employ automated remediation routines to adjust the network parameters, thereby reducing the down time and increasing the quality of service.

3 Autonomous networks will enable key business value outcomes

3.1 TM Forum provides a framework for achieving autonomous networks

CSPs will not implement autonomous networks in a short timeframe. It is a journey that requires CSPs to adopt a stepwise approach. The TM Forum defined the levels of autonomous networks in order to provide an industry standard for evaluating the maturity of autonomous networks.[3] Its classifications of autonomous networks run from level 0 to level 5, as seen in Figure 3.1.

According to our interviews, most CSPs are at level 2 in TM Forum's classification system, with more advanced CSPs operating some domains at level 3. Most CSPs have started to lay the foundations to take their whole network to level 3 and will continue to expand autonomous functionality through their networks incrementally to progress to the higher levels.

The journey to the fully autonomous network is expected to take at least a decade. New technologies and services will be added to the network over the years to come, which will create additional requirements for what constitutes a fully autonomous network.

> *"Automation is not new to our industry; we have applied scripting and robotics to automate existing manual workflows for many years. But now we are talking about a fundamental shift in the way networks are built and operated. For autonomous networks to become a reality, automation needs to be natively built in so that the network can handle the lifecycle management operations by itself."*
>
> **– Converged group CSP from Western Europe**

> *"Autonomous networks are a continuous moving target for us. It is a big step up moving from level 0/1 to level 2, but progression to the higher levels will be incremental with a gradual scale-up in technology, operations and organizational capabilities."*
>
> **– Tier-1 CSP from Western Europe**

FIGURE 3.1: THE SIX LEVELS OF AUTONOMOUS NETWORKS AS DEFINED BY TM FORUM [SOURCE: TM FORUM, 2012]

Autonomous network level	Description
Level 0 (manual management)	The system delivers assisted monitoring capabilities, which means that all dynamic tasks have to be executed manually.
Level 1 (assisted management)	The system executes a certain repetitive sub-task based on pre-configured to increase execution efficiency.
Level 2 (partially autonomous network)	The system enables closed-loop O&M for certain units based on an AI model under certain external environments..
Level 3 (conditional autonomous networks)	Building on L2 capabilities, the system with awareness can sense real-time environmental changes, and in certain network domains, optimize and adjust itself to the external environment to enable intent-based closed-loop management.
Level 4 (high autonomous networks)	Building on L3 capabilities, in a more complicated cross-domain environment, the system enables analyzes and makes decision based on predictive or active closed-loop management of service and customer experience-driven networks.
Level 5 (full autonomous networks)	The system possesses closed-loop automation capabilities across multiple services, multiple domains, and the entire lifecycle, achieving Autonomous Networks.

[3] TM Forum (2020), Autonomous Networks: Empowering Digital Transformation For The Telecoms Industry. Available at: https://www.tmforum.org/resources/whitepapers/autonomous-networks-empowering-digital-transformation-for-smart-societies-and-industries/

3.2 Service providers will adopt different identities as they automate their networks; the scale and scope of automation will vary for each role

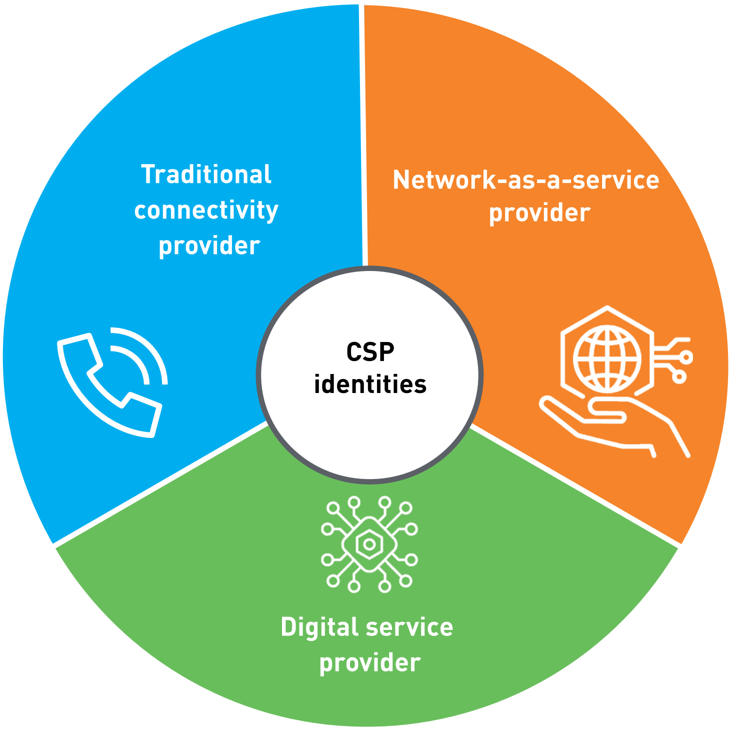
CSPs are looking to transform their businesses and operations as they work to provide value beyond just connectivity. As a result, they are likely to adopt a new identity. These identities can be segmented into three broad but non-exhaustive categories that build on each other (Figure 3.2).

- **Traditional connectivity service providers** are focused on owning differentiated physical network infrastructure and delivering traditional communications services. Traditional CSPs still play an important role because connectivity is fundamental in an increasingly interconnected world, but differentiated network capabilities enabled by automation are critical for CSPs that retain this identity in the long term. 5G will be a key factor in traditional CSPs' strategies in order to provide dense coverage and fast connectivity.

- **Network-as-a-service (NaaS)[4] providers** add value by giving customers and partners access to an API-driven digital network platform and network-related services over owned or leased physical infrastructure. NaaS providers will aim to deliver network and network-based services on-demand to support services provided by digital service owners such as cloud, security, IoT and content delivery services. NaaS providers will also supply on-demand and differentiated network properties such as latency and bandwidth through network slicing and edge computing capabilities.

- **Digital service providers (DSPs)** add further value using non-network-related services on a common digital platform. DSPs build on the capabilities of NaaSPs by diversifying their revenue with non-connectivity-based services. This allows them to move up the value chain and become digital service owners.

FIGURE 3.2: SERVICE PROVIDER IDENTITIES [SOURCE: ANALYSYS MASON, 2020]


Traditional connectivity provider
Network-as-a-service provider
CSP identities
Digital service provider

[4] NaaS is also used to explain the architectural approach for network abstraction and service exposure to internal software systems within the CSP. In principal, the same abstraction layer could be used for service exposure for customers and partners.

All three identities will require automation in order to succeed in the long term.

- Traditional CSPs will benefit greatly from achieving at least a level-2 network as next-generation networks are developed and commercialized at scale.
- NaaS providers will need to have an autonomous network that is at least level 3 in order to achieve the business and operational outcomes expected of the dynamic connectivity and platforms that they offer.
- DSPs will require an end-to-end automated network (level 4). Closed-loop network management will enable DSPs to automatically orchestrate the network and services and achieve the twin benefits of increased revenue and lower costs.

3.3 Increasing network automation and migrating from one identity to the next will enable service providers to achieve key business outcomes

Autonomous networks are critical for CSPs that want to transform from traditional CSPs to NaaSPs and DSPs. As service providers take on different identities, they need to develop strategic and enablement capabilities to achieve and secure a progressively stronger hold on five key business outcomes (Figure 3.3).

> *"We are implementing automation on a per-domain basis, but we are also being very deliberate about achieving cross-domain end-to-end automation and breaking down silos in the process. We are including specific requirements in the vendor RFPs to ensure that we do not get tied to a closed and rigid domain-specific solution."*
>
> **– Converged group CSP from Western Europe**

FIGURE 3.3: FIVE KEY BUSINESS OUTCOMES ACHIEVED THROUGH NETWORK AUTOMATION [SOURCE: ANALYSYS MASON, 2020]

Business outcome	Description
Service innovation	Service innovation enables service providers to differentiate their connectivity, platform and digital services. Migrating through the identities naturally opens more possibilities for service innovation. A highly autonomous network provides the foundation for service providers to build their services on, from high-quality basic connectivity to on-demand network slice instantiation and orchestration.
Superior customer experience	A superior customer experience is enabled through customer-centric operations. Service providers must ensure that business and network processes are designed around the customer journey, which means that network operations must evolve to focus on the quality of service. Customer centricity demands that network KPIs, service KPIs and contextual customer data are analysed and correlated using ML/AI tools, which then autonomously adjust network and service configurations for optimal service quality.
Infrastructure excellence	Infrastructure excellence can be achieved by maintaining highly optimised network coverage and providing the right level of capacity when and where necessary. It can also be achieved by optimising digital infrastructure across owned and shared/neutrally hosted physical infrastructure to expand reach while maintaining low operational costs and providing low-cost connectivity.
Lean operations	Autonomous networks underpin lean operations, which are a critical enabler of cost efficiencies. Lean operations use common models that support the self-service selection, configuration and management of complex on-demand services that rely on end-to-end automation. Standards-compliant open APIs enable a standardised approach to intent-driven operations and enable operational systems to seamlessly integrate with each other. Lean operations also include digital partner management, whereby service partners are integrated into the service provider platform via open APIs to support economies of scale and enhance service portfolios.
Organizational agility	Organizational agility enables siloed operations to be dismantled across departments. An autonomous network integrated with automated business and IT systems will enable a smooth customer journey and a unified customer experience across the departments involved (ranging from network operations to customer care). An agile organization can also make full use of the autonomous network to support service innovation and new business models and address new market opportunities.

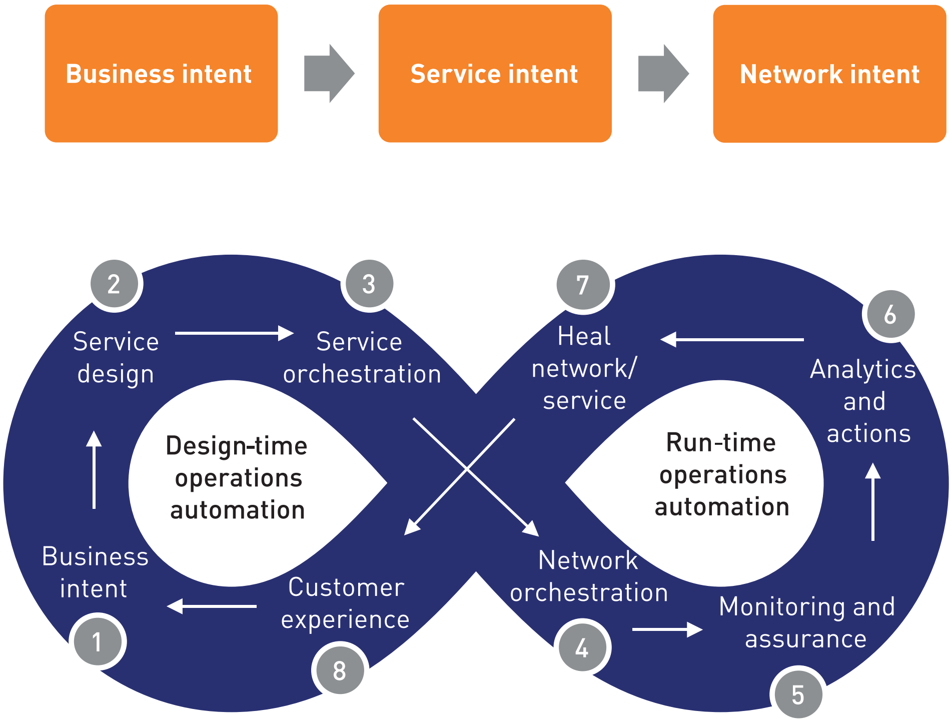
4 Building autonomous networks

4.1 A common industry framework for achieving the autonomous network vision is emerging

The main processes such as network design, planning, fulfilment, assurance and maintenance are highly disjointed in the current mode of operations, and often require manual interventions and inter-departmental handovers. This is because CSPs historically implemented numerous network technologies, OSS, E/NMS and ad-hoc tools and solutions as vertically integrated network/service-specific siloes, thereby resulting in complex, fragmented network operations. Autonomous networks require a radical departure from this model. CSPs need to simplify and streamline their entire operations and join up all these processes end-to-end through domain and cross-domain closed-loop mechanisms with software and AI/ML systems to achieve full lifecycle automation.

There is a range of network and service automation visions and projects set by CSPs and vendors, as well as numerous industry initiatives by standard bodies and groups including TMF Autonomous Networks Project, ETSI Zero-touch Network and Service Management (ZSM), 3GPP, GSMA and ONAP, all of which are striving towards enabling a high level of end-to-end automation (level 4 or 5). A common understanding and a high-level framework for enabling autonomous operations is emerging from these efforts. Figure 4.1 illustrates Analysys Mason's reference framework for autonomous networks.[5]

FIGURE 4.1: FRAMEWORK FOR AUTONOMOUS NETWORKS [SOURCE: ANALYSYS MASON, 2020]



[5] For more information, see Analysys Mason's Network automation: a solution framework for service agility and cost economics in cloud-enabled 5G networks.

This framework is centred around the idea of building customer- and service-oriented autonomous networks, so intent-driven operations are a fundamental principle of this new operational model. The framework starts with the definition of business intent by the customer, which is the declaration of a business objective (for example, an enterprise demanding to set up branch and WAN connectivity or deploy a new IoT application). An autonomous network should fulfill the business intent using service policy, design, orchestration and AI/analytics capabilities in a fully closed automation loop across design-time and run-time operations.

The business intent must then be translated into service intent through service orchestration by decomposing the business intent into various steps and mapping them to service requirements and relevant network resources. Network orchestration converts this service intent into network intent, and instantiates and activates the networking resources associated with the service within specific domains as well as across domains. It also validates and monitors the network and service and performs analytics-driven automated actions to self-heal and self-optimize the network to resolve issues before they impact service quality and customer experience. The insights and patterns generated by AI/ML tools also drive the automation of the service design and network and resource planning processes.

Achieving this automation framework will require a series of steps, including the adoption of new network technologies (such as cloud-native functions, SDN, orchestration, AI/ML, telemetry and open APIs), simplified network architecture and redesigned operational processes with a long-term vision and platform thinking (discussed in Section 5). An organizational and cultural transformation will be critical in this journey (discussed in Section 5).

4.2 CSPs should build hierarchical autonomous network architecture using a stepwise approach

CSPs' networks consist of several domains such as mobile core, data centre, WAN, RAN and edge. These networking domains typically have complex architecture composed of multiple services, vendors, technologies, and datasets. To achieve end-to-end automation that spans all of these complex and dispersed domains, CSPs should consider a hierarchical automation architecture approach as follows (Figure 4.2).

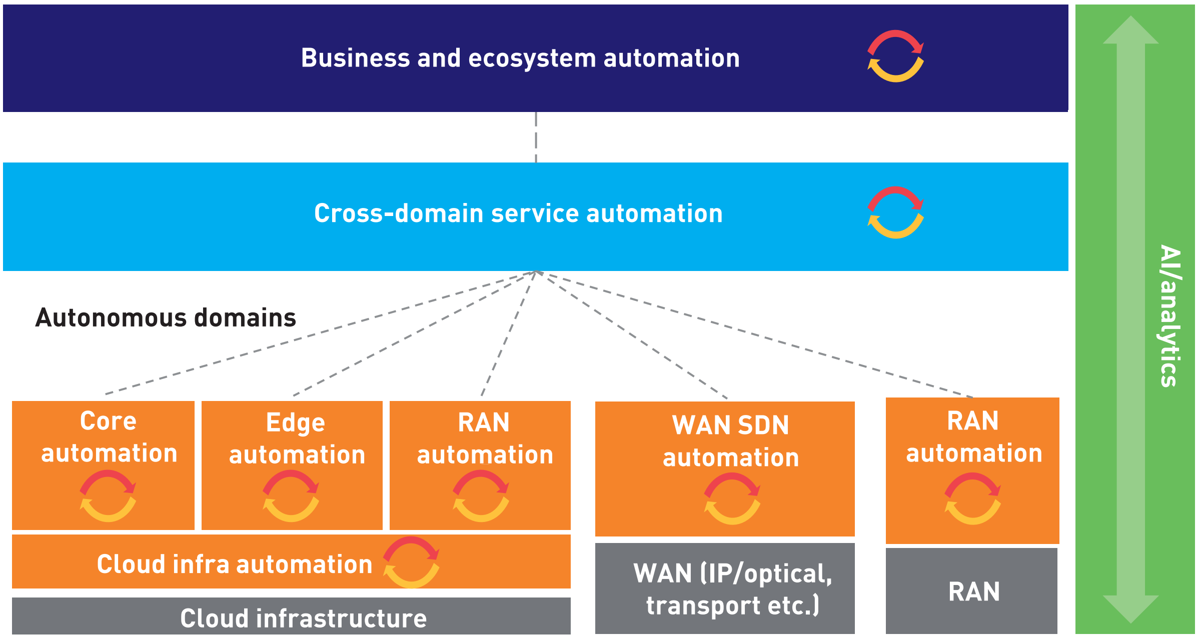
- CSPs should build autonomous domains in a stepwise fashion with domain-level local abstraction and orchestration for intra-domain closed-loop automation and self-sufficient operations (self-configuration, scaling, healing and optimization) over hybrid physical and cloud resources.

- These multiple autonomous domains should then be integrated into an end-to-end cross-domain service automation layer using open northbound APIs for service automation. The cross-domain orchestrator should stitch together the different domains and automate the resource selection, configuration and optimization for the service (for example for creating end-to-end network slices across the core, transport, edge and RAN).

- Cross-domain service automation capabilities should be exposed to a business and ecosystem automation layer for agile, on-demand service delivery and customer and partner management.

- Advanced analytics with AI/ML will be pervasive in this architecture; there will be several instances running across these layers and embedded in the network nodes and elements. CSPs should create centralized data lakes and a common set of AI/ML tools, processes and governance to further increase efficiencies.

FIGURE 4.2: MAIN BUILDING BLOCKS OF AUTONOMOUS NETWORKS [SOURCE: ANALYSYS MASON, 2020]



4.3 CSPs should collapse network siloes into autonomous domains with cloud-native, software- and AI-driven digital infrastructure

Digital network infrastructure composed of virtual, cloud-native software and programmable network components will be the foundation of autonomous network operations. Many traditional, monolithic network elements are increasingly being transformed into virtual network functions and cloud-native functions that are developed in container-based architecture and deployed with Kubernetes (K8s) and its open-source ecosystem components. These cloud-native functions and K8s ecosystem components give CSPs the ability to fully automate network resource lifecycle management from the point of initial deployment through to operations such as self-healing and horizontal scaling capabilities. They also allow the use of DevOps and CI/CD methodologies. In particular, the declarative and model-driven nature of K8s lends itself to the intent-based operations discussed in the previous section. Domain-specific network orchestrators (such as NFVO) can work together with K8s to support the automation of network lifecycle management tasks such as onboarding and scaling network functions.

Autonomous networks should embrace SDN-enabled physical infrastructure alongside the cloud-native components and should use open intent APIs to manage and control WAN infrastructure in order to achieve end-to-end WAN automation, network visibility and programmability. There is a range of approaches for this, including:

- using domain- (IP, optical) and vendor-specific SDN controllers and multi-layer, multi-domain WAN SDN platforms that unify the control and management of these domain-specific controllers
- the automated multi-vendor configuration of network devices with NETCONF/YANG
- SD-WAN traffic steering and security at the network edge and for multi-cloud connectivity.

The availability of standardized interfaces (for example, IETF NETCONF/YANG, ONF T-API and MEF) and modelling languages (such as YANG) enables CSPs to consolidate control and management data from multiple WAN layers and export it up to the cross-domain orchestrator through REST interfaces.

Domain orchestration and self-optimizing networks powered by online data, telemetry and AI/ML techniques can be deployed to automate network planning and design, capacity planning and optimization functions in a continuous, closed-loop fashion for the RAN.

The use of industry-standard open APIs allows CSPs to abstract network complexity and transform the underlying network into a platform, thereby allowing northbound applications such as SDN controllers, OSS applications and partner applications to access the network in a standardized way. By applying a similar abstraction approach to each of the domains, CSPs can abstract the underlying domain-level complexities from the high-layer cross-domain functions, while continuing to automate at both the domain-level and at the end-to-end level. Moreover, workflow automation and robotic process automation techniques can be deployed to increase operational automation in legacy physical network domains. Broadly, these foundational capabilities enable CSPs to accelerate the journey towards level-5 autonomous networks, while continuing to manage and operate the existing physical networks cost effectively.

4.4 The cross-domain service automation layer stitches autonomous domains together for end-to-end service orchestration

To abstract the complexity of underlying network domains and enable the end-to-end creation and provisioning of services, multiple self-contained, autonomous domains can be brought together with a cross-domain orchestration layer. This layer will manage and orchestrate the customer-facing services over autonomous domains through intent-driven abstraction and open APIs/interfaces, and work in conjunction with OSS and business automation systems.

A key challenge for building this layer is the lack of industry alignment on intent-driven languages and data models. Several standardization efforts exist; for example, TOSCA is being widely used for service modeling, but the industry is divided in terms of the support and adoption of these standards, which is leading to slow progress, fragmentation and incompatibility issues. Waiting on standardization may stall progress, so some CSPs and vendors are forging ahead by creating variants of these standards or by building their own proprietary modeling languages, policies and interfaces to address their specific business and operational requirements.

AI/ML-powered service assurance will be another key part of cross-domain network and service automation. By applying AI/ML intelligence to assurance, CSPs will be able to perform a wide range of automation capabilities, including automated issue identification and root-cause analysis, automated anomaly detection and prediction, automated pattern discovery and automated creation of rules and policies. These can be combined with domain-level automation systems to perform open- and closed-loop automation in order to reduce the reliance on manual operations and manage complexity.

> *"5G is expected to support dynamic use cases where it will be critical to provision the networking functions at the right place at the right time. Autonomous networks will enable us to do this. The COVID-19 situation demonstrated that this capability is very important as we were able to automatically move the networking workloads to meet with changing needs. We will build on these learnings as we make our journey to autonomous networks."*
>
> **– Tier-1 converged group CSP from Western Europe**

4.5 AI/ML will be essential in all layers of autonomous networks

CSPs will need advanced AI/analytics capabilities in all networks at level 3 and above. Such capabilities can aid self-learning from fast-changing environments, provide accurate predictions of potential network problems and anticipate trends and ensure the continuous improvement and adaptation of the rules that govern autonomous operations. Our interviews revealed that advanced CSPs typically start with piecemeal, tactical implementations of AI/ML with various tools, methodologies and datasets that are specific to a network element, domain, use case or business problem. However, as they expand the number and scope of these individual implementations and their sub-components over time, they plan to join them together to create end-to-end operations with centralized data lakes and common tools, models, processes and governance. This suggests that autonomous networks should be developed with a layered AI/ML and analytics approach that is aligned with the hierarchical architecture discussed in the previous section. The three layers in this approach are described below (Figure 4.3).

- At the network infrastructure level, intelligent infrastructure with near real-time data collection and embedded AI/ML inference capabilities execute local closed-loop management scenarios based on domain-level or cross-domain level frameworks and algorithms.

- Domain-level data collection, intelligence, analytics and knowledge management will support variable degrees of automated decision making (levels 2–5) inside each autonomous domain. This layer should monitor, collect and analyse live data streams from intelligent infrastructure within a single domain, provide domain-specific insights and predictions and trigger actions based on policies and scenarios.

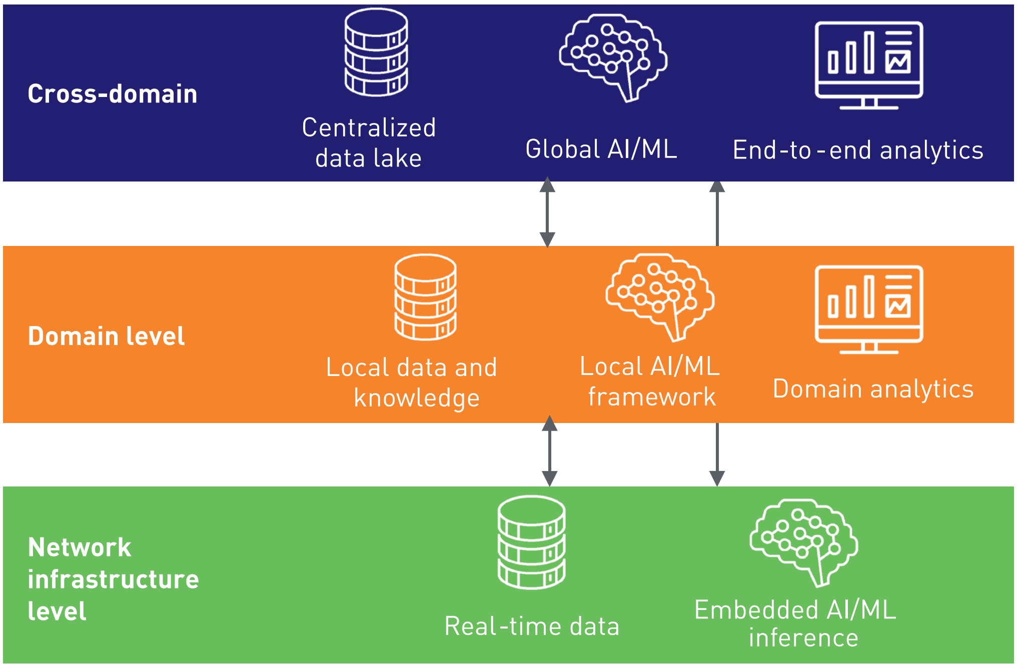
- CSPs will also need an overarching unified and centralized AI platform to enable cross-domain and complete closed-loop service automation. Such a platform is responsible for aggregating and federating data sources, generating AI/ML models and supporting cross-domain automation with end-to-end service insights, KPIs, predictions and actions.

A unified, centralized AI/ML and network analytics platform can accelerate the journey to a level-5 multi-domain autonomous network. It will allow CSPs to move away from a siloed approach of gathering network data, and towards a horizontal, unified platform that can record, process, aggregate and analyse all forms of data (log files, faults, transaction data and network telemetry data) originating from the autonomous domains.

The centralized data lake forms the crux of the data acquisition layer, as seen in Figure 4.4. It enables CSPs to ingest network data and create clean and curated outputs for further processing. The analytics layer processes the clean network data to generate reusable data structures and metadata in standard formats, which can then drive algorithms and ML/AI models. The models generate various outputs such as historical KPI trends, anomalies, insights and predictions in near real time, which can be combined with policy rules to generate and trigger autonomous actions and drive zero-touch closed-loop automation.

> *"We are already introducing AI, machine learning and big data analytics technology. We are making use of pretty much everything that is available in the market to accelerate our journey to autonomous networks."*
>
> **– Tier-1 Converged CSP from Western Europe**

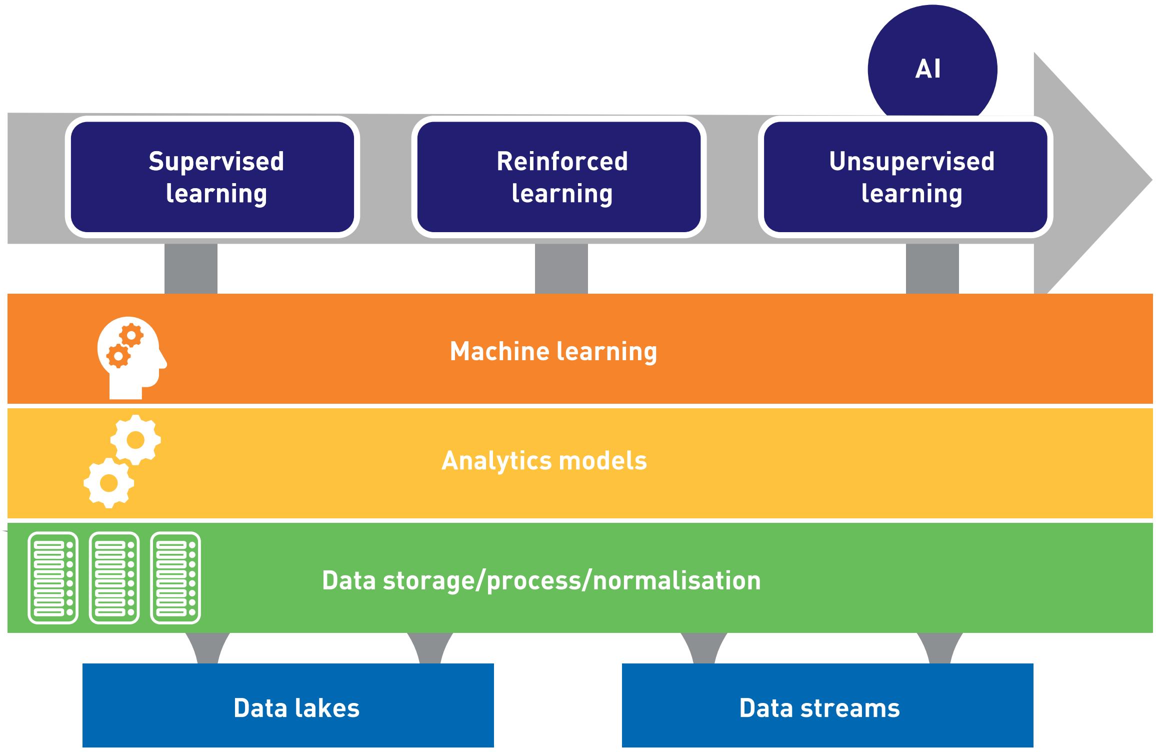
FIGURE 4.3: THE THREE-LAYERED AI/ANALYTICS APPROACH FOR AUTONOMOUS NETWORKS [SOURCE: ANALYSYS MASON, 2020]



CSPs can apply various ML/AI techniques such as supervised, reinforced, and unsupervised learning techniques, all of which are expected to play a critical role in achieving the autonomous network's vision.

- **Supervised machine-learning** algorithms can use historical operations data to identify patterns (for example, a degradation in network performance) and trigger remediation actions (such as scaling up network capacity) under predefined conditions in level-3 operations. The continuous calibration of these algorithms can increase the accuracy of pattern matching and decisioning and can pave the way to level-4 predictive operations. In predictive operations, the models predict network or service issues hours, days or even weeks in advance, thereby allowing sufficient time to take proactive remediation actions.
- **Reinforced learning** is when the machine-learning algorithm makes a single action, receives feedback about how good the decision was and calibrates its next move based on this feedback. The feedback loop is an important feature of this method; continued use of the loop fine-tunes the algorithms and increases the accuracy of predictions over time to a point where CSPs can fully trust the algorithms to make the right decisions.
- **Unsupervised learning algorithms** have not had prior training on how to classify or label patterns, but employ grouping or clustering to organize data in order to understand potential structures and patterns before predicting outcomes.

FIGURE 4.4: AN ILLUSTRATIVE EXAMPLE OF A UNIFIED NETWORK ANALYTICS PLATFORM [SOURCE: ANALYSYS MASON, 2020]



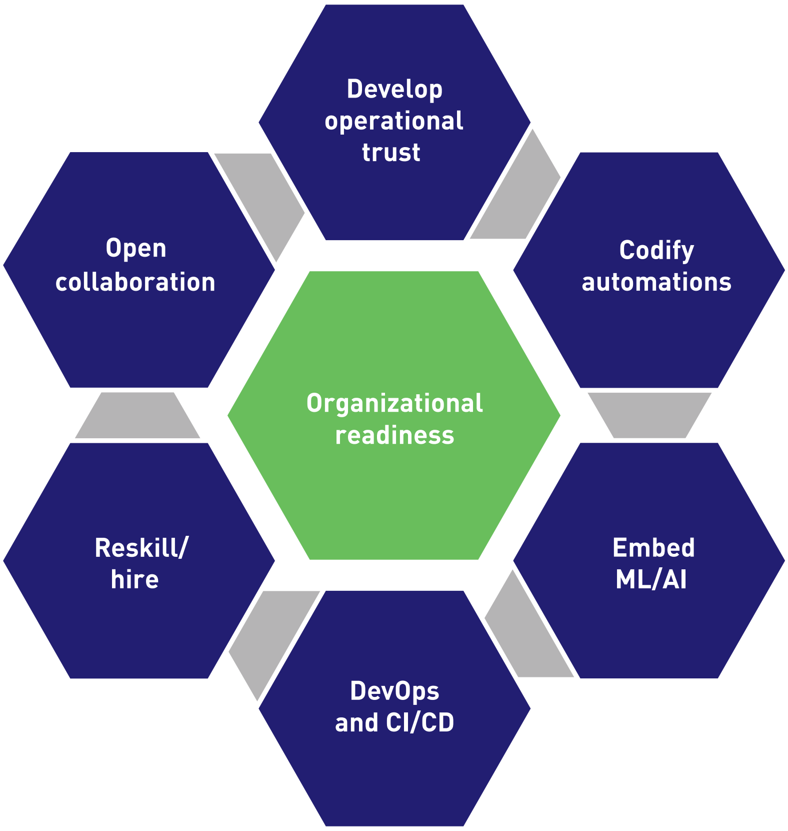
5 Preparing the organization for autonomous networks

The largest obstacle to making progress towards autonomous networks is organizational readiness. Highly skilled personnel in network engineering and operations departments have developed a rich body of knowledge that is often undocumented. This expertise is typically formed from years of performing manual procedures, so engineers tend to be more practical than strategic and are deeply resistant to change. CSPs can therefore find it extremely difficult to impose the new practices required to achieve the goal of autonomous networks. As such, CSPs need to devise a multi-pronged strategy to prepare their organizations for autonomous networks (Figure 5.1).

The evolution to autonomous networks will require an incremental approach, built on the foundation of operational trust. As part of this journey, CSPs should constantly pursue opportunities to automate, and should automate as many processes as possible. Engineers need to trust automations enough that they can completely relinquish control and let the automations drive operations; this is the end state of autonomous networks.

CSPs need to use advanced technology to develop incremental and partial automations in order to gradually ease engineers into trusting automations and should create a flexible automation framework that enables varying degrees of programmatic control and manual decision checkpoints. Using approaches such as microservices- and API-based programming techniques, engineers can codify the repetitive manual processes as reusable components, which can then be programmatically triggered and executed based on data-driven decision points and rules. Such a component-based software engineering approach enables the identification of repeatable manual tasks at the most granular level and codifies them into reusable software components to form the smallest unit of automation.

FIGURE 5.1: HOW CSPS CAN PREPARE THEIR ORGANIZATIONS FOR AUTONOMOUS NETWORKS [SOURCE: ANALYSYS MASON, 2020]



The decision checkpoints allow engineers to analyse the performance of the automation and decide upon the next best action. Once they have gained trust and confidence in the automations, CSPs can then embed ML/AI models to drive decision making and only enable manual interventions for approving or rejecting decisions.

DevOps and CI/CD processes and tools enable engineering and operations personnel to rapidly and continuously add automations to the production environment. This nurtures a culture of agile innovation by frequently delivering small chunks of incremental functionality. CI/CD processes mandate regular code delivery and the automated building, testing and deployment of code into a test environment, followed by the release to the production environment. DevOps and CI/CD also allow CSPs to adopt a fail-fast mindset by rapidly trialling new automations, retaining the ones that work, learning from the failed attempts and quickly moving on to the next iteration. With this approach, CSPs can realise quick wins and see the results in a matter of weeks, rather than months. Showcasing early successes to the key stakeholders and the senior executive team can increase confidence in the process and strengthen the case of continuous investment, thereby creating an agile virtuous cycle of automation delivery, benefit realisation and re-investments.

> *"It is not only a purely efficiency-driven motivation, but business continuity as well. Automating the backend processes reduces the dependency on people-driven processes."*
>
> **– Tier-1 converged CSP from Western Europe**

To realize the autonomous network's vision, CSPs also need to imbue their staff with a whole new set of skills. This is critical, especially during the early stages of the journey, when engineers are expected to 'own' the automations before the networks become truly autonomous in the latter stages of the evolution.

Staff will need to have programming skills in order to develop, maintain and continually update the automations. Skills in data design and data science will also be required to design data architecture and to develop, train and calibrate the analytical models and associated ML/AI algorithms. A large proportion of CSPs' existing employees do not possess these skills, and all CSPs will need to either hire or reskill or both.

CSPs will need to cultivate a culture for open collaboration between departments, especially the network engineering, network operations and IT operations departments. DevOps styles of working and co-operation across the network and IT domains is likely to threaten current ways of working, and employees may have little incentive to codify their knowledge if they are worried about losing their jobs. To avoid such pitfalls, CSPs should strive to re-educate their staff and make them key stakeholders in the journey towards autonomous networks.

Executing the organization transformation and the overall operational transformation to achieve autonomous networks will be complex and time-consuming with high business risks. Some CSPs with sufficient finances and a large appetite for risk may choose to execute the transformation themselves. However, the scale and scope of the transformation means that the vast majority of CSPs will require external support from vendor partners in many different areas, including consulting and advice, process re-engineering, software programming, cloud computing, virtualisation, big data architecture, data science and machine learning. Additionally, CSPs should consider vendor partners that:

- are deeply committed to the vision of autonomous networks
- can provide a CSP-specific roadmap to achieve autonomous networks
- can provide state-of-the-art operational technology and platforms that are built from the ground up to achieve the goal of autonomous networks
- offer innovative engagement approaches such as outcome-based and managed services models where the vendor can share some of the business and operational risks.

6 Conclusion and recommendations

CSPs are in the midst of a long journey towards autonomous networks. Our research for this whitepaper established that most CSPs are at level 2 in TM Forum's autonomous networks framework, though some advanced CSPs are operating some domains at level 3. The CSPs that we spoke to have built the technology foundations to either make the transition to level 3 or achieve a complete level-3 autonomous network.

To accelerate the journey towards autonomous networks, Analysys Mason makes the following recommendations for CSPs.

- **CSPs should have a roadmap for achieving autonomous networks.** As networks become more complex and dynamic, CSPs will find it increasingly difficult and expensive to manage them. In the current mode of operations, business processes such as network design, planning, fulfillment and assurance are highly disjointed, and often require manual interventions and inter-departmental handovers. This model is not sustainable in the emerging telco cloud network environment. CSPs will need a new operations model that is based on a vision for autonomous networks.

- **CSPs should pick a starting point and a preferred automation approach that can quickly yield results.** Automation approaches vary based on each CSP's market situation and business strategy. As a first step, CSPs should consider a domain-based automation approach with enabling technologies such as ML/AI, open APIs, network abstractions and orchestration to fully automate the domain. CSPs should also implement a horizontal cross-domain strategy for end-to-end automation.

- **CSPs should transform their organizations for autonomous networks.** Organizational transformation is much harder to achieve than technological transformation, but it is critical for success. CSPs should reskill their existing workforces alongside hiring new talent with the requisite DevOps and software engineering skills. CSPs should also consider seeking support and should adopt best practices from external vendors to ease and accelerate the journey of organizational change.

7 About the authors

Anil Rao (Principal Analyst) is the lead analyst for the Automated Assurance and Service *Design and Orchestration* research programmes, covering a broad range of topics on th existing and new-age operational systems that will power operators' digital transformations. His main areas of focus include service creation, provisioning and service operations in NFV/SDN-based networks, 5G, IoT and edge clouds; the use of analytics, ML and AI to increase operations efficiency and agility; and the broader imperatives around operations automation and zero touch networks. In addition to producing both quantitative and qualitative research for both programmes, Anil also works with clients on a range of consulting engagements such as strategy assessment and advisory, market sizing, competitive analysis and market positioning, and marketing support through thought leadership collateral.

Gorkem Yigit (Principal Analyst) is the lead analyst for the *Cloud Infrastructure Strategies* and *Media Platforms* programmes, focusing on producing market share, forecast and research collateral. His research focuses on the building blocks, architecture and adoption of the cloud-native, disaggregated and programmable digital infrastructure and networks that underpin the delivery of 5G, media and edge computing services. He also works with clients on a wide range of consulting projects such as market and competitive analysis, business case development and thought leadership collaterals.

William Nagy (Analyst) is a member of the Telecoms Software and Networks research team in London, contributing to various research programmes with a focus on *Automated Assurance, Service Design and Orchestration* and *Forecast and Strategy*. He previously worked with the regional markets team. William holds a BSc in Physics from Queen Mary University of London.

This whitepaper was commissioned by Huawei. Analysys Mason does not endorse any of the vendor's products or services.

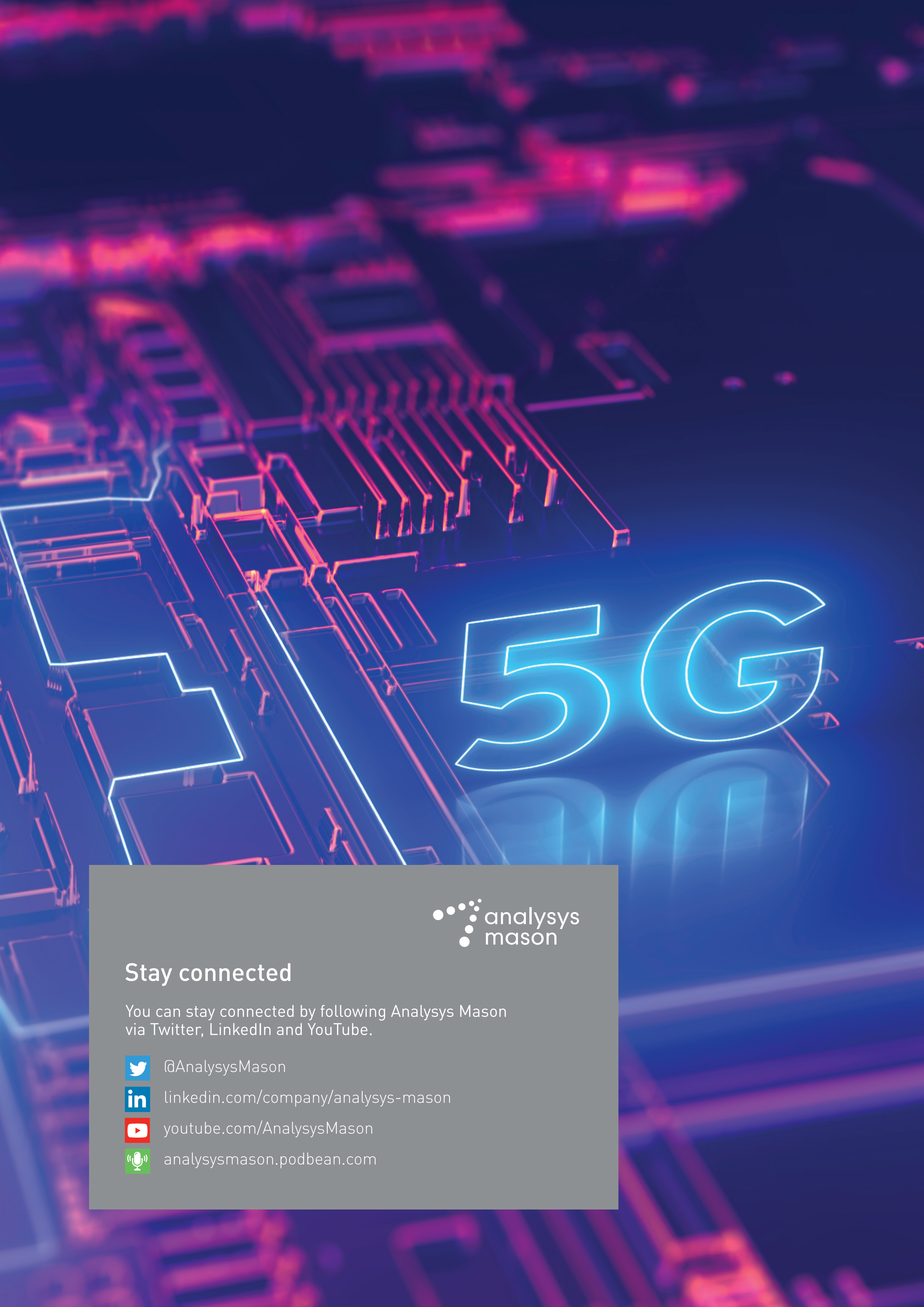
Learn more about Huawei's Autonomous Driving Networks proposition at https://carrier.huawei.com/en/adn.

Published by Analysys Mason Limited
North West Wing, Bush House
Aldwych
London WC2B 4PJ
UK
Tel: +44 (0)20 7395 9000
london@analysysmason.com
www.analysysmason.com
Registered in England and Wales
No. 5177472

Figures and projections contained in this report are based on publicly available information only and are produced by the Research Division of Analysys Mason Limited independently of any client-specific work within Analysys Mason Limited. The opinions expressed are those of the stated authors only.

Analysys Mason Limited recognises that many terms appearing in this report are proprietary; all such trademarks are acknowledged and every effort has been made to indicate them by the normal UK publishing practice of capitalisation. However, the presence of a term, in whatever form, does not affect its legal status as a trademark.

Analysys Mason Limited maintains that all reasonable care and skill have been used in the compilation of this publication. However, Analysys Mason Limited shall not be under any liability for loss or damage (including consequential loss) whatsoever or howsoever arising as a result of the use of this publication by the customer, his servants, agents or any third party.



Stay connected

You can stay connected by following Analysys Mason via Twitter, LinkedIn and YouTube.

- @AnalysysMason
- linkedin.com/company/analysys-mason
- youtube.com/AnalysysMason
- analysysmason.podbean.com