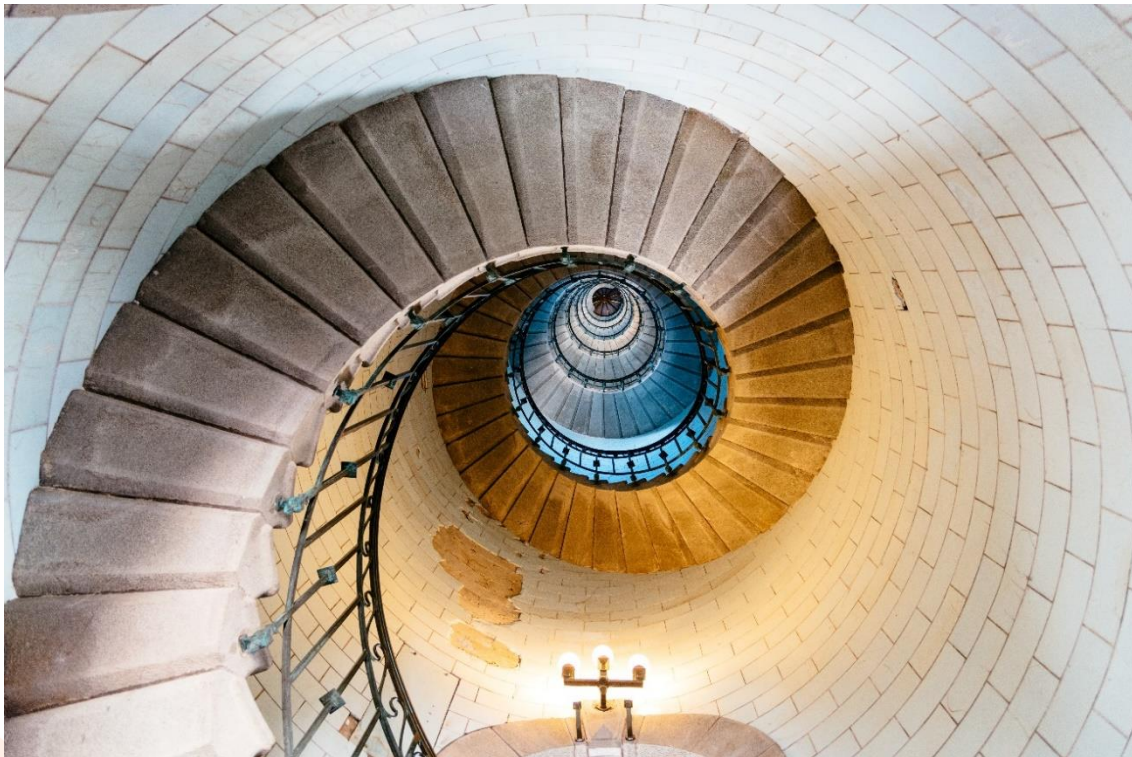




## Executive Briefing

# ACHIEVING NEXT-LEVEL NETWORK AUTONOMY

Implementing autonomous networks offers an average CSP cost savings and annual revenue uplift of around US\$794 million. However, challenges impede progress to realise this financial potential. This report addresses five of the main challenges faced by CSPs and provides recommendations to help overcome them.



# Executive Summary

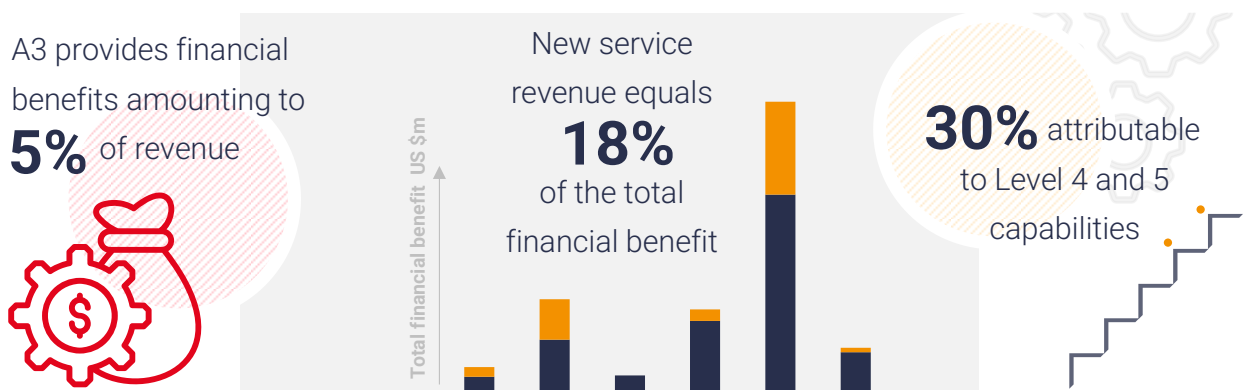
The drive to deliver profitable new service offerings amidst growing network complexity has become a common challenge for communications service providers (CSPs) across the industry. This requires CSPs to run networks with less human intervention. Leveraging insights from CSP interviews and secondary research, this report outlines the financial benefits of introducing automation and intelligence into networks and identifies the barriers limiting progression to higher levels of autonomous networks, providing key recommendations on how these can be overcome.

STL projects the implementation of AI and automation in the network will unlock US\$650 million yearly in capex and opex savings for an average CSP (one with around US\$15 billion in annual revenue, 31 million mobile customers, and 12 million fixed-line subscribers). On top of this, a further US\$144 million in value will result from revenue uplift from faster and more profitable service innovation. These financial benefits together amount to approximately 5% of an average CSP's revenue<sup>1</sup>. See Figure 1.

Further analysis showed:

- Resource management, service assurance, and network planning are the three network domains where AI and automation will have the biggest impact.
- 30% of the cost savings and revenue increase will only be unlocked by more sophisticated AI and automation (for example, when CSPs reach Levels 4 and 5 of autonomous networks).

**Figure 1: Estimated financial value of autonomous networks for an average CSP**








*Note: Total financial benefit includes capex and opex savings as well as revenue uplift*

Source: STL Partners

<sup>1</sup> STL Partners, Charlotte Patrick Research (2024), [Finding value from AI, analytics, and automation \(A3\) in the CSP network](#). An average operator is defined as having revenue of US\$15.6 billion, 31 million mobile subscribers and 12 million fixed subscribers. Note: This report outlines the full methodology. Some numbers have been iterated based on industry conversations.

Progressing to higher levels of network autonomy is imperative to manage this complexity. Despite its challenges, it is a journey worth pursuing, and critical to improve margins in an increasingly competitive market. As illustrated in Figure 2, this report identifies five crucial barriers that CSPs must overcome and proposes strategic measures to realise their ambitions. This will pave the way for CSPs to capture the substantial financial and operational benefits of advanced network autonomy.

**Figure 2: Barriers limiting the advancement of network autonomy**

	Key barriers	Mitigative efforts
 <b>01</b>	<b>Usefully interpreting industry frameworks and building a business case for nascent opportunities</b>	<ul style="list-style-type: none"> <li>Establish progress in automation to date, intent of new automated systems, and a clear roadmap based on best practice for meaningful adoption of use cases</li> <li>Converge network and IT functions to encourage cross-domain collaboration</li> </ul>
 <b>02</b>	<b>Accessing the right data at the right time from multiple domains and systems</b>	<ul style="list-style-type: none"> <li>Establish common, transparent, and accessible data structures to organise data across domains</li> <li>Gauge an understanding of process workflows and infrastructure dependencies to identify which tools and platforms to share</li> </ul>
 <b>03</b>	<b>Ensuring people trust systems to deliver high-quality outcomes</b>	<ul style="list-style-type: none"> <li>Define clear policies, ethical guidelines, and governance to reskill and upskill people for high quality human-to-machine interactions</li> <li>Ensure comprehensive documentation for successful network design</li> <li>Create automated feedback loops to continuously monitor and improve systems</li> </ul>
 <b>04</b>	<b>Overcoming the unique risks of AI-driven innovation in mission-critical environments like the network</b>	<ul style="list-style-type: none"> <li>Establish robust AI and MLOps frameworks to effectively leverage network data</li> <li>Engage in partnerships with network and IT specialists</li> <li>Establish cross-organisational reporting mechanisms to assess the returns and risks of key initiatives</li> </ul>
 <b>05</b>	<b>Understanding the role of generative AI in the network</b>	<ul style="list-style-type: none"> <li>Consider critically where generative AI can add value in the networking domain</li> <li>Ensure learnings from other telco business units are shared e.g., around skills, risk mitigation, and best practice experience</li> </ul>

Source: STL Partners

# Table of Contents

Executive Summary..... 2

Introduction..... 6

The US\$800 million opportunity: The estimated impact of network autonomy ..... 8

CSPs must overcome five barriers to achieve autonomous networks ..... 11

    Usefully interpreting industry frameworks and building a business case for nascent opportunities ..... 11

    Accessing the right data at the right time from multiple domains and systems..... 14

    Ensuring people trust the systems to deliver high-quality outcomes ..... 15

    Overcoming the unique risks of AI-driven innovation in mission-critical environments like the network..... 16

    Separating fact from fiction: Understand the role of Generative AI in the network..... 17

Conclusions and recommendations ..... 19

# Table of Figures

Figure 1: Estimated financial value of autonomous networks for an average CSP .....	2
Figure 2: Barriers limiting the advancement of network autonomy .....	3
Figure 3: TM Forum's autonomous networks maturity model and example use cases .....	7
Figure 4: Financial value of autonomous networks, Level 1/2/3 vs. Level 4/5 .....	8
Figure 5: Upside of automating vs. downside of not automating.....	9
Figure 6: Service lifecycle management and the differentiating autonomous-level capabilities.....	12
Figure 7: CSPs' commitment to network autonomy .....	13

# Introduction

CSP networks are growing in complexity. The amount of data they generate and require to function is increasing and network-tied services are growing more diverse (for example, private networks and network slicing). Steve Jarrett, Chief AI Officer at Orange reveals that they are managing petabyte-scale data daily from network telemetry alone<sup>2</sup>. Handling this complexity demands change. Traditional human-driven operational models fall short of managing this dynamic operating environment with the coexistence of legacy networks and next-generation technologies.

Taking AI and automation to the next level, to autonomous networks, requires a fundamental shift from executing simple rules-based tasks to orchestrating complex processes with minimal human oversight. This transition can create faster and error-free network operations. To achieve this, CSPs must implement automation across domains (access, transport, and core networks) and vertical stacks, and implement advanced intelligence for more agile learning and decision-making. Achieving autonomous networks is imperative to creating more effective business outcomes. This includes ensuring services never fail by uncovering hidden issues and pre-empting problems that would have not otherwise been anticipated, and reducing the dependency on humans to operate networks, enabling CSPs to develop more state-of-the-art services.

The TM Forum's Autonomous Network Maturity Model<sup>3</sup> is a globally recognised framework used to evaluate CSPs' advancement toward network autonomy (see



The industry on a whole has an average autonomous network level of around 2.5.



– Andy Tiller, EVP of Member Products and Services  
at TM Forum (via Telecom TV)

---

<sup>2</sup> Google Cloud (2024), [Using AI and Edge Infrastructure to Dynamically Analyse Petabyte Scale Data](#)

<sup>3</sup> TM Forum (2022), [CSPs' progress towards autonomous networks](#)

Figure 3 for a detailed breakdown). Many CSPs have achieved Level 1 or 2 automation to date, with most network operations still facilitated by some degree of human intervention or oversight. CSPs want to pursue system-wide automation to reach Level 4 automation and beyond, but they face challenges.



**Figure 3: TM Forum's autonomous networks maturity model<sup>4</sup> and example use cases**

Level	Description	Example use case
<b>LEVEL 0</b> Manual management	Network operations are handled manually, with no assisted automation systems or capabilities. This spans from design to operations and assurance.	Telephone exchanges where people were manually connected to other telephone lines
<b>LEVEL 1</b> Assisted management	Some automation is introduced to assist (routine) operations managed by humans. Humans continue to play a central role in decision-making and performing most tasks.	<b>At the individual component or domain level:</b> <ul style="list-style-type: none"> <li>• Radio planning prediction models</li> <li>• Trouble ticket management</li> <li>• Order-to-cash process (e.g., order management, self-serve capabilities on customer portals)</li> <li>• Root cause analysis</li> <li>• Capacity management</li> <li>• Optimise parts of the network</li> <li>• Network configuration</li> </ul>
<b>LEVEL 2</b> Partial autonomous networks	Automation is more advanced, with some tasks run autonomously. There is significant reduction in manual interventions through closed-loop operations in set environments.	
<b>LEVEL 3</b> Conditional autonomous networks	The network operates autonomously under predefined conditions and systems can capture real-time changes to the environment. In some domains, operations can be optimised to enable intent-based, closed-loop management. Humans in the loop handle complex tasks and high-level decision making.	
<b>LEVEL 4</b> High autonomous networks	The network operates highly autonomously in cross-domain environments, with minimal human oversight. Manual intervention is limited, with human operators mostly involved in overseeing processes and driving unique strategic decisions.	<b>At the cross-domain level:</b> <ul style="list-style-type: none"> <li>• Proactive fault identification, management, and resolution</li> <li>• Intent-based service orchestration</li> <li>• Resource management</li> <li>• Zero-touch operations</li> <li>• End-to-end lifecycle management for services and network slices</li> <li>• More complex network optimisation</li> <li>• Self-healing loops for service assurance</li> <li>• Dynamic SLA management</li> </ul> <i>Note: use case list is non-exhaustive</i>
<b>LEVEL 5</b> Full autonomous networks	Network operates entirely autonomously, with no manual participation in managing, organising, or optimising processes. Through closed-loop, intent-based automation capabilities, processes are designed to learn, adapt, and evolve continuously without human input across domains and the end-to-end lifecycle.	

Source: TM Forum, STL Partners and Charlotte Patrick Research analysis

To move beyond Level 3 automation, CSPs must pivot from intra-domain automation to inter-domain automation. Intra-domain automation are siloed automation efforts focusing on the automation of isolated workflows or processes. In comparison, inter-domain automation focuses on the integration of automation across domains, teams, and processes. To achieve highly autonomous networks (Level 4 or 5), CSPs must also add intelligence into their automated processes. For instance, instead of using automation to do the same process as previously would have been done manually, adding intelligent decision-making systems means that the processes continuously change and adapt to deliver the most efficient and accurate outcomes. These shifts (intra- to inter-domain, simple automation to intelligent automation) can unlock significant opex and capex savings, and new monetisation opportunities through better allocation of human capital towards service innovation.

This report leverages key insights from CSP interviews and secondary research to set out the financial benefit of introducing automation and intelligence in the networks and identifies the conditions CSPs need to create to progress to greater autonomy.

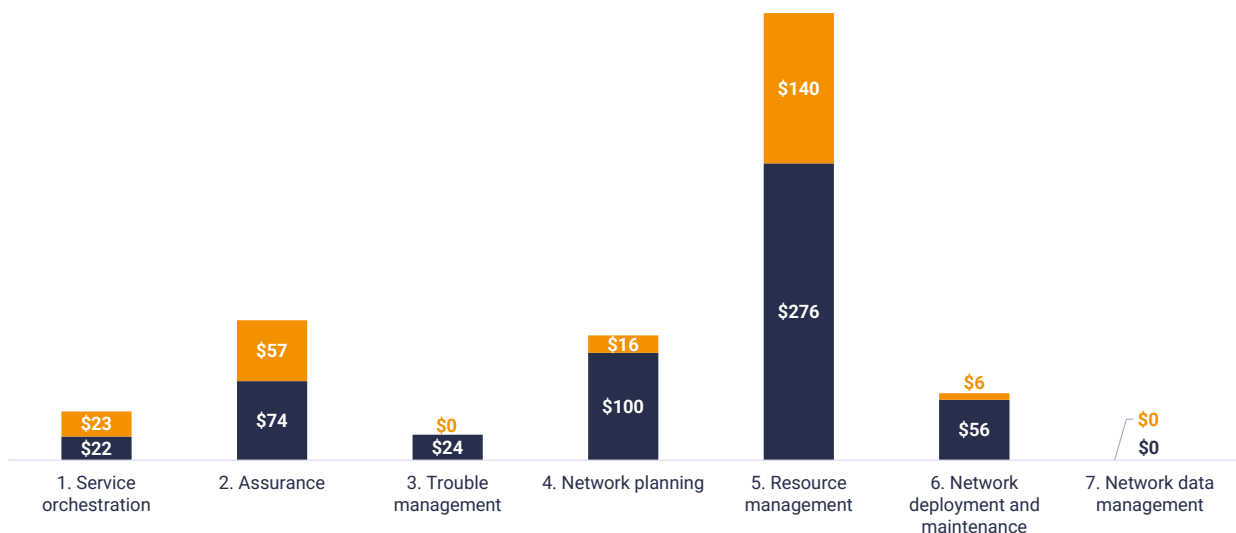
<sup>4</sup> TM Forum (2022), [CSPs' progress towards autonomous networks](#)



# The US\$800 million opportunity: The estimated impact of network autonomy

STL estimates that deploying AI, automation, and analytics in the network can yield annual capex and opex savings of approximately US\$650 million for an average CSP over a five-year period<sup>5</sup>. Of this, around US\$300 million of the total cost savings is attributed to capex savings and US\$350 million is opex savings. On top of this, a further annual revenue uplift equivalent to approximately US\$144 million is expected from newer, faster, and more profitable, services – this translates to around 18% of the total financial benefit (Figure 4). These financial benefits amount to approximately 5% of an average CSP's revenue. Further analysis suggests that implementing Level 4 and 5 capabilities contribute to around 30% of the total financial benefit.

**Figure 4: Financial value of autonomous networks, Level 1/2/3 vs. Level 4/5**



Source: STL Partners, Charlotte Patrick Research

Resource management, service assurance, and network planning are the three domains expected to generate the most benefits. More complex, self-healing use cases produce significant value in assurance and there is also significant value in using automation and AI to help to design, run and optimise a cloud-native network.

Use cases benefiting from Level 4 or 5 capabilities include:

<sup>5</sup> STL Partners, Charlotte Patrick Research (2024), [Finding value from AI, analytics, and automation \(A3\) in the CSP network](#). An average operator is defined as having revenue of US\$15.6 billion, EBITDA of US\$8.3 billion, 31 million mobile subscribers, and 12 million fixed subscribers.

Note: This report outlines the full methodology. Some numbers have been iterated based on industry conversations.

- **Resource management:** Dynamic and intelligent management of resources and power across domains based on patterns in usage and demand, automating load distribution across the cloud. This requires provisioning the network beyond the RAN.
- **Service assurance:** Monitoring network performance as close to real-time as possible to manage faults and troubleshoot across domains based on root-cause analysis and predictive capabilities.
- **Network planning:** Move from leveraging simple visualisation tools to understand the network and analyse traffic for capacity management, to more advanced and intelligent orchestrations across multiple domains that can self-optmise.

“Using AI and automation for service assurance has been very successful for us. We’ve seen a 75% reduction in total incidents in 10 years and have had zero A-severity incidents in 8 years.”

– Automation Manager, and CIO, Tier 1 EMEA operator

Across the other potential use cases (including service orchestration and network maintenance), STL expects less significant value to be unlocked. Most AI and automation use cases have a larger impact at lower autonomous levels – hence, much of the financial benefit is realised at these levels. Secondly, some categories (such as data management) are assumed to have a support function role, for which its value is distributed more horizontally across several use cases and does not have specific value of its own. Although these domains require less advanced automation and intelligence capabilities and have smaller financial implications, they are nonetheless important. CSPs must establish simple tools and technologies (such as robotic process automation) to ensure processes are as efficient as possible and optimally underpin other network processes as CSPs strive towards end-to-end autonomous networks.

**Figure 5: Upside of automating vs. downside of not automating**

STL’s estimate of nearly US\$800 million in financial value for an average CSP captures the concrete, measurable benefits of autonomous networks. However, the numbers are potentially underestimated because it does not fully capture the upside opportunities in terms of new service development and downside risks of stalling at Level 3.

Upside of automation:	Downside of not automating:
<ul style="list-style-type: none"> <li>• STL forecasts revenue uplift of US\$144m from network automation.</li> <li>• This increase reflects the direct value of more autonomous and intelligent network technology, through:               <ul style="list-style-type: none"> <li>– Reduced churn</li> <li>– Improved availability</li> <li>– Increased usage of networks owing to on-demand and efficient service provisioning.</li> </ul> </li> <li>• However, it does not include potential value linked to:               <ul style="list-style-type: none"> <li>– Investment in entirely new services</li> <li>– Sales and marketing capabilities</li> <li>– Commercial relationships that leverage more autonomous networks</li> </ul> </li> <li>• This presents upside opportunities for operators with strong commercial strategies.</li> </ul>	<ul style="list-style-type: none"> <li>• Traditional CSPs face significant risks by not automating and developing on-demand services</li> <li>• One is the risk of being <b>crowded out the market by competitors.</b></li> <li>• Existing services built into monolithic architectures are less agile and difficult to integrate into the wider service ecosystem.</li> <li>• So, CSPs may underperform with revenues below industry averages.</li> </ul>



Source: STL Partners

Intent is another key enabler for higher levels of autonomy. Intent-based technology enables CSPs to set the goals and parameters for automated systems and AI models without prescribing the specific actions needed to be taken to get there. This approach allows the network to adapt more fluidly to business needs and help expand CSPs' business opportunities by simplifying the process of defining these needs and making the process less technical or standards oriented. Intent-based automation can therefore free up resource for service innovation, enabling CSPs to generate novel solutions which go beyond what is possible with human-defined instructions and boost network monetisation.

Telstra has recognised this possibility, adopting a holistic approach to unify inventory management across domains and integrate open technologies to orchestrate and streamline operations. Automation across the service lifecycle has simplified network architectures, reducing service complexity and enabling near real-time provisioning of existing and differentiated use cases. As a result, Telstra has accelerated time-to-market for advanced offerings such as network-as-a-service which benefit from the resilient networks and improved latency. Consumer and enterprise customers increased access to these new and high-quality offerings have positively influenced customer experiences<sup>6</sup>.

To capitalise on this opportunity, CSPs must begin by mapping out the network processes that are ripe for applying advanced automation and intelligence. By channelling investments towards network domains that are expected to yield substantial returns – such as those highlighted in Figure 4 – CSPs can modernise their infrastructure and transition to more progressive operating models. Following this, there are five other barriers CSPs are facing on their journey to network autonomy, which they need to address. This report explores these challenges and proposes strategies for overcoming them.

---

<sup>6</sup> Noka (2022), [Nokia deploys Orchestration Centre software for Telstra to drive enhanced automation and customer experience](#)

# CSPs must overcome five barriers to achieve autonomous networks

Below are the five crucial barriers that CSPs must overcome to capture the substantial financial and operational benefits of advanced network autonomy.

## Usefully interpreting industry frameworks and building a business case for nascent opportunities



Usefully interpreting industry frameworks and building a business case for nascent opportunities



TM Forum's Autonomous Networks Maturity Model (as explained in

Figure 3) offers a framework for CSPs to gauge their progress towards autonomous networks. However, until recently its definitions have not been prescriptive, allowing for subjective interpretations that can complicate benchmarking maturity against other industry players. The Forum's AN Project has now normalized the detailed scoring for two scenarios (fault management on RAN and core networks) and is working through other high value scenarios to eliminate subjectivity from the AN Level scoring.

“

Through enhanced use of data and AI at Level 4 autonomy, our network will be, more agile, more effective, more resilient, and higher performing.


”

- Laurent Leboucher, CTO at Orange and SVP at Orange Innovation Networks (via [Mobile Europe](#))

Levels 1 to 3 focus on intra-domain automation that reduce manual effort and accelerate processes. In contrast, Level 4 and 5 autonomous networks demands a holistic, end-to-end approach.

Figure 6 delves deeper into service lifecycle management as an example, capturing the difference between some autonomy (Levels 1 to 3) and achieving high or full autonomy (Level 4+).

**Figure 6: Service lifecycle management and the differentiating autonomous-level capabilities**

		Level 1/2/3	Level 4/5
	<b>Service lifecycle management</b>	<ul style="list-style-type: none"> <li>Up to L3, provisioning the access is sufficient to meet service needs in single domain automation</li> <li><b>Levels 0/1</b> – Services are manually developed, with basic automation applied to a simple process within predefined boundaries</li> <li><b>Level 2</b> – Manual effort is reduced. Service operations autonomously adapt to certain network events within defined environments</li> <li><b>Level 3</b> – Service operations dynamically adjust to support higher volumes based on real-time data, whilst within the set rules</li> </ul>	<ul style="list-style-type: none"> <li>Level 4+ automation requires provisioning the transport and core to support inter-domain activities</li> <li>Dynamic and intent-based service orchestration and assurance leverages advanced automation and intelligence capabilities</li> <li><b>Level 4</b> – More complex services can self-optimize based on real-time analytics to improve performance and reduce opex</li> <li><b>Level 5</b> – Service operations are fully autonomous with little to no human intervention</li> </ul>
	<b>Examples</b>	<ul style="list-style-type: none"> <li>Automations in customer self-service portal and order management</li> <li>Automated troubleshooting within the fulfilment processes</li> <li>Automated resource allocation in a single domain and management of network inventory</li> </ul>	<ul style="list-style-type: none"> <li>New services are designed automatically using closed-loop feedback mechanisms to monitor and improve service offerings</li> <li>Spin up network resources across domains as traffic increases for E2E lifecycle management of network services</li> <li>Automated assurance to recover quickly from service faults</li> </ul>

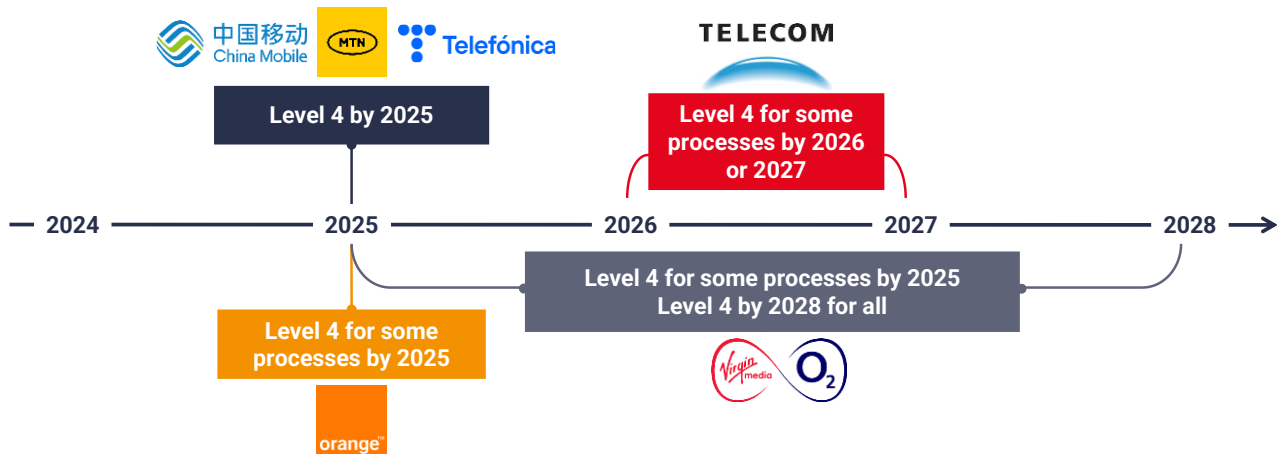
Source: STL Partners

The reason that TM Forum's framework is important is because CSPs are inherently key performance indicator (KPI)-driven organisations. In fact, many CSPs have announced their commitment to achieving Level 4 autonomy in the next few years (see **Error! Reference source not found.**). With an average autonomous level of 2.85 as of 2023, China Mobile is one CSP making significant strides in this space, aiming for Level 4 autonomy across its RAN, mobile core, IP, optical and telco cloud networks by 2025<sup>7</sup>. Orange is another CSP with similar ambitions, looking to maximise the value of its core infrastructure-based activities to move from Level 1 or 2 to Level 4 autonomy<sup>8</sup>.

<sup>7</sup> TM Forum (2023), [China Mobile aims for widespread network autonomy by 2025](#)

<sup>8</sup> TM Forum (2023), [Orange sets ambitious autonomous network operation goals](#)



**Figure 7: CSPs' commitment to network autonomy**

Source: Various

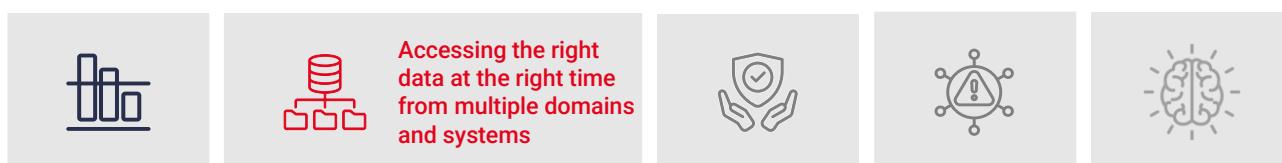
Despite it being a strategic priority for many CSPs, they often lack a clear roadmap. During STL's research programme, one CSP mentioned that while it had made a C-suite commitment to achieving Level 4 automation, it did not believe that, at each domain level, it really had a clear plan for achieving its objectives.

It is therefore critical for CSPs to take a measured approach to understand their current progress and develop a clear path forward. This process should include the following steps:

1. Understand the maturity of its automation efforts to better understand the degree of autonomy they have achieved to date.
2. Establish the extent to which use cases can be made autonomous, as some operations will always require intervention by a field technician. This will also support the business case for future investments by pinpointing areas where automation and AI are most impactful.
3. Assess the impact of use cases on other domains and systems such as BSS systems. A balance may have to be struck if older, more monolithic systems cannot support the autonomous use case.
4. Identify byte-size use cases to focus automation applications and resolve specific problems. This is necessary to guarantee use cases deliver measurable benefits and allow CSP progression to greater autonomy.
5. Define the desired outcome and the parameters of the automated systems to solve the fundamental problem at hand and achieve intent-based automation.

These steps sound simple but can be challenging. Prescribing and achieving a common goal across domains necessitates cross-domain input from many process experts and domain owners, who each require an end-to-end view for better lifecycle management. Hence, successful automation hinges on the establishment of cross-functional teams, led by C-suite champions who can align network and IT domains (for instance, a CTIO group). This is especially important as networks become more cloud-based and software-driven as the opportunity to consolidate automation initiatives, technologies, and platforms across domains to achieve a common goal has expanded.

## Accessing the right data at the right time from multiple domains and systems



Cross-domain, cross-process interoperability is necessary to reach higher levels of autonomous networks. This necessitates seamless access to the right data at the right time from multiple systems. And, of course, this data has to be accurate and of a high quality. To achieve this, CSPs must implement common, transparent, and accessible data structures to ensure workflows capture and organise appropriate data in a logical order. Data must be correlated, and interdependencies and relationships need to be identified.

CSPs encounter several challenges with their data management systems and practices, such as:

- **Inconsistencies in internal data structures and reporting methods across different domains.** This is exacerbated by having different generations of networking technology running concurrently. To mitigate this, CSPs must engage with their current and historic network vendors to ensure that data extraction and modernisation is being made available across all deployed network functions and domains. CSPs must also implement dynamic reporting to continuously update data, ensuring a timely and accurate representation of network status is available for improved decision-making.
- **Ensuring data security and compliance while using a unified data framework.** Bringing all networking data into a single data lake creates new potential risks. Instead, a data mesh with a single unified framework can be more effective. To achieve this, CSPs must roll out mature and well-documented data management training and practices, as well as automatic permissioning for who can view and access what data. Compliance to data privacy and sovereignty regulations, such as GDPR which strongly governs the European market, is essential to access the right data safely.
- **Balancing domain-specific progress with investing in common tools and platforms** to try to not stagnate progress while also future-proofing for more cross-domain efforts. These tools should be selected based on a set of criteria which frame key requirements across specific domains into a broader overarching goal.

- **Avoiding vendor over-reliance or lock in.** CSPs should ensure that any vendors which support with data management platforms have a demonstrated commitment to using open standards and clear documentation on the data migration process and effort for if the CSP wanted to move away from using its solution.

A centralised data repository, with network telemetry being captured in near real-time, paves the way for the creation of a digital twin of the network. Digital twins create a near real-time virtual replica of the physical counterpart, allowing CSPs to proactively assess scenarios under which a new service or input is introduced before deployment. This minimises operational risks of service disruptions and downtime. They also allow CSPs to test use cases which can be too costly to do in the physical domain – for instance, consider fibre planning and deployment which is capital-intensive.

Although digital twins are nascent and lack widespread adoption, initial progress is being seen in digital inventory programmes and partial network simulations. One priority area is the role of digital twins for experimentation in the RAN, since overall network opex and capex spend in this domain is so high, and there exists a large number of scenarios around planning and maintenance of network architecture, service roll out, and coverage.

## Ensuring people trust the systems to deliver high-quality outcomes



In previous sections of this report, we highlighted the significance of advanced automation and intelligence in achieving greater network autonomy. Over time, networks have evolved significantly with the advent of next-generation technologies, and, equally, the skills required to manage them must also progress. This helps bridge gaps between legacy skill sets and those needed for modern, cloud-native network management. The ability to harness automation and AI well comes down to the ability of network engineers and architects to effectively employ these tools to optimise existing processes but to also build their own use cases. This requires reskilling and upskilling – a crucial step in the technical and organisational change management process to establish high-quality human-machine interactions for governance, reportability, and observability.

In STL's research programme, the Automation Director at a Tier 1 EMEA-based operator mentioned that they are evaluating skill requirements on a bi-annual basis and developing training programmes to enhance employee skills. This proactive approach in training has been critical to retain essential process experts with crucial CSP-specific knowledge. They also mentioned that some industry players are forging partnerships with ecosystem players such as network and IT specialists to ensure people readiness for more advanced automation and AI.

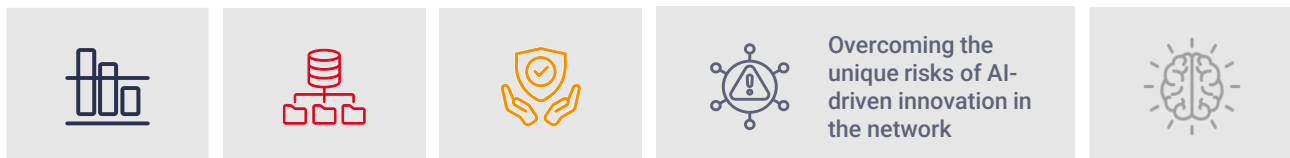
“To transform to Level 4 network autonomy, it's not only us who have to change. Our ecosystem, including vendors, system integrators, hyperscalers, and software providers, will have to reskill or upskill people to drive this change forward”

- Juan Luis Mulas, Head of Telco Cloud, OSS, and automation at Orange Spain (via [Mobile Europe](#))

To augment these efforts, CSPs need to define clear policies, ethical guidelines, and governance for people to trust the systems designed to deliver autonomous outcomes all the while being reliable, accurate, and in line with quality of service and service-level agreements (SLAs). This starts with people thoroughly documenting key processes using appropriate knowledge management tools. This is crucial to not only preserve the knowledge of key processes within the organisation during the rollout of automation initiatives, but also facilitate better integration across both existing and new components and networks. Comprehensive documentation can also help upskill software engineers and AI experts to understand specific network protocols and processes.

Creating automated feedback loops is another way to monitor incidents and continuously improve systems. This automation enables humans to step out of the loop of routine, manual tasks to instead focus on more complex decision-making processes and agile service innovation, leveraging their expertise where it adds the most value to the organisation.

## Overcoming the unique risks of AI-driven innovation in mission-critical environments like the network



CSPs are focusing on AI in the networks to reduce the risk of overlooking incidents, making manual errors, or not tending to network faults with speed and precision before it impacts the end customer. Despite these possibilities and a demonstrable value attributed to AI (with automation and analytics) as seen in Figure 4, implementing AI into network systems also creates its own set of unique risks, unlike those in comparably less mission-critical domains like customer care or sales and marketing. Transparency and accountability in network AI are crucial – if an AI algorithm makes a recommendation that disrupts network coverage, there must be a single stakeholder within the CSP who takes responsibility for this outcome.

To mitigate these risks, CSPs must deploy robust machine learning operations (MLOps) frameworks to effectively leverage network data, while ensuring compliance with SLAs and regulations. MLOps provides a framework for end-to-end data management, enabling essential continuous

integration/continuous deployment workflows to happen autonomously. Key areas of focus should include:

- Implementing automated feedback loops to fine-tune and retrain models consistently.
- Monitoring and validating models continuously to ensure their effectiveness and identify model drift.
- Scaling and deploying models in an agile manner to manage increasing data volumes.

“Using AI within networks is uniquely complex. You require full MLOps to check for drift and retrain the models.”

– Head of Artificial Intelligence, Tier-1 NAM operator

Establishing artificial intelligence operations (AIOps) is also crucial. It is necessary to effectively implement AI across multiple systems, processes, and domains. Given the volume of data generated from multiple sources across an intricate network, AIOps uses AI to gather and correlate data from various sources and domains across the network to perform predictive analytics and automatically generate insights. These insights are used to facilitate proactive, closed-loop actions for network optimisation. Some areas where AIOps is instrumental include:

- Troubleshooting for network faults, detecting anomalies, and filtering out noise or false alarms in the network operations centre to isolate potentially critical network issues.
- Driving automated incident response to mitigate network threats and self-healing measures to prevent service failures and downtime.
- Proactive service planning to enhance performance and manage energy consumption.

Finally, CSPs should implement reporting mechanisms to continually assess the returns and risks of their automation and AI initiatives. As part of STL's research programme, the Automation Director at a Tier 1 EMEA operator also revealed that they have seen value from automation of processes like service design and assurance. This was identified through monthly assessments of automation and AI project outcomes aggregated to capture a cumulative annual value. Teams responsible for sub-processes report this data to workstream leads, which is then amalgamated across the network. This helps the CSP to pinpoint high-value areas and identify potentially riskier areas.

## Separating fact from fiction: Understand the role of Generative AI in the network



Understanding the role of generative AI in the network

Networks produce a lot of structured data which is harnessed in automation use cases. Traditional AI and ML algorithms (along with rules-based automation) are well placed to do this sort of analysis. However, to reach Level 5 autonomous networks, generative AI (Gen AI) will be required. This is because it introduces a capacity for generating new insights from unstructured data. For example, ML is well able to do pattern recognition to identify an anomaly. Gen AI, however, is able to do the pattern

recognition, and then autogenerate other versions of this same pattern and flag to the system that these other versions should also proactively be monitored for. CSPs should ensure they have investment and implementation strategies for both ML and Gen AI – the former to analyse structured data while the latter integrates and correlates insights from various ML models.

CSPs are exploring the use of Gen AI in the network, though only about 5% of Gen AI deployments are applied in the networks, according to STL's Gen AI adoption tracker<sup>9</sup>. Some applications indicate a clear role for embedding Gen AI in network operations and maintenance. As part of China Mobile's phased approach to Level 4 autonomous networks by 2025, its collaboration with Nokia to incorporate Gen AI and AIOps frameworks has resulted in US\$7 million in operational savings by enabling engineers to efficiently query knowledge bases for resolving network faults and drive cost efficiencies in data analysis<sup>10</sup>. Other use cases which help bridge Level 4+ capabilities include:

- Autogenerating rules to forecast data trends, identify anomalies, or map data to measure KPIs.
- Creating synthetic data to train models on various scenarios and evaluate operational changes in digital twins.
- Turning customer requests (e.g., for a slice optimised for video transmission) into relevant network service design and KPIs (e.g., in this example into a guaranteed minimum uplink).

The exploration of Gen AI in the networks is set to unlock value, but it is still at an early stage. CSPs should take a cautious approach, recognising its potential but balancing feasibility against the risk of complex deployments. In the short term, CSPs should focus on low hanging fruit use cases such as digital assistants and troubleshooting systems. Doing this will ensure investments are made where they can generate the most impact, steering clear of costly ventures with unproven returns. It also gives CSPs the time to find the right talent to resolve any potential risks (e.g., security or SLA violations), thus safeguarding customer experience.

“AI is crucial to advance to Level 4+, but it is important to define a role for this in the network and assess the impact on manual effort, quality and other technologies. We have added AI to our BSC”

– Automation Director, Tier-1 EMEA operator

<sup>9</sup> STL Partners (2024), [CSP generative AI adoptions tracker](#)

<sup>10</sup> TM Forum (2024), [China Mobile's new GenAI solution leads to \\$7 million in opex savings](#)

## Conclusions and recommendations

CSPs face a myriad of challenges when pursuing more complex automation and intelligence initiatives, yet this is crucial for greater autonomy. CSPs' end goal should focus on unlocking the added financial value that Level 4 or 5 autonomy offers and enabling differentiated customer experience through reallocation of resources to develop new and more performant network-based services. So where do CSPs start?

CSPs should start by addressing the following five core barriers, implementing the fundamental enablers that allow them to reach next-level autonomy:

**Finding relevant best practice and usefully interpreting industry frameworks.** CSPs must adopt a structured approach to define and implement a clear roadmap for achieving advanced autonomous network goals. This involves assessing the current maturity of automation efforts, understanding the extent of potential autonomy of network use cases, evaluating impacts across domains, and defining precise outcomes for intent-based automation. These efforts will need to be coordinated by cross-functional teams to align efforts across increasingly cloud-based and software-driven networks.

**Accessing the right data at the right time from multiple domains.** CSPs must implement a data mesh with a unified data framework. This involves standardising data aggregation processes and centralising it into a single pipeline through application programming interface exposure for continuous availability of high-quality data across domains. Crucial for deriving accurate insights, cross-domain data correlation not only informs the development, testing, and deployment autonomous systems, but also drives operational decisions and actions which minimises errors and biases. Additionally, CSPs should carefully consider their strategic partnerships with ecosystem players to ensure the tools provide both short-term value and long-term future proofing. This will need to internalise cross-domain requirements and ensure vendor solutions support open standards.

**Ensuring people trust systems to understand requirements and execute instructions to deliver high-quality outcomes.** CSPs must ensure comprehensive documentation of network protocols for knowledge management purposes and to preserve organisational knowledge during the rollout of automation and AI initiatives. On top of this, CSPs should improve human-to-machine interactions to ensure there are clear feedback loops between employees and systems. CSPs must reskill and upskill network engineers and architects through regular skills assessments and ongoing training to maintain expertise and effectively use new technologies, tools, and techniques.

**Overcoming the unique risks of AI-driven innovation in mission-critical environments like the network.** CSPs must establish robust MLOps and AIOps to correlate data across domains and ensure automated feedback loops are in place for continuous model validation. Moreover, developing systematic reporting which compares network performance with broader business objectives will allow CSPs to identify pain points, as well as high-value and high-risk areas. This framework can guide investment decisions and inform CSPs of their intent-based strategies (i.e., key objectives and outcomes) for network processes, balancing feasibility (i.e., complexity in integration) with expected returns on investment (i.e., monetisation and cost control opportunity).



**Understanding the role of Gen AI in the network.** CSPs must take a cautious and measured approach to guide tactical quick wins, focusing on practical use cases with low deployment risk. To do this, CSPs must start with well understood applications for Gen AI (in combination with ML) that offer immediate benefits. One example is using ML and Gen AI to automatically analyse the data and generate insights through natural language-based interfaces. The auto-generation-based inference and assistive reasoning capabilities of AI/ML enable CSPs to develop more advanced solutions which better handle human-to-machine interactions (for example, develop human-to-machine interfaces such as bots which respond to network-related questions and follow instructions) and push for greater autonomy, moving from human-driven to system-led operations.

By putting in place these fundamental enablers, CSPs can accelerate their path to higher levels of network autonomy, aligning technological upgrades with broader business objectives and ensuring readiness for future challenges.

# PARTNERS



Research



Consulting



Events