Publication date:
July 2022
Author:
James Crawshaw

AIOps for Network Operations

Solving problems faster, more accurately, and at scale

Commissioned by:
mycomOSI

Brought to you by Informa Tech

Contents

Introduction

The growing sophistication and complexity of telecom networks is stretching the operational capabilities of communications service providers (CSPs) to their limits. To increase agility and automation, telecom networks are becoming more software centric and cloud based. Networks are changing from physical infrastructure to a mix of physical, virtualized, and containerized network functions. Technology environments are being redesigned in accordance with cloud-native principles and deployed across all cloud types (private, public, and hybrid). The demarcation of responsibilities between network and IT is increasingly blurred.

Historically, telecom networks were largely static, and the impact of network changes was easy to predict. With virtualization, the network has become highly dynamic. As network functions and IT systems become cloud native and disaggregated, the number of components that must be managed will increase significantly. Monolithic applications will be split into highly distributed and ephemeral microservices hosted across the private and public clouds. Failure to detect problems with any of these components and resolve them quickly could affect service quality, hence customer experience, hence revenue. Trying to manually troubleshoot problems in this new paradigm is not economically viable.

Migration to 5G will drive further complexity, especially as 5G core and capabilities such as network slicing are added. CSPs' current reactive approaches to managing networks will not suffice in the 5G era. They depend too heavily on human expertise and hence are time-consuming, error prone, and not scalable. The number of parameters that can be tracked in 5G networks has increased significantly from 4G. Today's service assurance systems follow prescriptive rules set by experienced engineers. But the complexity of 5G will require new rules that change dynamically as new patterns emerge.

In addition to increasing technological complexity, service portfolios have also evolved from being simple voice and data-centric products to become sophisticated digital services such as streaming video and gaming that carry strict performance requirements. And 5G will support additional services with SLAs that require real-time network changes and hence a high degree of network automation.

Telcos are in the early stages of this transition. To cope with these changes, CSPs must transform their operational practices from reactive to proactive. They must automate not just the identification of network issues but also their remediation. Artificial intelligence (AI) is a key technology that can help them make this transition.

The role of AI

The key role of AI is to automate the analysis of data at scale. AI solves specific problems, faster, more accurately, and at much higher scale than a human. As data sources and volumes increase, analyzing data manually becomes unfeasible. Using AI technologies such as machine learning (ML), models can be trained to recognize patterns in multiple large datasets (events, logs, traces, etc.). Leveraging this capability, AI-based solutions can perform

- **Anomaly detection:** ML-based applications can identify baselines in a data series and spot deviations from the normal pattern. These baselines are not static parameters but can be seasonal or periodic (e.g., diurnal).

- **Predictive analytics:** Given AI's strong pattern recognition capabilities, it can be used to predict the likelihood of events such as network failures based on time-series analysis.

- **Root-cause analysis (RCA):** ML can detect/identify interactions between different parameters to predict the root cause of a problem. Once a potential problem has been identified, ML can enable fault clustering of related problems with the same root cause to speed troubleshooting and prioritize resolution.

- **Next best actions:** ML models can be trained to identify the best remedial actions to take based on actions that were previously successful. These recommendations can either be activated through closed-loop automations or communicated to network and IT operations teams to implement (open loop).

Defining AIOps

AIOps is the abbreviation of artificial intelligence for IT operations, a term that refers to the application of AI (including machine learning and natural language processing) to traditional IT operations.

According to Dang et al.,[1] AIOps is about empowering engineers (developers, program managers, site reliability engineers, etc.) to build and operate services at scale by leveraging AI and ML techniques. AIOps can help organizations to improve

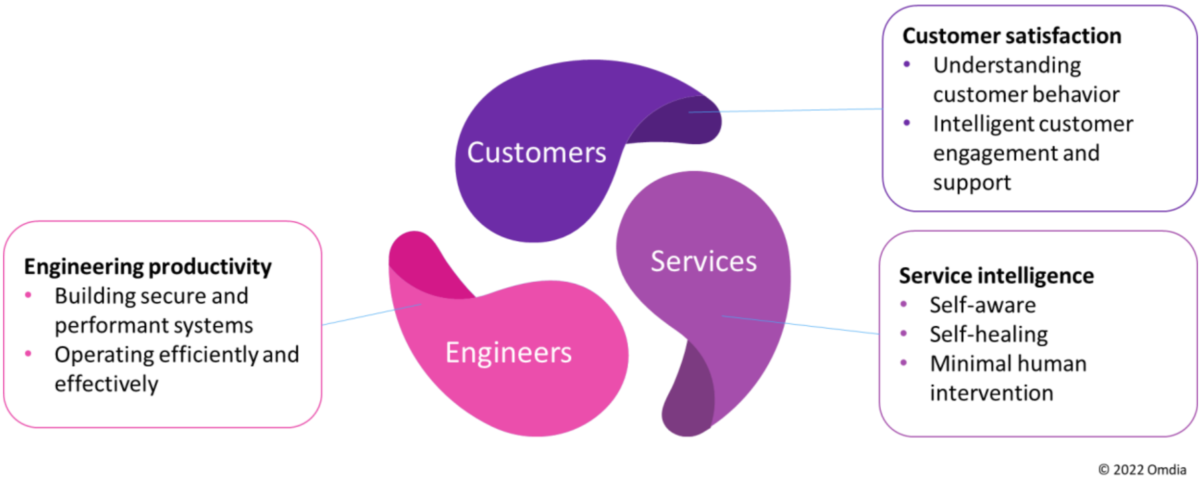
- **Service intelligence:** An AIOps-powered service will quickly identify quality degradation. It could predict its future state and trigger self-healing actions that need no human intervention.

[1] Yingnong Dang, Qingwei Lin, and Peng Huang, "AIOps: Real-World Challenges and Research Innovations," 2019 IEEE International Conference on Software Engineering, 2019, DOI: 10.1109/ICSE-Companion.2019.00023

- **Customer satisfaction:** Proactive actions can be taken to improve customer satisfaction. For example, a service may know that a customer is suffering from a quality issue and proactively engage with them to provide a solution instead of responding to customer complaints through human support.

- **Engineering productivity:** Engineers can be relieved of tedious tasks such as collecting information to investigate an issue or fixing recurring problems.

Figure 1: AIOps for service intelligence, customer satisfaction, and engineering productivity

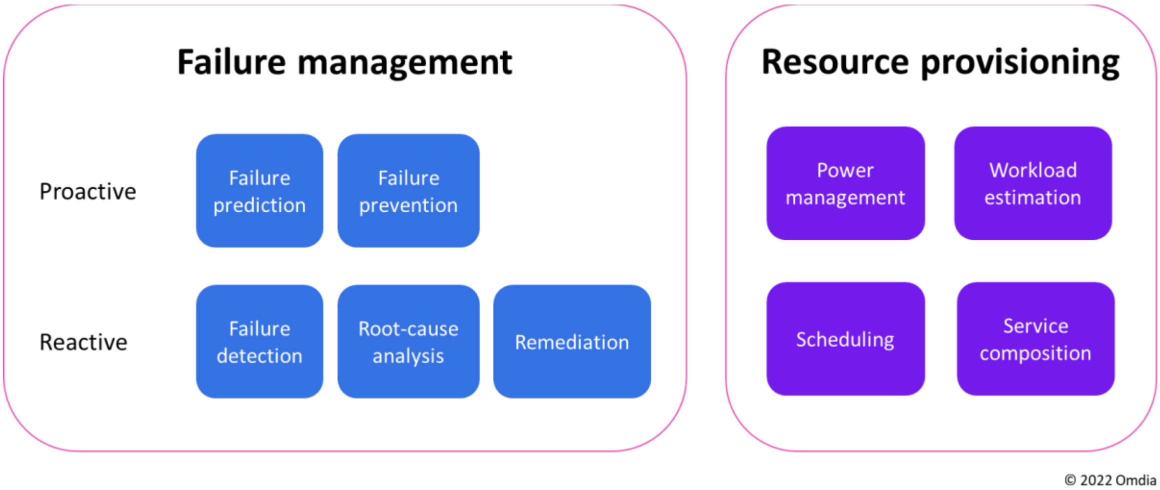


Source: Omdia

According to Notaro et al.,[2] the academic research into AIOps can be split into two main branches as shown below. Failure management is the study of techniques deployed to minimize the appearance and impact of failures. In large-scale systems failures are inevitable, so adequate protection mechanisms are needed to minimize their occurrence and satisfy service-level objectives. The other branch, resource provisioning, includes aspects such as workload estimation and power management.

[2] Paolo Notaro, Jorge Cardoso, and Michael Gerndt, “A Survey of AIOps Methods for Failure Management,” *ACM transactions on intelligent systems and technology*, 12 (6), 2021, DOI: 10.1145/3483424

Figure 2: Taxonomy of AIOps academic research



Source: Omdia

TM Forum[3] provides a more telecoms-centric definition of AIOps service management: "an evolution or a complement of existing frameworks (DevOps, Agile, ITIL ...), where we add and suggest specific principles and practices that need to be adopted and implemented for managing a blend of AI and traditional applications in complex operations environments." The TM Forum paper argues that the main differences between traditional and AI software are as follows:

- Training of AI algorithms and the retraining of AI models in production are new processes, which are not yet widely adopted in OSS software development and operations.
- The software lifecycle for traditional systems flows from development to operations, but in AIOps the flow is bidirectional because AI models can autonomously change their state and configuration while in production (e.g., through unsupervised learning).
- The introduction of AI models in operations makes the production environment more dynamic, which requires operations to overcome its fear of change.
- New data sources can enable the evolution of AI models, potentially bringing more optimized operations.
- AI models are mostly "black boxes." While code review can explain the logic behind traditional software, different techniques are needed to make AI-based software explainable.

AIOps platforms combine big data and AI technologies such as ML to analyze data across multiple data sources. Application, service, and network performance are monitored to find related triggers

[3] TM Forum, "AIOps: A practical framework for AI driven operations in the telecom industry," July 2020

that indicate an issue is likely to occur. Based on the correlation of these triggers (including metrics, time-series data, and events), root causes can be determined and resolved accordingly.

AIOps is becoming a necessity as telecom applications, and the infrastructure they run on, become more distributed and complex. By adopting AIOps, engineers can be more productive. The time they no longer spend on troubleshooting, RCA, and conducting routine maintenance can be redirected to more value-added activities.

The AIOps lifecycle

According to Lyu et al.,[4] the process for deriving interpretations from AIOps models can be considered as four phases: preprocessing, model training, model evaluation, and model evolution.

Preprocessing

AI algorithms learn from and make predictions about data. Preprocessing (sometimes referred to as feature engineering) is the collection of data and its transformation into features (attributes) that can be used as inputs to ML algorithms. The training dataset could comprise structured and/or unstructured data from a variety of sources, including monitoring tools and workflow platforms. Logs, KPIs, alerts, trouble tickets, and topology can be ingested and analyzed. A strong understanding of telecom networks is key in the preprocessing stage to identify which data and which features will create the most useful models.

The proper selection of data and its features can prevent two common issues with ML:

- **Overfitting:** The ML model cannot generalize well on new data because the model has learned irrelevant noise (random fluctuations) in the training data that do not help with inferencing production data.
- **Underfitting:** The model is too simple and neither models the training data well nor generalizes to new data.

Underfitting is easy to detect in the model training phase, while overfitting will only come to light in the model evolution phase.

Model training

Training is the key process to create AI models. An ML model uses linear algebra, mathematical optimization techniques, and statistics to find patterns in the input datasets. These patterns can be used to make predictions or decisions. Common types of ML include supervised learning, unsupervised learning, semisupervised learning, and reinforcement learning. Examples of ML algorithms include decision trees and support vector machines. The techniques used to train AI algorithms (loss functions, regularization, optimizers, etc.) are implemented in libraries such as PyTorch and TensorFlow. Services such as Amazon SageMaker, Azure Machine Learning, and Google Datalab provide ML development and training environments, MLOps tools, and the computing power to perform model training.

[4] Yingzhe Lyu et al., "Towards a Consistent Interpretation of AIOps Models," *ACM transactions on software engineering and methodology*, 31 (1), 2022, DOI: 10.1145/3488269

Model training consists of three steps:

- **Data sampling** for selecting a representative subset of a large dataset
- **ML learner fitting** to select the appropriate learner for the task; the learner is the program, which builds a decision tree from the input data
- **Hyperparameter tuning** to find the optimal parameters for the model

Some authors (e.g., Yang and Rossi) refer to this phase as design. The AI models that data scientists design will typically go through a phase of supervised training in which the model is presented with examples of events to recognize (classify) or the real-valued function to learn (regression).

The choice of the ML algorithm (or combination of algorithms) will vary depending on the choice of the ML training method. The three main categories are supervised learning, unsupervised learning, and reinforcement learning. In supervised learning, labeled input data is used to train and evaluate ML models. In unsupervised learning, the training data is unlabeled, and the system must spot patterns that enable it to classify the data into separate groups. In reinforcement learning, the system tries to maximize a notional reward for its analysis of the data.

Model evaluation

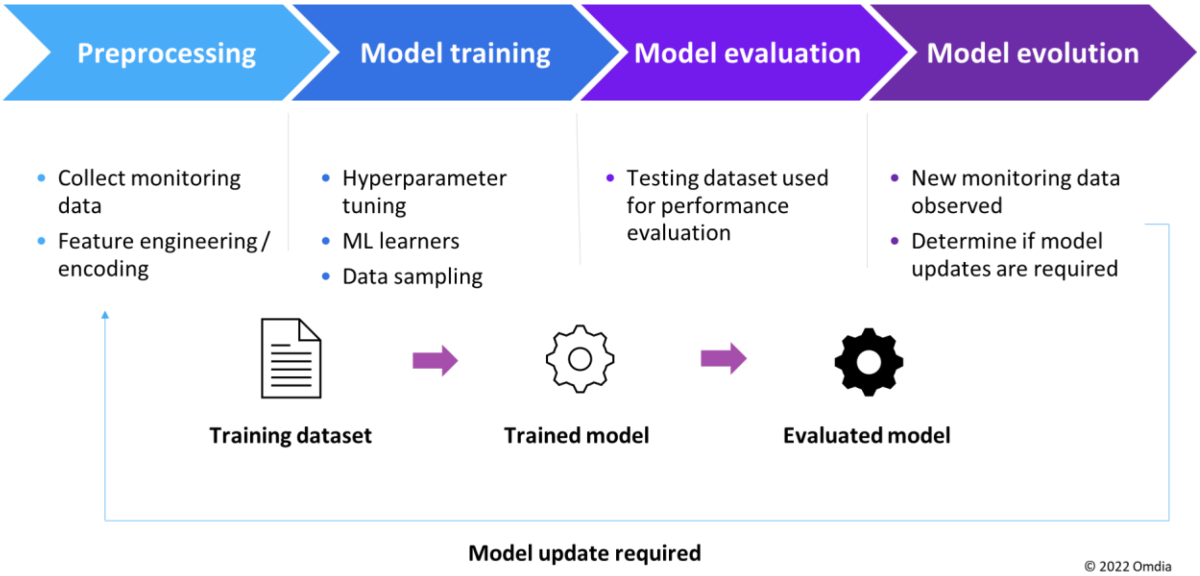
Once an AI model has been trained and deployed, real production data is used to generate predictions or classifications. A well-trained AI model should be able to correctly process data it has never seen before. Model evaluation looks at the performance (accuracy, sensitivity, and specificity) of the trained models using the testing dataset. Several methods (hold-out, cross validation, bootstrapping, etc.) can be used.

Model evolution

Model evolution refers to the practice of deploying and regularly updating models. If the behavior of the system that is being modeled changes over time, the deployed model may need to be retrained with fresh data. Performance is monitored to understand if models are still fit for the environment where they have been deployed, or if they have become “stale” and need retraining. When the statistical properties of the target variable, which the model is trying to predict, change over time in unforeseen ways the model is said to exhibit “concept drift.”

As **Figure 3** indicates, the AIOps model lifecycle is iterative with models being measured and improved to ensure their performance remains satisfactory.

Figure 3: AIOps model lifecycle



Source: Omdia

Business benefits of AIOps

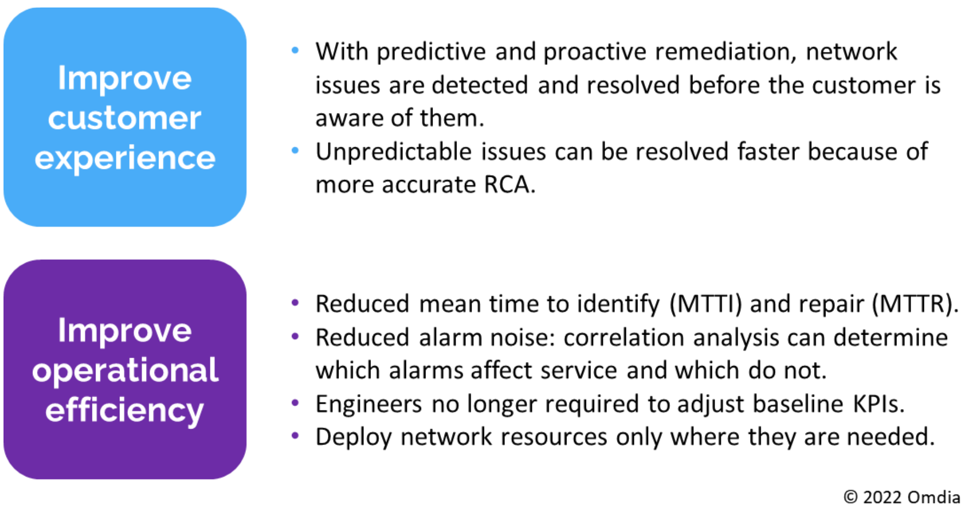
According to Notaro et al., compared with traditional approaches, AIOps is

- **Faster:** It can react autonomously to problems in real time without needing manual debugging and time-consuming analysis.
- **More efficient:** By forecasting workload requirements and modeling request patterns, AIOps can improve resource utilization, identify performance bottlenecks, and reduce wastage.
- **More effective:** It can offer actionable insights for RCA, failure prevention, fault localization, recovery, and other O&M activities.

As **Figure 4** indicates, AIOps can help improve customer experience and operational efficiency. With predictive maintenance and proactive remediation, network problems can be identified and resolved before they affect the customer. Through more accurate RCA, AIOps can reduce the mean time to identify and repair network problems. This improves the customer experience and increases productivity by freeing engineers from repetitive tasks.

Note, as well as improving network performance, AIOps can also be applied to network security to help protect against cyberattacks such as distributed denial of service (DDoS). With its anomaly detection capabilities, early signs of an attack can be detected, the root cause determined, and action taken to isolate affected nodes.

Figure 4: Benefits of AIOps



Source: Omdia

AIOps challenges

According to Yang and Rossi,[5] there are two main challenges in applying AI to the networking domain:

- **Lack of standard data representations:** Data in the network field is significantly more heterogeneous and diverse than in other fields such as image recognition.

- **Pace of technology evolution:** While training a deep learning model to recognize cats requires a significant volume of labeled images, cats do not change much over time. This is in stark contrast to the pace of evolution in network technology.

These factors are compounded by privacy / commercial sensitivity concerns that have so far made it impossible to construct and share large corpuses of telecom network data with academia, an issue that has constrained research efforts.

Omdia believes that AIOps will play an important role in transforming CSP operations. There are, however, challenges to its implementation. Building AIOps solutions requires an understanding about the whole problem space, from business value and constraints, data, and models to system and process integration considerations. It can be hard to coordinate staff in different disciplines (e.g., business stakeholders, engineers, data scientists) to build AIOps solutions collaboratively.

The TM Forum's AIOps Service Management Framework defines the various processes in the lifecycle of AI software including the management of configuration, change, acceptance testing, releases, knowledge, monitoring, incidents, and problems. According to TM Forum, AIOps is outside of the normal operational practices of service providers and will require different teams across the organization to work together to achieve common goals. For example, the traditionally siloed deployment and production teams must merge to be able to manage the dynamic nature of AI-based software.

Changing organizational culture and structure is a crucial challenge. Current processes, tools, and operational practices are siloed and focused on human effort to execute most functions. This needs to change to release the full potential of AIOps. Cross-functional teams within operations need to collaborate, particularly with respect to sharing siloed data. Education is also important to emphasize the benefit that AIOps will bring in terms of increased productivity and the quality of services delivered to customers. Having C-level executives and departmental heads champion AIOps-related projects will be key to its success in telco operations.

[5] Lixuan Yang and Dario Rossi, "Quality Monitoring and Assessment of Deployed Deep Learning Models for Network AIOps," IEEE Network, 2021, DOI: 10.1109/MNET.001.2100227

According to Li et al.,[6] the successful adoption of AIOps solutions requires that they be trustable, interpretable, maintainable, and scalable:

- **Trustable:** AIOps solutions must incorporate field-tested, engineer-trusted domain expertise into their ML models.
- **Interpretable:** AIOps solutions should be interpretable so that engineers can understand their recommendations. One of the barriers to the adoption of AI models is that they often appear as black boxes with no indication of how they make decisions, predictions, or classifications. Explainability is a key dimension that should be considered in AIOps.
- **Maintainable:** AIOps solutions should require minimal maintenance and fine-tuning because the operations teams that use them will not be ML experts.
- **Scalable:** AIOps solutions need to scale in line with the network and traffic they support.

[6] Yangguang Li et al., "Predicting Node Failures in an Ultra-Large-Scale Cloud Computing Platform: An AIOps Solution," *ACM transactions on software engineering and methodology*, 29 (2), 2020, DOI: 10.1145/3385187

Conclusions

To increase operational efficiency and agility, CSPs must embrace automation. A completely zero-touch network operations center is still a pipe dream for most CSPs. However, the application of AI to network operations can still bring meaningful benefits.

AI solves specific problems, faster, more accurately, and at higher scale than humans. AI-based solutions can perform anomaly detection and make predictions. AIOps is the application of AI to IT and network operations. AIOps platforms combine big data and AI technologies such as ML to analyze data across multiple data sources.

AIOps can improve customer experience and operational efficiency. It can enable CSPs to transition from reactive to proactive ways of operating and managing the network. With predictive maintenance, network problems can be identified and resolved before they affect the customer. And if problems cannot be predicted, they can still be resolved more quickly using AIOps through more accurate RCA and autoremediation. This improves the customer experience and increases engineer productivity.

Omdia believes that AIOps will play an important role in transforming CSP operations as telecom applications, and the infrastructure they run on, become more distributed and complex. There are, however, challenges to its implementation. For example, cross-functional teams within operations will need to collaborate more, particularly with respect to sharing siloed data.

AIOps is typically used today to guide operations teams to make better decisions based on what worked well in the past. But as operations teams gain confidence in AIOps, they will allow these systems to operate autonomously, avoiding manual checks. This confidence depends on AIOps solutions being trustable, and this in turn requires that they embed telecom network domain expertise into the algorithms and features of the AI models.

Appendix

Methodology

This paper is based on Omdia's ongoing research into telecom service assurance and the broader topic of service provider transformation leveraging new technologies such as AI.

Author

James Crawshaw
Practice Leader, Service Provider Transformation
customersuccess@omdia.com

Get in touch

www.omdia.com
customersuccess@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer