ADN Analysis-TMF

Why Autonomous Network

Telecom networks are becoming more and more complex. Network O&M in this case is dominated by manual operations, which therefore results in error prone, time consuming and high costs operations. One survey by Huawei technical support team found that manual intervention is required for 95% of the process and job nodes.

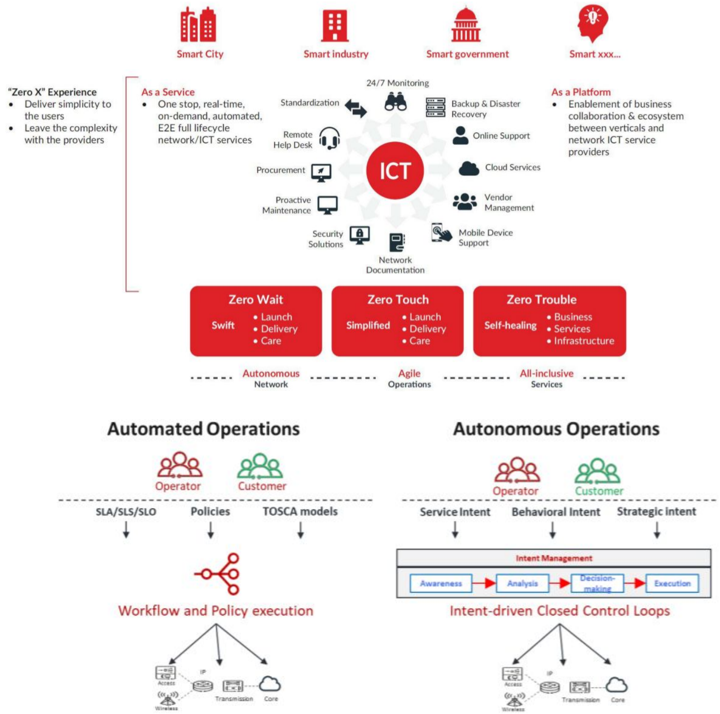
As the number of connections increases, the bandwidth grows rapidly, and the construction of telecom infrastructure accelerates. This in turn poses stringent requirements on balancing asset utilization and improving energy efficiency to obtain the optimal TCO.

Although the business scale and data availability in the telecom industry are extensive, its business monetization capability is poor. The industry lacks differentiated products and customer service capabilities. It also struggles to implement network SLA assurance. Service freezing, intermittent disconnection, and poor quality caused by network congestion frequently occur, and user complaints cannot be handled promptly or accurately.

The convergence and innovation of new services is slow. For example, the telecom industry takes more than 12 months on average to roll out a new service.

Facing these challenges, the telecom industry needs to leverage intelligent technologies to promote the evolution of network architecture and O&M. It also needs to move towards the autonomous driving network (ADN) era of man-machine collaboration, and continuously drive the intelligent upgrade in the industry.

Autonomous Networks

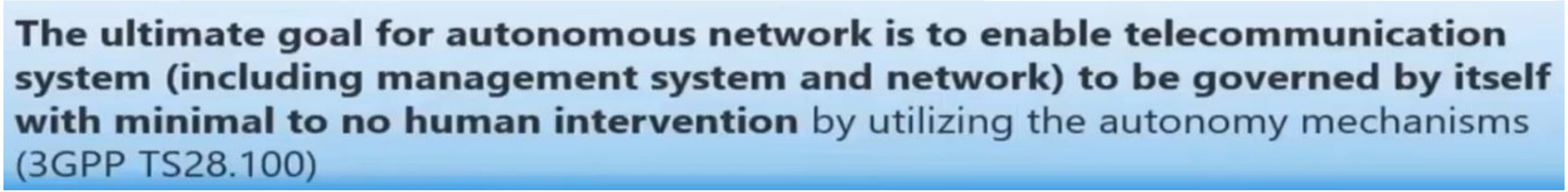


What is autonomous networks

Autonomous networks aim to provide

- Fully automated zero wait, zero touch, zero trouble innovative network/ICT services for vertical industries users and consumers.
- Support self-configuration, self-healing, self-optimizing and self-evolving telecom network infrastructures for telecom internal users: planner, service/marketing, operations and management.

The Autonomous Networks comprises simplified network architecture/autonomous domains and automated intelligent business/network operations for the closed-loop of digital business, which offer the best-possible user experience, full lifecycle operations automation/autonomy and maximum resource utilization.



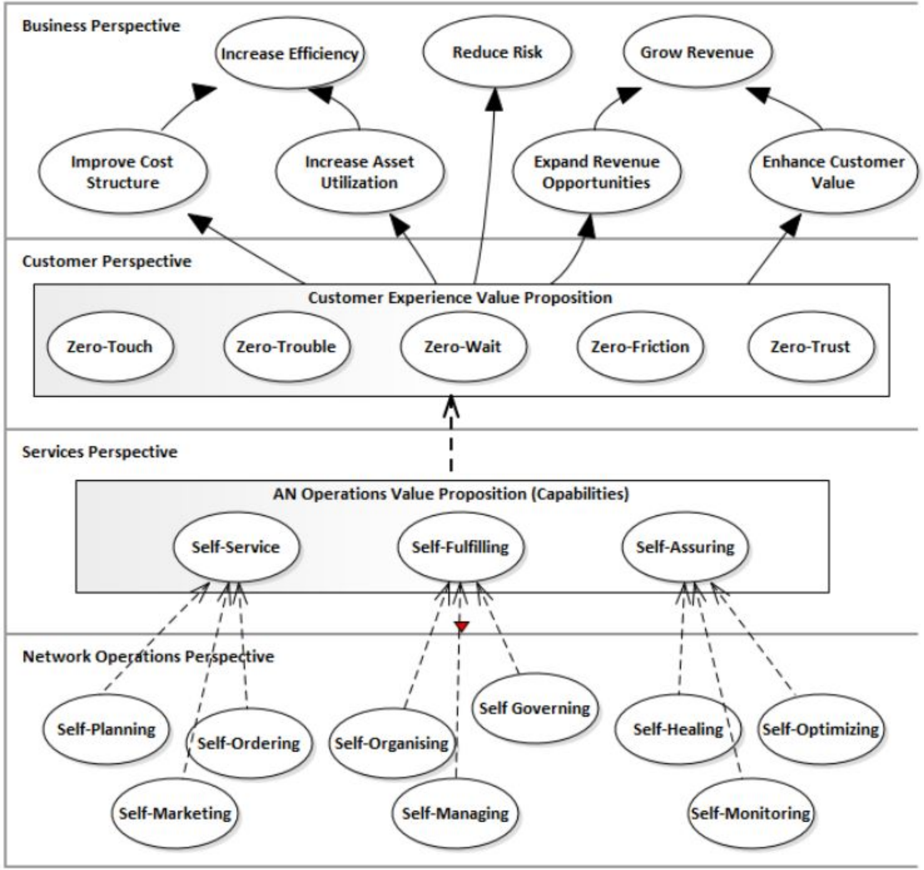
The ultimate goal for autonomous network is to enable telecommunication system (including management system and network) to be governed by itself with minimal to no human intervention by utilizing the autonomy mechanisms (3GPP TS28.100)

IG1193_Cross_Industry_Autonomous_Networks_Vision_and_Roadmap_V1.0.1.pdf

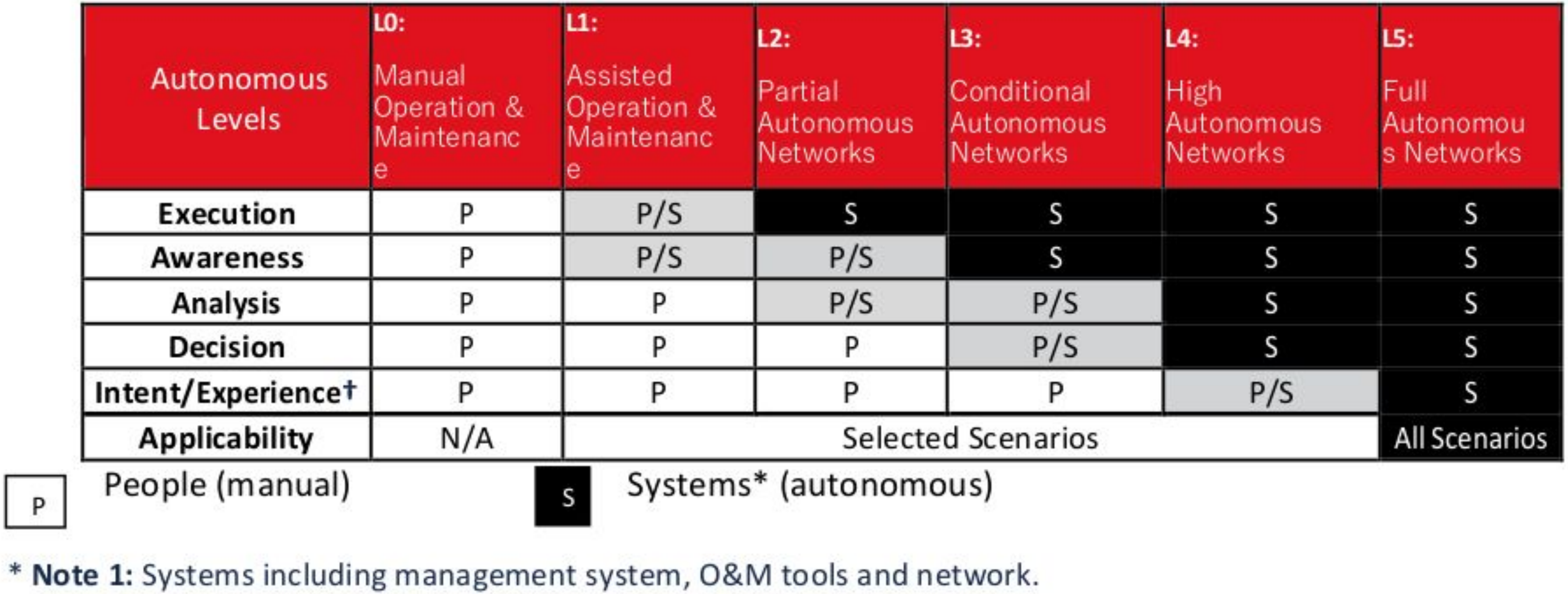
Why Autonomous Network

The autonomous networks addresses following challenges

- Processes are becoming more complex and associated data sets are growing exponentially
- It takes too long to develop the logic needed to support software and process
- Manual processes struggle to adapt to change or align to reduced lifecycle of services
- Manual interactions are many time error prone.



Levels of Autonomous Networks



Autonomous Levels	L0: Manual Operation & Maintenance	L1: Assisted Operation & Maintenance	L2: Partial Autonomous Networks	L3: Conditional Autonomous Networks	L4: High Autonomous Networks	L5: Full Autonomous Networks
Execution	P	P/S	S	S	S	S
Awareness	P	P/S	P/S	S	S	S
Analysis	P	P	P/S	P/S	S	S
Decision	P	P	P	P/S	S	S
Intent/Experience†	P	P	P	P	P/S	S
Applicability	N/A	Selected Scenarios				All Scenarios

P People (manual)

S Systems* (autonomous)

* **Note 1:** Systems including management system, O&M tools and network.

IG1193_Cross_Industry_Autonomous_Networks_Vision_and_Roadmap_V1.0.1.pdf

Autonomous Networks Framework

3-layers: Represent a group of common capabilities and business logics that can be utilized to support all scenarios, as well as business relationships between the groups of atomic capabilities.

Business operations layer: Including customer lifecycle management processes and product/offering lifecycle management processes.

Network operations layer/Service Layer: Including the flows of resource-facing services planning, deployment, maintenance, optimization and inventory management. Also, includes the flows of customer-facing services planning, deployment, service providing, maintenance, and optimization.

Network resources layer: Including the processes of resource/network planning, deployment, maintenance ,optimization and inventory management.

4-closed-loops: represent the execution/fulfilment of the full lifecycle of the operations that can use the select capabilities of above layers upon corresponding business process.

- Network resource closed loop
- Network operations closed loop
- Business operations closed loop
- Cross layer user service closed loop

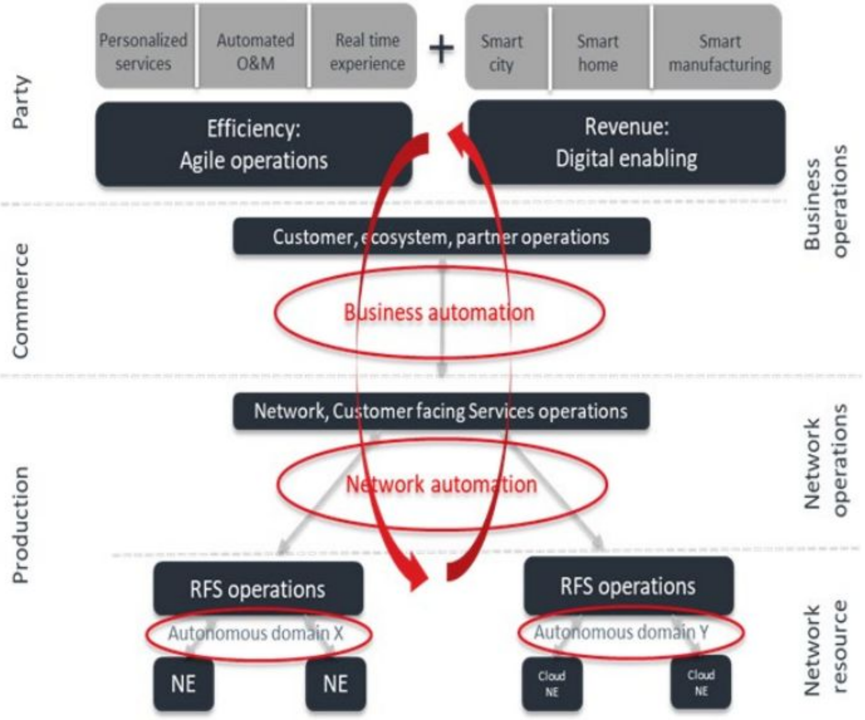


Figure 2. Overarching framework: 3-layer + 4-closed-loop

IG1193_Cross_Industry_Autonomous_Networks_Vision_and_Roadmap_V1.0.1.pdf

Key requirements of AN capabilities: Simplified infrastructure

The simplified infrastructure fundamentally guarantees an intelligent and hierarchically Autonomous Networks. The simplified network architecture, protocols, devices, sites, and deployment solutions offset complexity caused by ultra-high bandwidth and vast connections, improving efficiency and customer experience throughout the network lifecycle.

Simplified network protocols facilitate network configuration and maintenance. Services are decoupled from the physical network, adapting to different service scenarios on one network and allocating network resources on demand.

IG1218_Autonomous_Networks_Business_and_Framework_v2.0.0.pdf

Key requirements of AN capabilities: Autonomous domains

An Autonomous Domain is an operational management domain that defines the scope of encapsulated autonomous behavior. It is the ‘building block’ (i.e., unit) of autonomous behavior that when federated together form a complete Autonomous Network. It serves as the basic unit that can fulfill closed-loop automation of specific network operations.

The examples of autonomous domain instances can be the closed loops of access, metro backbone, core, edge, customer network from infrastructure perspective, or SD-WAN, VoLTE, CDN etc. from service perspective.

L	Indicates interactions reference points between operation Layers. Expressions use Intent.	L1, L2, L3
F	Indicates interactions reference points between Domains . Expressions use Intent.	F1, F2, F3
K	Connect the operational layers to a Knowledge and Intelligence platform	K1, K2, K3

IG1251_Autonomous_Networks_Reference_Architecture_v1.0.0

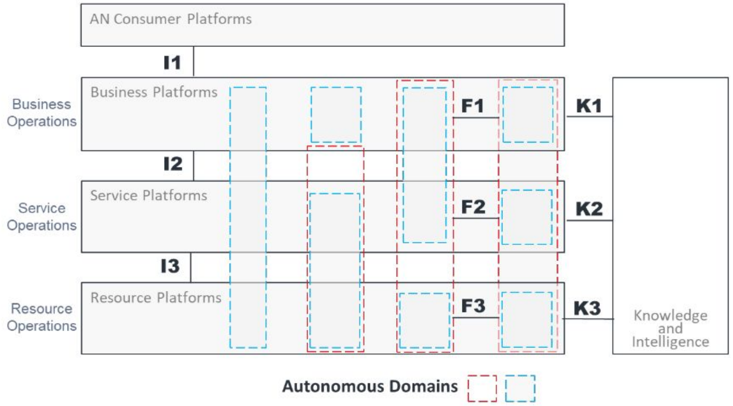
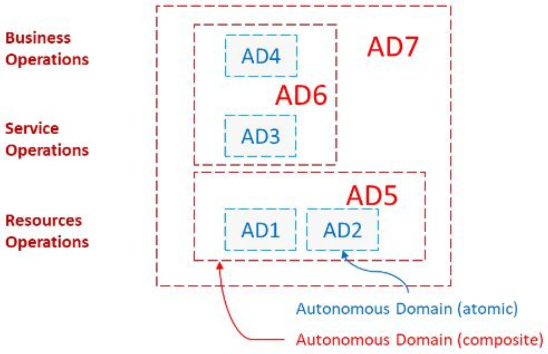


Figure 4-2 Autonomous Domains Building Blocks within the Reference Architecture



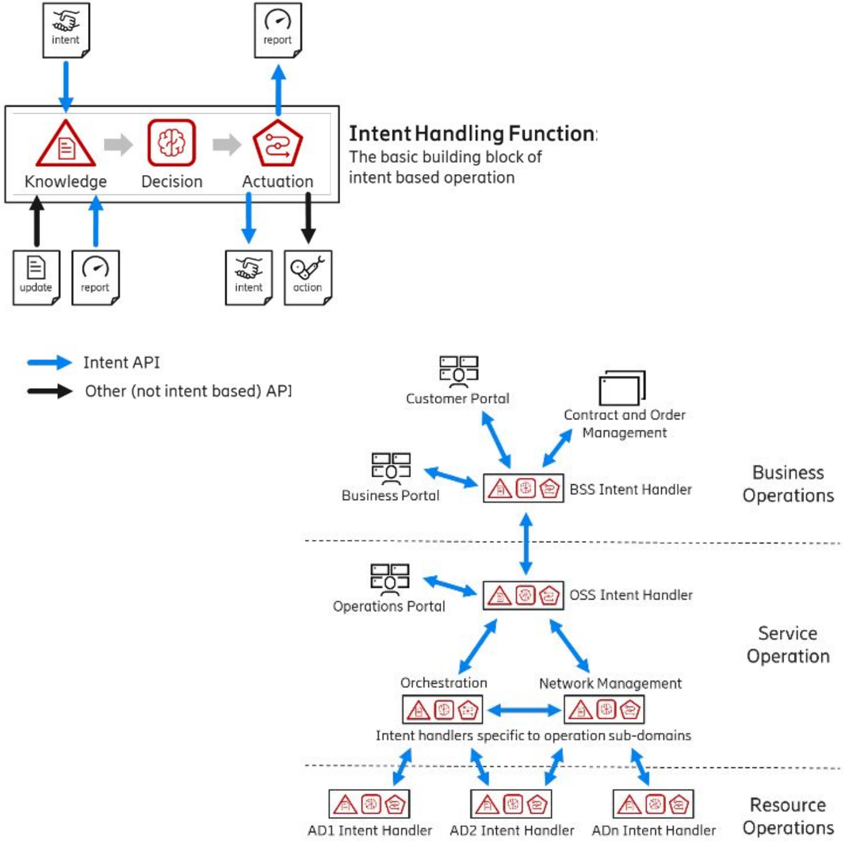
Key requirements of AN capabilities: Intent driven interaction

Intent defines what Autonomous Networks are expected to achieve, but it leaves the details of how a network is designed and operated to the internal operations of the network platform. This means that the smart software in the platform can constantly optimize how the service is delivered and we can incrementally add new technologies like Analytics and Machine Learning to constantly improve the implementation.

Business intent represents the objectives of a business user. Operators expect their Autonomous Networks to operate service contracts while meeting revenue targets. Their customers expect a good user experience.

Service intent represents the objectives of a service user. A service is expected to deliver functional as well as non-functional attributes. This includes targets for example on connectivity, bandwidth, latency or availability.

Resource intent represents the objectives of resource users. Resources are expected to be allocated so that performance and quality of service targets are met.



IG1230_Autonomous_Networks_Technical_Architecture_v1.1.0.pdf

Properties of intent

Declarative goals and utility: the wanted state: an intent object is a collection of distinct expectations. They express a variety of requirements, goals and constraints. An individual intent may contain a variety of different expectations(functional and non-functional aspects of the service). Intent is solely declarative in the sense that it only specifies wanted outcomes versus outcomes that need to be avoided. This can include quantitative specifications. For example, a goal can be set by defining target values or value ranges using KPI and metrics.

Composible and additive: Intent are knowledge objects that define a set of these requirements. Setting an intent therefore means to add to the pool of requirements. Deleting an intent means to remove requirements from the pool. Intent and the additional requirements expressed by it can originate from many sources, they might overlap or even contradict. Autonomous system operating based on intent would need to be able to prioritize based on utility. It might also not be able to fulfill all its requirements at once in all situations.

Persistent and lifecycle managed: Intent objects have a lifecycle that is actively managed. The intent interface defines the procedures for executing this lifecycle management.(IG1253C)

Infrastructure agnostic and portable: Intent will need to cross the borders of major sub-systems and platforms, where often solutions from different system vendors are used and required to interact flawlessly. This need is addressed by defining a common interface for intent lifecycle management as well as a common modeling approach of intent objects.(IG1253A & IG1253B future)

Measurable and grounded in data : As intent can change dynamically, the receiving system might need to adapt and measure whatever the intent is expressing. Intent can only be handled successfully if the receiving system has the means to observe whatever the intent is stating.

IG1253_Intent_in_Autonomous_Networks_v1.1.0.pdf

Intent Life cycle

Intent Owner: The intent owner is the origin of intent. If has created the intent object and it is responsible to manage its lifecycle. This includes changing the intent content if needed and finally removing the intent object.

Intent Handler: The intent handler receives an intent object and operates the domain it is responsible for accordingly. Intent handlers do not modify intent, but they can reject it. However, once accepted they are obliged to fulfill the requirements and goals as well as possible based on the resources and solutions it has available. Intent handlers report back to the intent owners about the handling status and success.

- **Detection**: In the detection phase the intent owner identifies if there is a need to define new or change/remove existing intent to set requirements, goals, constraints.
- **Investigation**: In the investigation phase the intent owner finds out what intents are feasible. This has two aspects: first, it needs to find suitable intent handlers that have the right domain responsibilities. 2nd, finding out if the wanted intent is realistic.
- **Definition**: In the definition phase the intent owner formulates the intent it needs to use, and it creates the respective intent objects.
- **Distribution**: Intent owner contacts an intent handler in order to send a new intent or modify or change an existing one.
- **Operation**: Executing and reporting back of Intent by Intent handler.

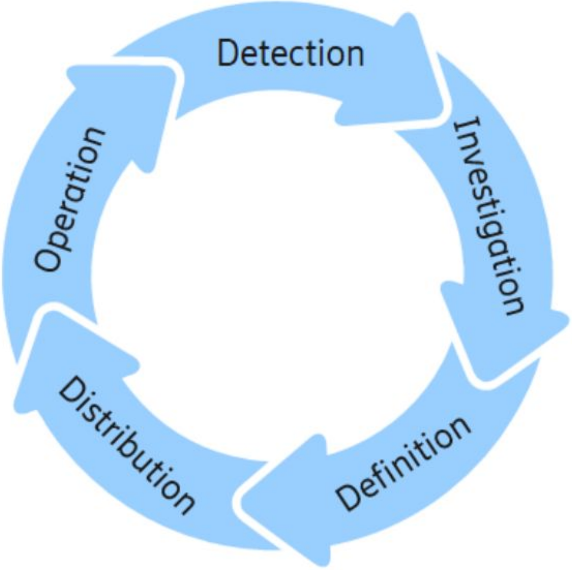


Figure 8.1: Intent lifecycle phases

IG1230_Autonomous_Networks_Technical_Architecture_v1.1.0.pdf

Key requirements of AN capabilities: Closed loops

4-closed loops: to fulfill the full lifecycle of the inter-layer interaction

User closed loop: the interaction across above three layers and three closed loops to support the user service fulfillment. The interactions across the different layers should be based on simple, intent based API interfaces.

Business closed loop: the interaction between business and service operations. The operations need to be upgraded from isolated business to on demand, automated business collaboration and ecosystem, which enables the closed loop for customer/business/ ecosystem operations, normally requiring collaboration across multiple service providers globally.

Service closed loop: the interaction between service and network resource operations. The operations need to be upgraded from legacy customized project-centric approach to a data/knowledge driven platform based on full lifecycle operations automation.

Resource closed loop: the interaction of network resource operations in the granularity of autonomous domains.

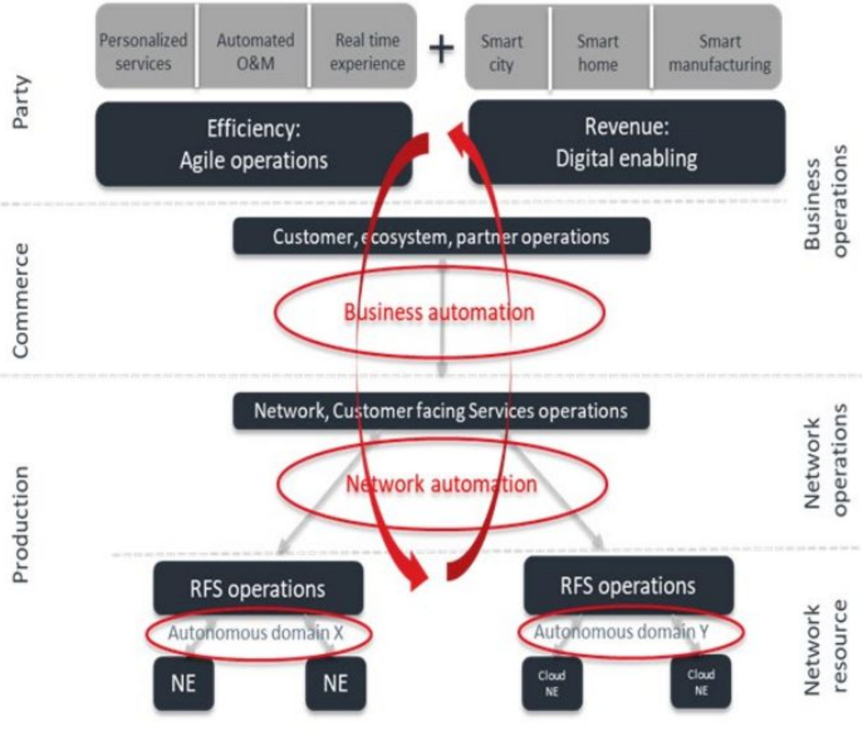


Figure 2. Overarching framework: 3-layer + 4-closed-loop

IG1218_Autonomous_Networks_Business_and_Framework_v2.0.0.pdf

AI in Autonomous Networks

In the Autonomous Networks, AI can be used anywhere as needed. Similar as a human brain in terms of perception, training, inference, decision-making and execution processes, AI capabilities need to be provided at different layers of Autonomous Networks. This will support AI-based automated closed-loop network operations, implement intelligent automation in different service scenarios for meeting autonomous levels of Autonomous Networks.

four key telecom AI use case categories :

1. Perception and Prediction

2. Detection and identification

3. Control optimization

4. Process optimization

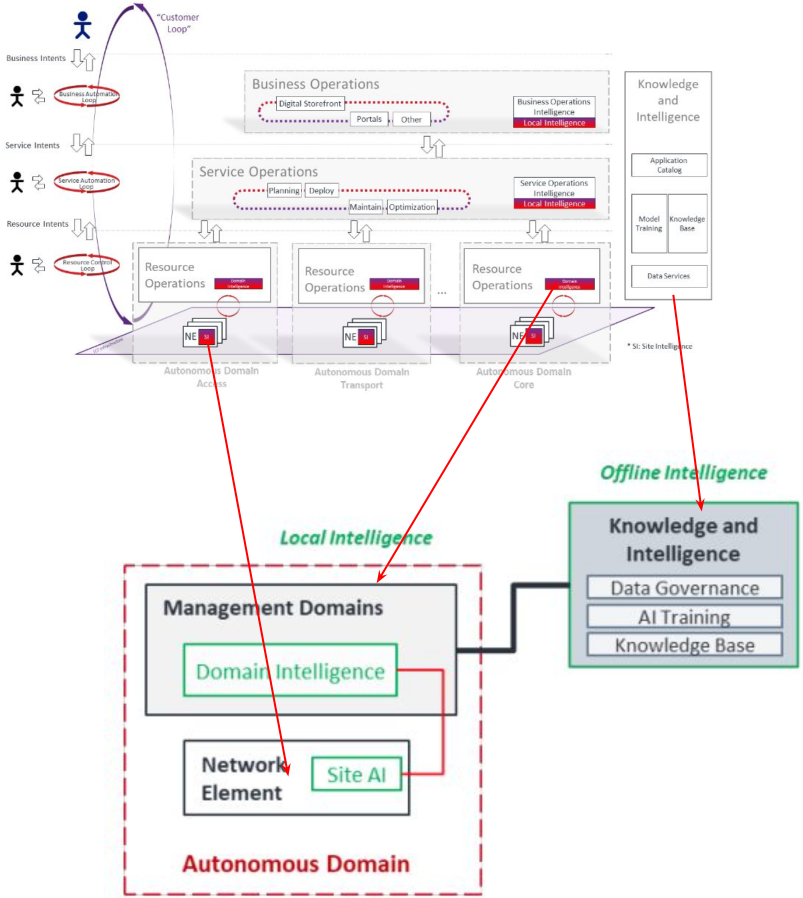
IG1218_Autonomous_Networks_Business_and_Framework_v2.0.0.pdf

AI in ADN

AI/ML will become ubiquitous as a core component of network operations and maintenance intelligence. TMF defines 3 layer intelligence framework in ADN framework.

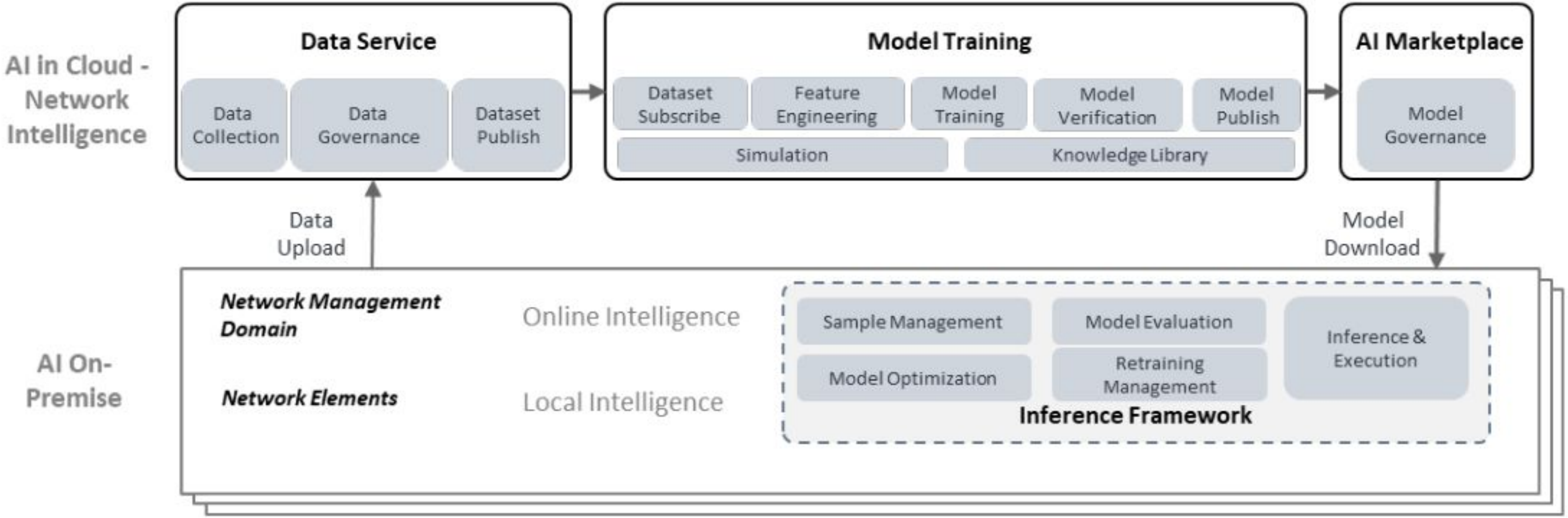
The Knowledge and Intelligence platform is a centralized design and development platform and is the source for the digitization of operations, network and human expert knowledge.

The localized Intelligence includes **management domain Intelligence and network element intelligence**. Management domain Intelligence provides an online AI inference service for the hierarchical autonomous network, focusing on real-time collection and filtering of network data. It mainly focuses on local real-time perception analysis and decision processing due to lack of storage and computing.



TMF defines 3 Layer Intelligence Framework

Close loop model of AI Development and Deployment



3 Layer Intelligence Framework Works in Close loop to active continuous development and deployment of AI applications

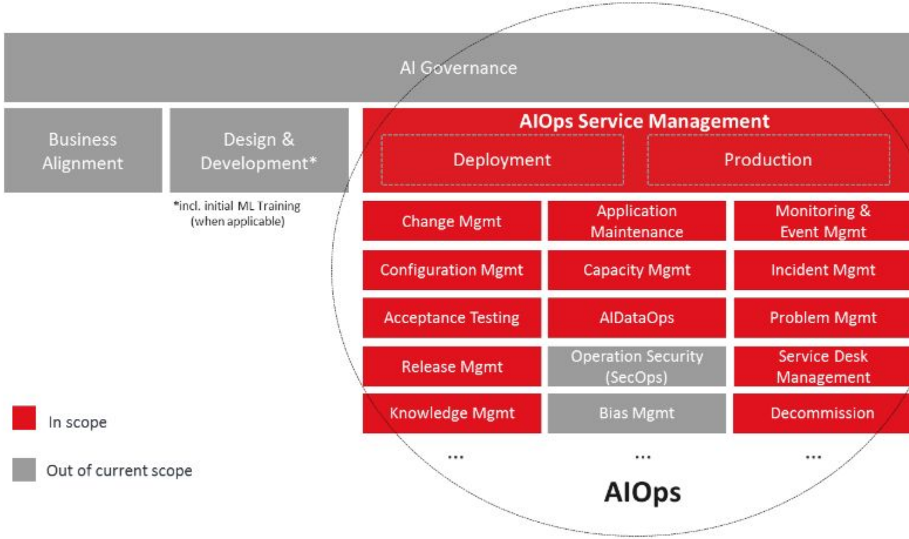
AIOps Service Management

AI Ops means how to operationalize AI, i.e., how to deploy, operate, control, maintain and govern hundreds or thousands of AI components which will eventually form part of core IT and network systems architecture.

AI operations need to be compliant with emerging regulatory frameworks for AI aiming to enable a trustworthy, responsible, reliable and secure development and adoption of AI applications and services.

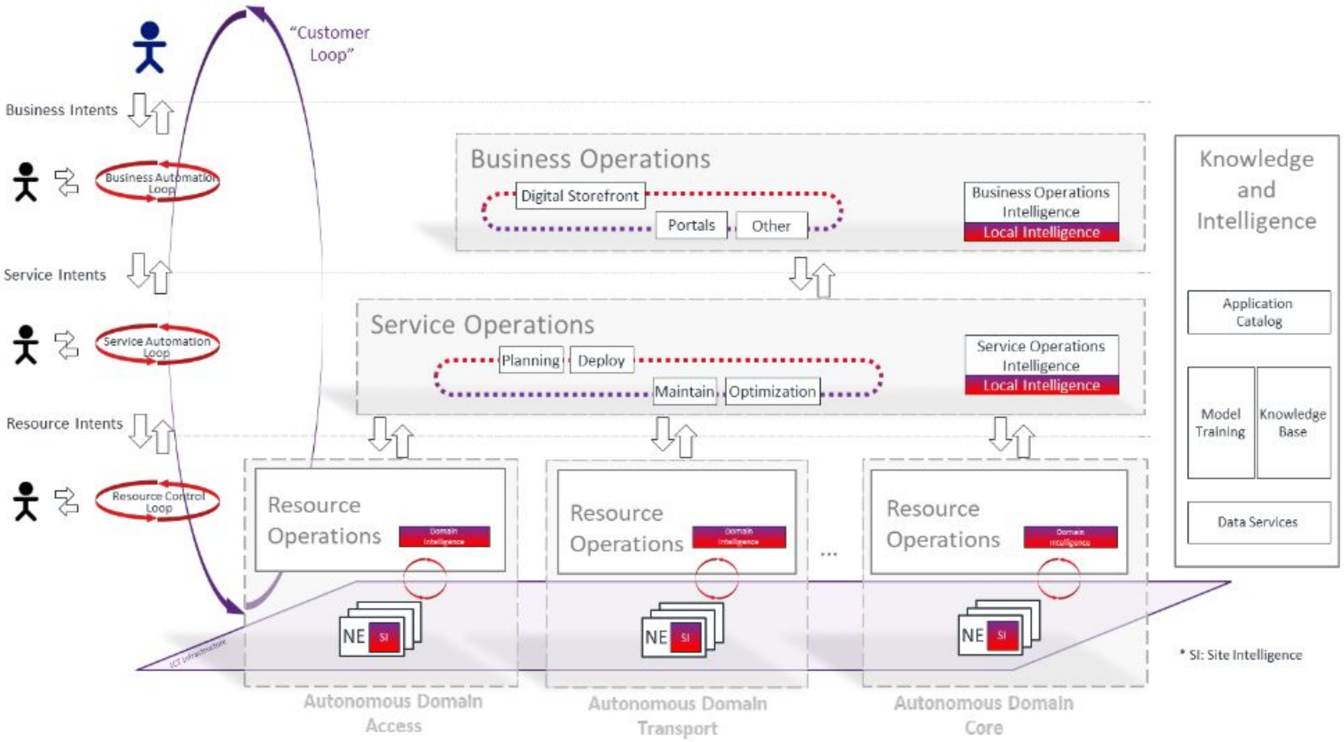
TM Forum is leading an initiative to formulate an industry-agreed framework called “AIOps Service Management Framework”, which focuses on reengineering the software and service lifecycle processes required to operationalize AI software at scale.

This framework enables operations teams, process owners and business users to exploit AI safely and properly, thereby maximizing its benefits, mitigating its inherent risks, and ensuring the appropriate level of quality, reliability, transparency, and regulatory compliance.



IG1230_Autonomous_Networks_Technical_Architecture_v1.1.0.pdf.pdf

Technical Architecture



IG1230_Autonomous_Networks_Technical_Architecture_v1.1.0.pdf.pdf

Knowledge and Intelligence	Provide Intelligence services for all three operational layers. Includes (AI/ML) model training, data services, knowledge base, and AI/Analytics application marketplace. Works with Localized Intelligence where local data and training services are provided by the layered platforms.
Application Catalog	Application Catalog manages the published AI applications/AI models in a secure catalog. The App Catalogs contain detailed information on ownership and execution requirements of individual models to simplified model selection.
Model Training	This service provides an integrated development environment for a one-stop training design environment, model development services, Domain model service, federated learning, and knowledge graph. The Training Platform delivers models to the localized intelligence in the operational platforms and (optionally) receives offline data to tune its training algorithms (using K1, K2, K3 ref points as appropriate depending on the operational layer in question).
Knowledge Base	A repository system that represents knowledge explicitly. The KB can also use tools enabling tacit knowledge exploitation also – e.g., a reasoning system that allows it to derive new knowledge and facts used to perform decision-making and reasoning within K&I.
Site Intelligence	Next Page

AI in Autonomous Networks

In the Autonomous Networks, AI can be used anywhere as needed.

AI capabilities need to be provided at different layers of Autonomous Networks. This will support AI-based automated closed-loop network operations, implement intelligent automation in different service scenarios for meeting autonomous levels of Autonomous Networks.

Four key telecom AI use case categories :

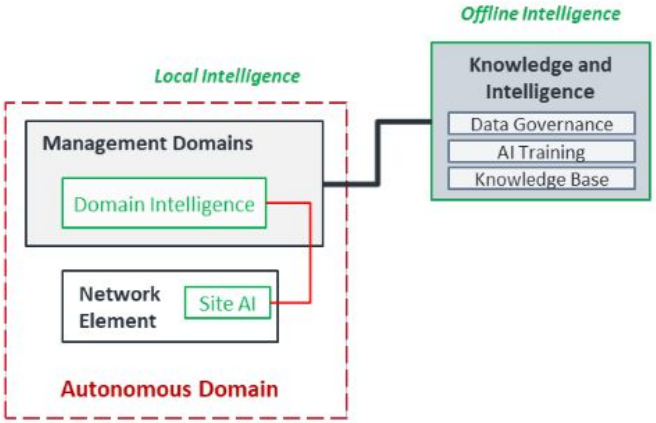
1. Prediction
2. Detection and identification
3. Control optimization
4. Process optimization

Three Layered Intelligence

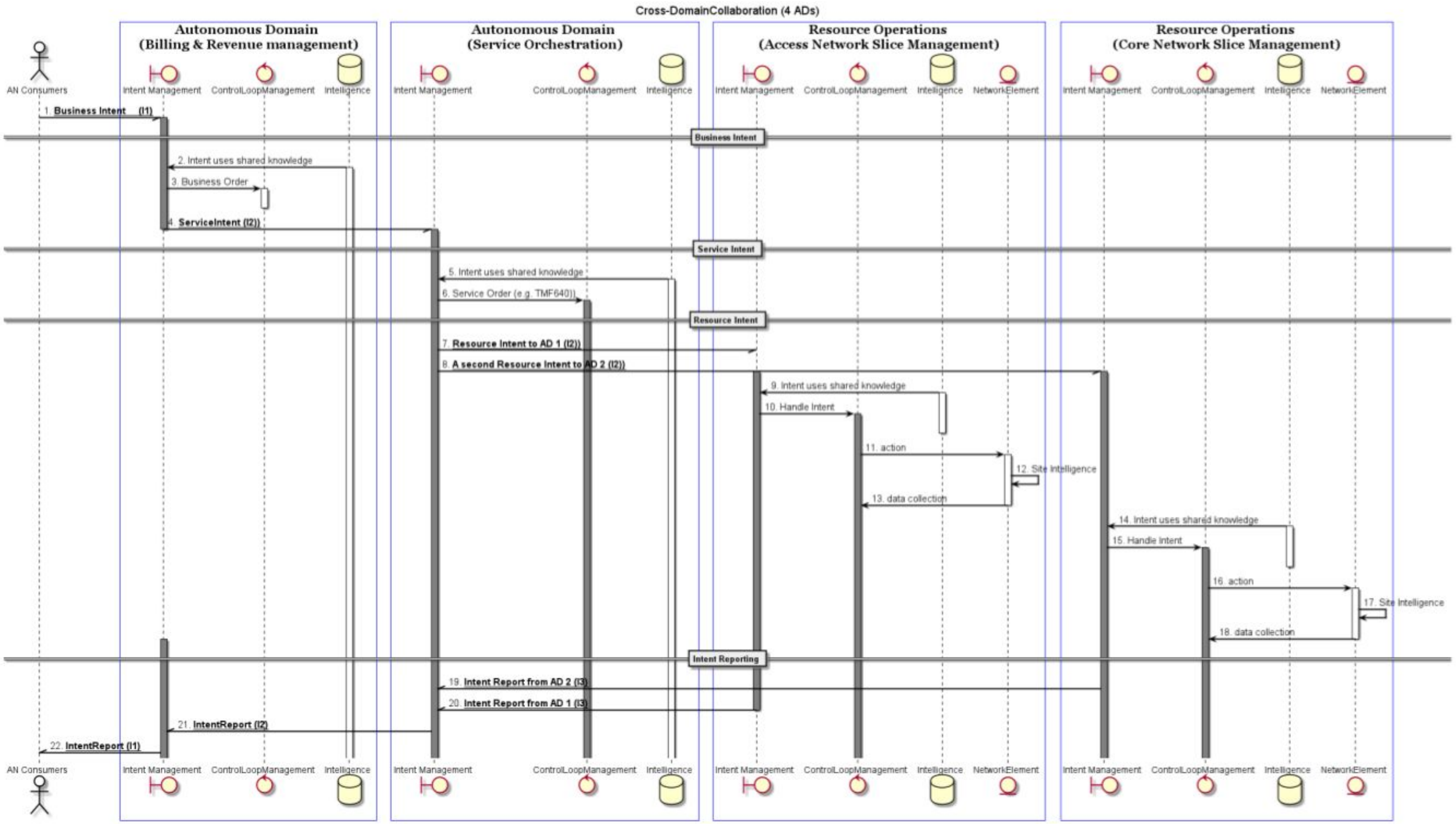
“Cloud + AI”– an open Knowledge and Intelligence platform, accelerate network AI innovation and development.

“Management layer + AI” − involving AI Inference framework, promote intelligent analysis and decision capability in the management layer.

“NE + AI” − Make the network real-time perceptible with built-in AI chips and sensors, enabling data collection acceleration and rapid inference at the edge.



IG1218_Autonomous_Networks_Business_and_Framework_v2.0.0.pdf

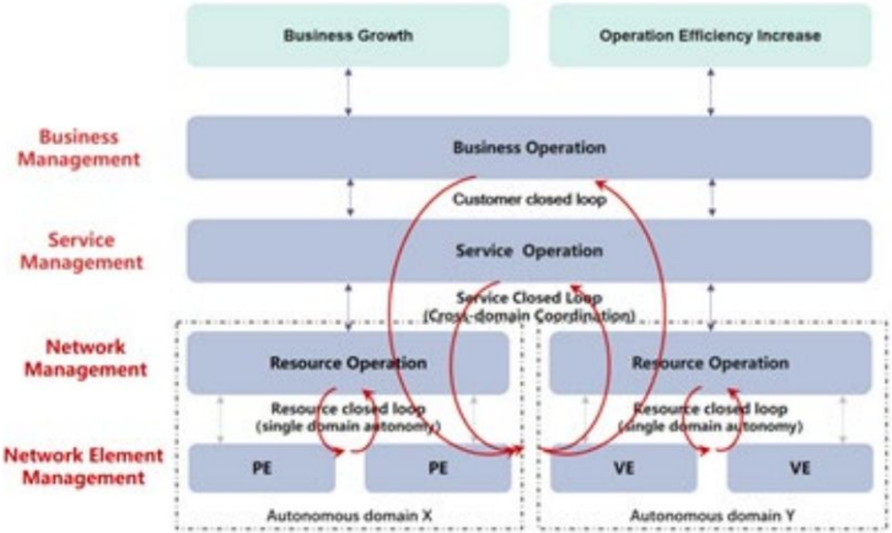

Cross-DomainCollaboration (4 ADs)
Autonomous Domain (Billing & Revenue management)
Autonomous Domain (Service Orchestration)
Resource Operations (Access Network Slice Management)
Resource Operations (Core Network Slice Management)
AN Consumers
Intent Management
ControlLoopManagement
Intelligence
NetworkElement
1. Business Intent (I1)
Business Intent
2. Intent uses shared knowledge
3. Business Order
4. ServiceIntent (I2))
Service Intent
5. Intent uses shared knowledge
6. Service Order (e.g. TMF640))
Resource Intent
7. Resource Intent to AD 1 (I2))
8. A second Resource Intent to AD 2 (I2))
9. Intent uses shared knowledge
10. Handle Intent
11. action
12. Site Intelligence
13. data collection
14. Intent uses shared knowledge
15. Handle Intent
16. action
17. Site Intelligence
18. data collection
Intent Reporting
19. Intent Report from AD 2 (I3)
20. Intent Report from AD 1 (I3)
21. IntentReport (I2)
22. IntentReport (I1)

China Mobiles Framework

Key O&M Scenarios: 6 first-class scenarios, including: planning, development, maintenance, optimization, operation and resource management. 11 second-class core scenarios, including: network planning, design and deployment, monitoring and troubleshooting, patrol inspection, testing, network analysis, network optimization, service subscription, network complaints, resource change management and resource data management.

Key Network Domains: Core network, Radio network, IP network, Transport network, and Telecom cloud.

Key Service Categories: Individual services including mobile Internet, voice, SMS; home services including home broadband Internet, IPTV; business services such as 5G industrial network, APN, IMS, transport VPN, Internet VPN, transport VPN, cloud VPN, MPLS VPN.



Use cases

Fault Analysis and Handling:
The security and reliability is the most important mission of the network, so quick alarm detection and quick fault healing are important. The fault analysis and handling scenario comprises several steps, including alarm monitoring, root cause analysis, and fault remediation.
Monitoring: Real-time monitoring of network alarm, performance, configuration, user experience, and other information.
Analysis: By analyzing the correlation between alarms and other dimensions data, root cause of fault and fault repairing can be achieved quickly.
Healing: Repair fault remotely or by site visiting based on the repairing suggestions

Level 3: Closed loop control of alarms analysis and handling process: Based on the intelligent correlation analysis of multi-dimensional data, accurate location of alarm root cause, precise fault ticket dispatching, and fault self-healing could be reached successfully.

Level 4: Proactive troubleshooting: Based on the trend analysis of alarms, performance, and network data, alarms and faults could be predicted and rectified in advance.

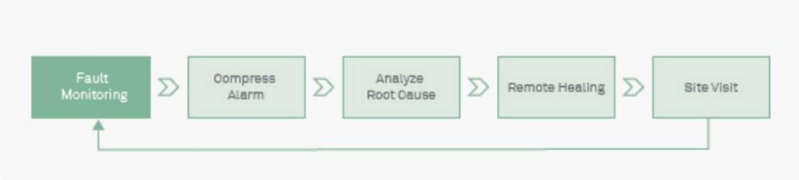


Figure 12. Flow of Fault Analysis and Handling

Use cases

Network Performance Improvement
Wireless networks are geographically very distributed, and activity varies significantly in different places and at different times of day. This makes the network very dynamic and complex. That complexity is further increased by the diversity of services and of terminal performance, and by the mobility of users. If the network cannot achieve the benchmark KPIs or SLAs (service level agreements), or enable good user experience, it must be adjusted to meet or exceed those requirements. The complete process of network performance improvement or optimization includes several stages:

- network monitoring and evaluation
- root cause analysis of performance problems
- optimization analysis and optimization decision-making
- optimization implementation
- post- evaluation and verification

Level 3: Closed loop control of network performance improvement: Automatic identification of network coverage and quality problems, automatic configuration of performance parameters, and automatic evaluation.

Level 4: Dynamic adjustment is implemented based on the scenario awareness and prediction to achieve the optimal network performance. Network prediction capability is available: scenario change trends could be perceived, and network configuration could adjust real-time to achieve optimal performance.

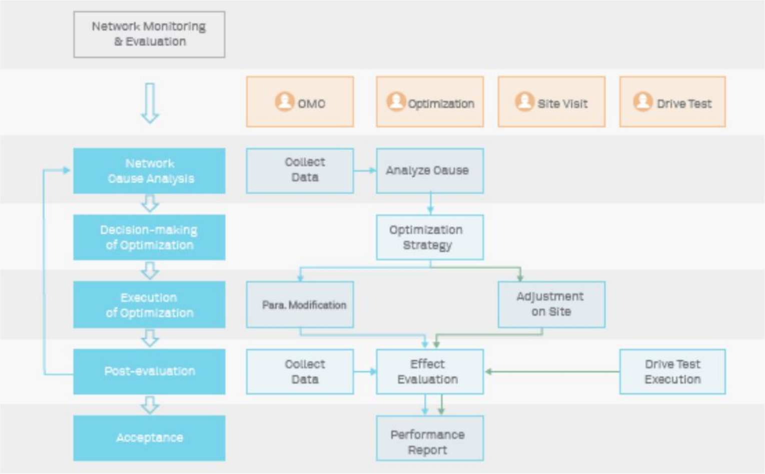


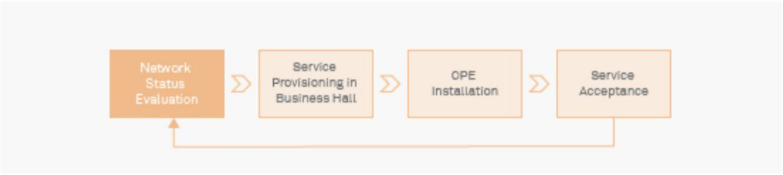
Figure 13. Flow of Network Performance Improvement

Use cases

Wireless Broadband Service Provisioning
WTTx has become a foundational service for mobile operators because of its convenient installation and low cost of single bit. Rapid launch of WTTx service, accurate evaluation after launch, and network development planning have become important supports for new business development.

Level 3: Closed loop for business launch: Integrated with BOSS system to achieve one-step precise launch, remote account launching, CPE installation, fault self-diagnosis and complaint analysis.

Level 4: Auto-balancing of multi-service, automatic value areas identification and network planning recommendation based on network problems forecasting.


Network Status Evaluation
Service Provisioning in Business Hall
CPE Installation
Service Acceptance

Important Docs

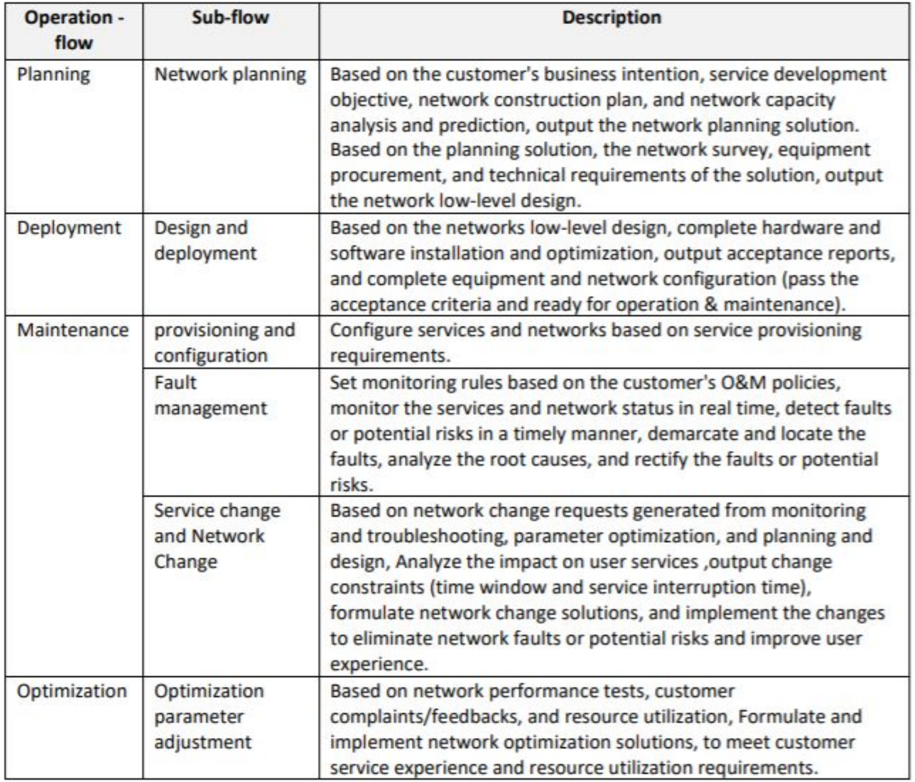
IG1260_Autonomous_Networks_Project_Deliverables_Guide_v1.0.0.pdf	Describe all other documents

Backup Slides

Glossary

Autonomy	The capability to make decisions free from human control.
Automatic	Able to operate independently of human control
Autonomous Networks	A set of network and software platforms that can sense its environment and adapting its behavior accordingly with little or no human input.
Autonomous Network Levels	(Or simply AN Levels) describe the level of autonomic capability in a given operational workflow or for an autonomous domain (L0 to L5). Autonomous Network Levels identify contextual autonomous capability. Also less formally referred to as ‘autonomy levels.
Control loop	Control loops are used to enable autonomous systems to adapt their behavior to respond to changes in user needs, business goals, or environmental conditions.
Intent	Intent is the formal specification of all expectations including requirements, goals, and constraints given to a technical system.
Autonomous Domain	Serves as the basic unit that can fulfill closed-loop automation of specific network operations. An autonomous domain is a set of systems or platforms that is capable of intervention. The autonomous domain does this by realizing self-management capabilities using a closed control loop mechanism, using four key phases: awareness, analysis, decision-making autonomous behavior (e.g., resolve tasks, adhere to objectives) without manual human, and execution. An autonomous domain is a logical construct that provides an administrative governance boundary that defines the scope of the encapsulated autonomous behavior.
Autonomous Platform	An autonomous platform is a system or agent with the ability to complete a task without human intervention, using behaviors resulting from the interaction of software with the external environment. Tasks or functions executed by a platform or distributed between a platform and other parts of the system, may be performed using a variety of behaviors, which may include reasoning and problem identification. In this guide the term ‘Platform’ is preferred over ‘system’ notwithstanding the latter’s ubiquity. The ‘platform’ term is not used in the software architecture sense of the term where a platform provides a foundational set of software services for a product.

Control Processes



Operation - flow	Sub-flow	Description
Planning	Network planning	Based on the customer's business intention, service development objective, network construction plan, and network capacity analysis and prediction, output the network planning solution. Based on the planning solution, the network survey, equipment procurement, and technical requirements of the solution, output the network low-level design.
Deployment	Design and deployment	Based on the networks low-level design, complete hardware and software installation and optimization, output acceptance reports, and complete equipment and network configuration (pass the acceptance criteria and ready for operation & maintenance).
Maintenance	provisioning and configuration	Configure services and networks based on service provisioning requirements.
	Fault management	Set monitoring rules based on the customer's O&M policies, monitor the services and network status in real time, detect faults or potential risks in a timely manner, demarcate and locate the faults, analyze the root causes, and rectify the faults or potential risks.
	Service change and Network Change	Based on network change requests generated from monitoring and troubleshooting, parameter optimization, and planning and design, Analyze the impact on user services ,output change constraints (time window and service interruption time), formulate network change solutions, and implement the changes to eliminate network faults or potential risks and improve user experience.
Optimization	Optimization parameter adjustment	Based on network performance tests, customer complaints/feedbacks, and resource utilization, Formulate and implement network optimization solutions, to meet customer service experience and resource utilization requirements.