TM Forum Introductory Guide

Autonomous Networks Scenario Realizations

IG1230A

Team Approval Date: 28-May-2021

Release Status: Production	Approval Status: TM Forum Approved
Version 1.1.0	IPR Mode: RAND

Notice

Direct inquiries to the TM Forum office:

181 New Road, Suite 304
Parsippany, NJ 07054 USA
Tel No. +1 862 227 1648
TM Forum Web Page: www.tmforum.org

Table of Contents

List of Figures

List of Tables

1 AN Scenario Realizations

1.1 Introduction

Autonomous Network practices can improve both the operational efficiency and end-user experience of today's operator use case. This guide describes scenario realizations of operator use cases using an autonomy mindset and, in particular, the mechanisms described in the AN technical architecture (IG1230). Using closed control feedback and intent-driven interactions, we can deploy smart software to continuously monitor and optimize the networks. Autonomous Networks have become a prerequisite for many more advanced use-cases. For example, with 5G and Software-Defined Networks, often the topology of the network itself is dynamic: higher-level application services dynamically change their network requirements in the same way as cloud-computing applications elastically change their compute requirements. Autonomous Networks can enable concepts like Digital Twins that allow you to model and dynamically simulate changes to a Network to de-risk such changing requirements.

Another example is for mission-critical services that require the network to be "in the loop". An Autonomous Network can interact with the higher-level mission-critical service through APIs to warn of potential service interruptions. An autonomous vehicle could, for example, be warned about crossing an international/roaming boundary and the vehicle could adopt a limited-network mode where it drives more slowly. For industries like healthcare, aviation, and transport, Autonomous Networks must support the move from "best-effort" networks to ultra-reliable "network-in-the-loop" services. This section describes several real-world examples of where operator use cases and requirements were realized using the core concepts of the AN technical architecture.

2 An Example of Self-Healing Capability

2.1 Realizations

The following sections describe examples of how AN Technical Architecture can be practically realized by some implementation functions:

- Business Service Controller
- Service Status
- Elements delivering the service (managed elements)
- Intelligence Management

2.2 Simple 'Canonical' Pattern

The flow for how these implementation features implemented self-healing are described below:

- Start the service running using TMF640 service configuration and activation or TMF664 resource function activation – includes the "intent" parameters.
- Service controller will start a service element **START SERVICE**
- Service element will start producing outputs (TMF635) and performance statistics (TMF628) **PRODUCE SERVICE STATUS**
- The internal service monitor will read the status and compare it against the service intent **MONITOR SERVICE**
- If the intent is not being achieved, then based on analytics, ML or AI the service controller will attempt to achieve the intent by either reconfiguring the service or starting a new service element **REPAIR SERVICE**
- Closed loop control is delivered within the domain. **CLOSED LOOP CONTROL**

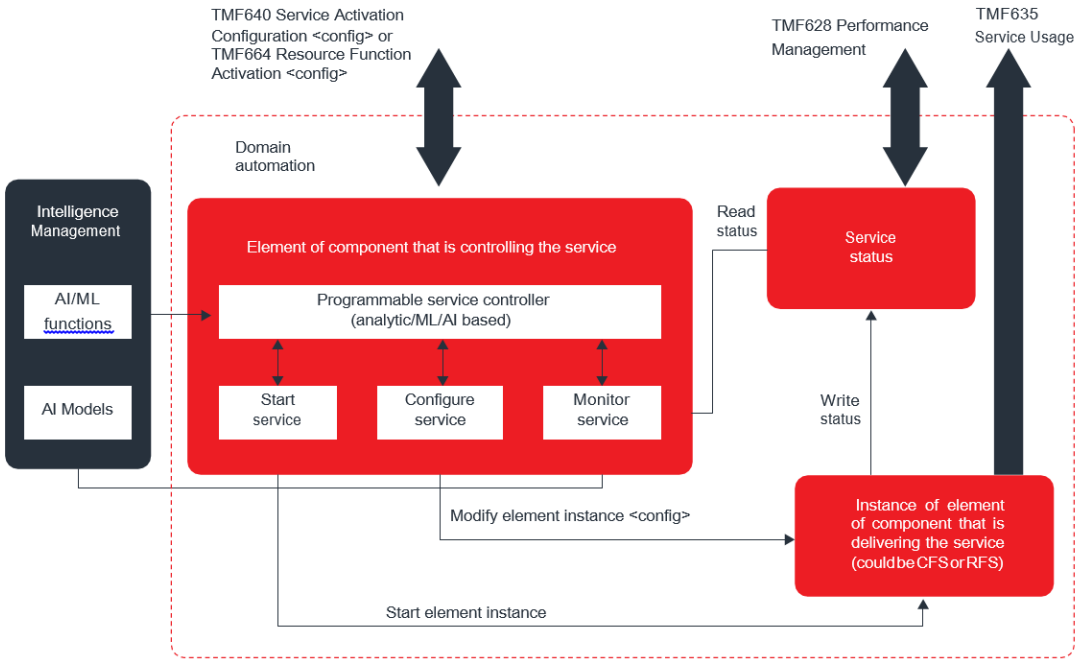

Figure 2-1 Implementation functions for Autonomous Domains

2.3 Recursive Pattern

This simple implementation of a 'canonical' model can be applied recursively to each layer (see Figure 2-2). The flow in this case

- Start each of the required service domains running using TMF622 Product order – includes the "intent" parameters.
- Customer order orchestration and distribution will activate a set of TMF641 Service Order management and start a set of service domains **START BUSINESS SERVICE**

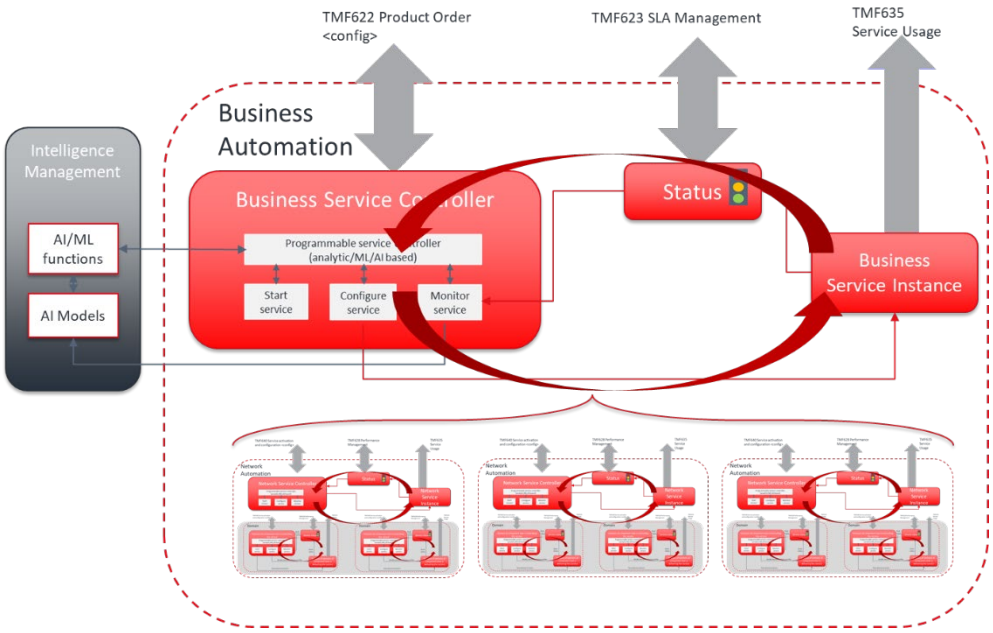

Figure 2-2 Recursive Pattern applied at Business Operations layer

- Service domains will start producing outputs(TMF635) and performance statistics (TMF628) **PRODUCE BUSINESS SERVICE STATUS**
- The internal business service monitor will read the status and compare them against the business service intent **MONITOR BUSINESS SERVICE**
- If the business intent is not being achieved, then based on analytics, ML or AI the business service controller will attempt to achieve the intent by either reconfiguring the network service or starting a new network service **REPAIR BUSINESS SERVICE**
- Closed loop control is delivered within the business domain and between the business layer, the network layer and the resource layer. **CROSS LAYER CLOSED LOOP CONTROL**

3 Electric Vehicle (EV) charging infrastructure business continuity solution

Catalyst	**5G Ride On! (TM Forum Catalyst 2020)** **Electric vehicle charging infrastructure business continuity solution**
Champions	BT, Orange, Telecom Italia
Participants	MDS Group (BSS/CRM) Incognito Software Systems (OSS/Service Activation) TEOCO (OSS/Service Assurance) Huawei (Network Technology and Management)

3.1 Customer Requirements

1) The EV charging customer journey is both a physical journey and an online journey and involves a complex business ecosystem (see Figure 3-3) to make it work. The ecosystem is heavily reliant on connectivity services, and oftentimes communication issues (especially outages) won't go unnoticed by customers. This challenge presents a differentiation opportunity for those who have continuity plans for all scenarios. Connectivity and connectivity related services are needed to enable the EV charging customer journey in several ways:

   - Finding nearby public charge points and checking their availability, connector compatibility, charge level, and in some cases: booking a charging time slot.
   - [In the event the driver is outside their local area] navigating to the selected public charge point using one of the many mobile navigation apps (Google Maps, TomTom Go, HERE WeGo, Sygic, etc.)
   - Performing a payment pre-authorization to unlock the EV charging station equipment. This is a key difference with the gasoline-based car industry: network connectivity is not required to pump gas, it is for the electric car industry (the one exception being home charger).

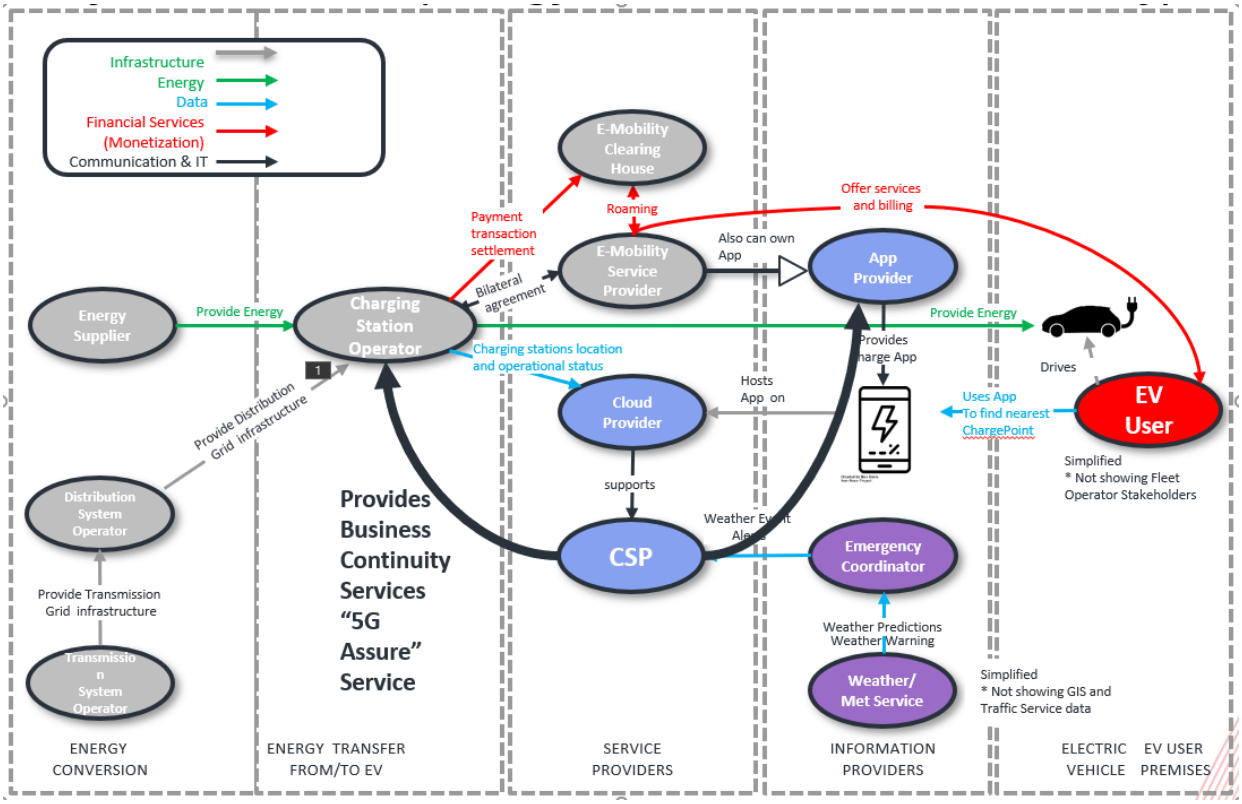

Figure 3-1 EV Charging Ecosystem

If any of the above have an issue they can debilitate the EV charging customer journey, and result in lost revenue for charge point station operators. This has consequences across the broader ecosystem. Thus, a differentiated business continuity solution offering from a CSP (or even a group of CSPs working together) can help better address these pain points and enable a smoother customer experience.

The solution addresses two requirements addressed by different autonomous services, as outlined in Table 1. Note that the business capabilities are per reference guide [IG1218], and the Self-X capability applies to all of them.

3.2 AN Business Capabilities needed to support Services

Table 1 EV Charging infrastructure requirements, metrics, and business capabilities

Service	Autonomous Network Requirements, Metrics, & Business Capabilities			
	User perspective	Business perspective	Service perspective	Network/ICT perspective
	Self-X			
Assured location-based	**Requirements** • Find local EV charging points and their latest	**Requirements** • Advertise Chargepoint status,	**Requirements** • Provide reliable and secure connectivity for	**Requirements** • Provide on-demand onboarding of

Service	Autonomous Network Requirements, Metrics, & Business Capabilities			
	User perspective	Business perspective	Service perspective	Network/ICT perspective
information service	information using a location-based app (mobile, car dashboard) • Book a timeslot at a specific charge point. • Route to selected EV chargepoint station **Metrics** • Load speed **Business Capabilities** • Location awareness • Context-awareness • Automatic navigation • Online service selection • Online service ordering	availability, and price information to prospective customers. • Chargepoint Information must be consistently up-to-date to meet end-user. expectations **Metrics** • Chargepoint Info publish success rate. • Time since the last Chargepoint info publish. **Business Capabilities** • Channel management • Partner management • Product management • Agreement management • Order management	periodic Chargepoint data transfers. • Make local information service available in specific geographical areas in the event of an outage. **Metrics** • Information service availability **Business Capabilities** • Network management • Incident management • Asset management	application to targeted MEC data centers for temporary use. • Assure availability of application across MEC data centers. **Metrics** • MEC platform availability • MEC host availability • MEC application availability • Mobile slice accessibility • Mobile slice traffic volume **Business Capabilities** • Network design • Application onboarding • Application lifecycle management • Network performance management • Incident management
Assured connectivity	**Requirements** • Pre-authenticate for payment and charge electric vehicle 24-7-365 • Frictionless transaction: cashless, secure payment, no human contact needed, email receipt available if required. **Metrics**	**Requirements** • Provide efficient reliable service whenever needed. • Maximize kWh output per chargepoint. • Minimize the number of support staff required to run EV chargepoint facility.	**Requirements** • Provide a highly resilient connectivity solution to meet the needs of the EV chargepoint operator. • Provide redundant connectivity option in event of an outage. • Minimize the resource cost of	**Requirements** • Provide robust connectivity solutions for fixed and wireless. • Scale capacity with demand (i.e., up or down as required) **Metrics** • Fixed Access availability

Service	Autonomous Network Requirements, Metrics, & Business Capabilities			
	User perspective	Business perspective	Service perspective	Network/ICT perspective
Assured connectivity	• Customer satisfaction • No of Customer complaints **Business Capabilities** • Order management (self-ordering) • Self-service	**Metrics** • Chargepoint availability • Chargepoint utilization • Transaction success rate • Average/Std dev transaction duration • #Security incidents • #Customer complaints • Net Promoter Score • #Staff : #Chargepoint Ratio **Business Capabilities** • Customer authentication and authorization • Customer information management • Partner management • Asset lifecycle management • Asset risk management • Product lifecycle management	providing redundant connectivity option. **Metrics** • Service accessibility • Network availability • Network failover success rate **Business Capabilities** • Order management • Product management • Product lifecycle management • Network performance management • Incident management • Partner management •	• Mobile slice accessibility • Scaling success rate • Traffic volume • Security incident rate **Business Capabilities** • Network design • Network activation • Network matching • Network performance management • Network risk management • Network compliance management

3.3 Services

To address the pain points and challenges mentioned, the following services are provided:

- *Online service selection and information: EV drivers can use a mobile or in-car dashboard application to locate the nearest charging stations providing charging services. Drivers can also see all details and status of the chargepoint infrastructure (e.g., what type of connectors are supported, how much power is available to discharge, usage state)*
- *Online service ordering: EV drivers can use a mobile or in-car dashboard application to book a timeslot at a specific chargepoint.*
- *Zero-touch payment: EV drivers can swipe a fob or card to authenticate for payment. The chargepoint then communicates over the network to the chargepoint management system which authenticates the account and subsequently unlocks the chargepoint. The charge to the customer account is applied after the vehicle has been charged.*
- *After the charge is completed the customer can opt to receive an email with a sales receipt.*
- *Agile deployment： The AN stack uses all-scenario automation capabilities to implement intelligent service orchestration, resource orchestration, and process orchestration, improving network deployment agility and implementing process scheduling and orchestration of atomic capabilities. Automated modeling from service requirements to slice and MEC resources, automatic online network resource evaluation, one-click slice deployment, and automatic slice configuration, automated service testing quickly implements automatic closed loop in all scenarios during network O&M and meets the requirements of agile provisioning of electric power services in the industry market.*
- *Intelligent O&M： The AN stack uses technologies such as neural networks and knowledge graphs to automatically provide optimal intelligent O&M policies. It uses ML-derived dynamic thresholds, KPI association analysis, and automatic sub-health detection to detect and provide notification of faults in advance, and AI-based fast fault locating and slice self-healing.*
- *Intelligent failover: The AN stack performs self-monitoring of both fixed and wireless networks involved in the business continuity solution. In the event of a fixed network outage, a wireless network slice is available and self-scaling is used to grow the size of the slice as needed, maximizing resource efficiency. If the geographical area of the fixed network outage grows the AN will perform automatic resource matching with the wireless network and automatically adds the relevant wireless to the scope of the network slice.*
- *Network outage prediction: AI-based network performance functions within the AN use weather and other IoT sensor data to make predictions on future weather conditions on how it will impact the network and network services.*

- *Auto application onboarding: At service order time the AN keeps a record of the mobile application used to serve consumers charging point information. This application would normally run in a centralized public cloud. If a network outage prediction is made that is deemed to impact the EV charging infrastructure the application is onboarded into the appropriate MEC data centers.*
- *Zero-trust DDoS in MEC: Within wireless and core networks there are backoff and access barring mechanisms that detect and prevent denial of service attacks. These mechanisms are governed by configuration. AI algorithms can be used to further optimize these parameters in the event of ever more sophisticated attacks.*

3.4 Business Capabilities

To address the pain points and challenges mentioned, the following business capabilities are provided. While the term not mentioned explicitly below these are fortified with "Zero X" capabilities in the context of AN.

Customer management: This capability provides the ability to control, predict, process, organize, present, and analyze all information, documents, preferences, experiences, and history related to an individual or organization that has, plans to have, or has had an account with the business. It encompasses several other detailed capabilities such as definition, authentication and authorization, preference management, portfolio management, customer matching, and customer information management. A few (not all) are mentioned below.

Customer authentication and authorization: This capability provides the ability to verify customer identity and access rights in the context of a given business scenario and allow a customer to proceed based on those rights or otherwise prevent the customer from proceeding.

Customer information management: This capability provides the ability to organize, track, report on or otherwise disseminate attributes, data, and other perspectives about a customer.

Order management: This capability provides the ability to place, validate, cancel, change, track, fulfill, and otherwise manage a request by one party to another to buy, sell, or exchange goods or services.

Incident management: The capability provides the ability to detect, collect data on, organize, respond and remediate reported troubles/incidents.

Product management: The capability provides the ability to conceptualize, design, develop, bundle, price, launch, maintain and retire goods and services offered by the business.
Network management: The capability provides the ability to design the architecture and plan, develop, deploy, monitor, and report on the network infrastructure. It encompasses several other detailed capabilities such as design, lifecycle management, performance management, compliance management, access management, A few (not all) are mentioned below.

Network design: This capability provides the ability to conceptualize, specify, and model features that a network should have. From an AN perspective, the designs would be automatically generated based on network intent and verified.

Network compliance management: in addition to customer and service intent there are also other business requirements to comply with local rules, e.g., EMF emissions in wireless networks. These would be fed into the business layer and implemented within the wireless autonomous domain.

Network matching: This provides the capability of locating the appropriate resource instances with which to deliver the network intent.

3.5 Using the AN Framework

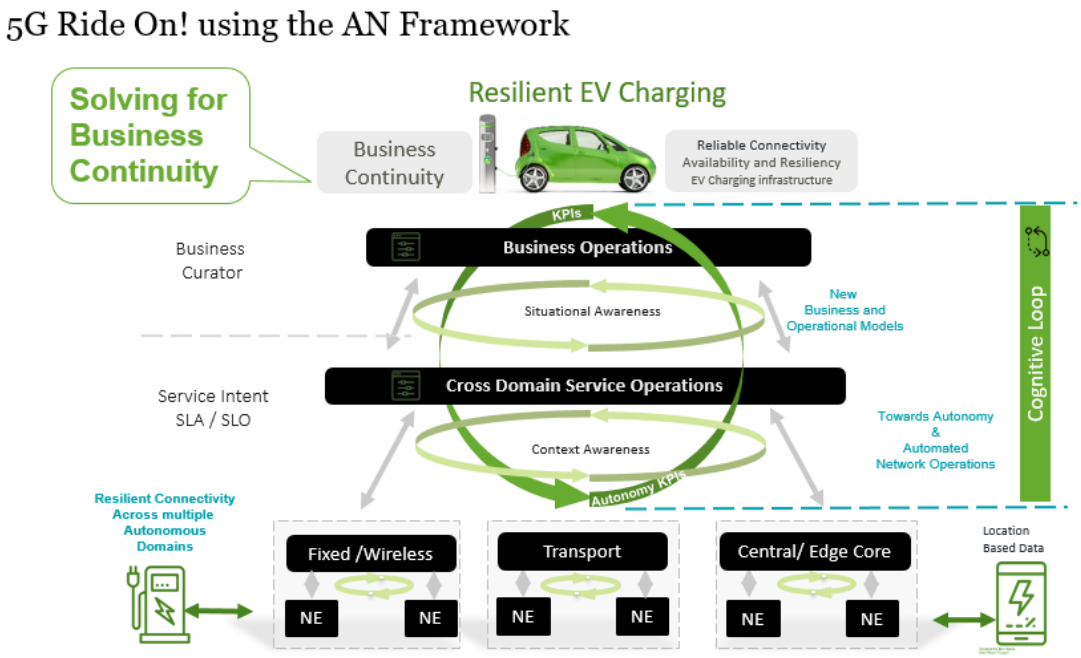

Figure 3-2 5G Ride On! 2020 Catalyst using AN Framework

Figure 3-2 shows how the AN framework can be applied to a specific business objective, namely business continuity. The need for resilience connectivity to provide reliable services was the key focus. The Charge Point Operators as CSP customer is connected to the network using cross-layer customer loop. The vendors provided the system platforms that realized Self-X capabilities and closed loops required. The network is organized into three separate autonomous domains, namely Access, Transport, and Edge-Core. Self-healing and Self-protection within Fixed and Wireless access using 5G, with MEC orchestration and MEC offloading for self-optimization in the Edge Domain.

4 Use Cases using AN Level Evaluation Methodology

This section now describes two use case examples that apply the AN Level evaluation methodology described in IG1230.

4.1 Level Evaluation for IPRAN Assurance

This section selects the monitoring and troubleshooting of the IPRAN network of mobile 2C service as an example to describe the Autonomous Network Level. The monitoring and troubleshooting process is one of the most important processes in CSP network O&M. The full autonomy of the monitoring and troubleshooting process can reduce the workload of personnel and lower the skill requirements for O&M personnel, the troubleshooting duration can be shortened to improve end-user experience. Operation process and operation tasks for the IPRAN network of mobile 2C service are divided into the monitoring and troubleshooting operation process into nine operation tasks.

Task A: Intent Translation. Based on the monitoring and assurance requirements and SLA assurance policies, determine network monitoring rules, such as the monitored area, monitored object (such as NEs or services), alarm type, alarm severity, KPI type, and alarm reporting policy for KPI exceptions. The system monitors the network based on the network monitoring rules.

Task B: Fault identification. Monitors and analyzes network operation data and external data to detect unexpected service interruptions or service quality deterioration promptly.

Task C: Potential Risk Prediction. Monitors and analyzes network operation data and external data, predicts the trend of network software and hardware status, and detects potential exceptions in advance.

Task D: Problem Demarcation. Demarcate faults based on the identified faults and potential risks. In the cross-domain scenario, demarcate the fault to a specific technical domain. In the single-domain scenario, demarcate the fault to a specific NE.

Task E: Root cause location. Based on the problem demarcation result, further locate the specific software and hardware causes (such as configurations, boards, and optical modules) of the problem to support the generation of rectification solutions and rectify services as soon as possible.

Task F: Recovery solution generation. Based on the fault demarcation and locating results, generate several alternative recovery solutions, such as modifying configurations, restarting NEs, replacing boards, and isolating NEs.

Task G: Solution evaluation and decision-making. Evaluate the repair solution (such as whether the solution can solve the problem, whether the repair cost is acceptable, and the extra impact on the network), and provide the optimal solution.

Task H: Recovery solution implementation. Recovery faults and eliminate potential risks based on the optimal solution. For example, deliver configurations to the network for software faults, isolate NEs or links for hardware faults, or replace or remove boards or optical modules onsite.

Task I: Service verification. After fault recovery and risk elimination are performed, verify and confirm the execution results, such as whether service interruption, quality deterioration, and alarms and KPI exceptions are cleared.

6.1.1 Task Criteria for monitoring and troubleshooting of IPRAN network of mobile 2C services

Each task can be completed manually by a human operator, or jointly by the operator and the system, or fully automatically by the system. The following table lists the monitoring and troubleshooting autonomous level standards based on the division of Manual and system：

Table 2 Level Evaluation for monitoring and troubleshooting of IPRAN

AI-based cognitive workflow	Task	L0	L1	L2	L3	L4	L5
Intent	Task A:Intent Translation	Person	Person	System assit person	System assit person	Person assit system	System
Awareness	Task B:Fault identification	Person	System assit person	Person assit system	System	System	System
	Task C: Potential Risk Prediction	Person	Person	System assit person	Person assit system	System	System
Analysis	Task D:Problem Demarcation	Person	System assit person	Person assit system	System	System	System
	Task E:Root cause location I	Person	System assit person	Person assit system	Person assit system	System	System
Decision	Task F:Recovery solution generation	Person	Person	System assit person	Person assit system	System	System
	Task G:Solution evaluation and decision-making	Person	Person	System assit person	Person assit system	System	System
Execution	Task H: Recovery solution implementation	Person	System assit person	System	System	System	System
	Task I:Service verification	Person	System assit person	Person assit system	System	System	System
Scenario applicability		Selected Fault Scenarios					All Fault Scenarios

Level0： All monitoring and troubleshooting tasks are manually completed.

Level1： Problem identification (Task B), Problem Demarcation (Task D), Root cause analysis(Task E), recovery solution implementation (Task H), and Services verification(Task I) are completed by manual and systems (for example, automatic data collection and manual fault identification).

Level2： Based on level 1, Recovery solution implementation (Task H) can be completed automatically by the system.

Level3： Problem identification (Task B), Problem Demarcation (Task D), recovery solution implementation (Task H), and service verification (Task I) can be automatically completed by the system.

Level4： All other tasks except Intent Translation (Task A) are automated.

Level5： All tasks are automatically completed by the system.

4.1.2 Evaluation Method

The evaluation procedure is as follows:

1) *Determine the evaluation object.*

Defined Evaluation Object from service, network, operation process. In this example, select Mobile 2C Service, IPRAN network, Monitoring Troubleshooting operation process as an evaluation object.

2) *Describes the evaluation object operation process and sub=process*
3) *Map to operational tasks and evaluate autonomous level of tasks*

Evaluate the level of each task based on the task criteria and automation capabilities in practice.

Table 3 Level Evaluation for monitoring and troubleshooting of IPRAN network

AI-based cognitive workflow	Task	L0	L1	L2	L3	L4	L5
Intent	Task A:Intent Translation	Person	Person	System assit person	System assit person	Person assit system	System
Awareness	Task B:Fault identification	Person	System assit person	Person assit system	System	System	System
	Task C: Potential Risk Prediction	Person	Person	System assit person	Person assit system	System	System
Analysis	Task D:Problem Demarcation	Person	System assit person	Person assit system	System	System	System
	Task E:Root cause location I	Person	System assit person	Person assit system	Person assit system	System	System
Decision	Task F:Recovery solution generation	Person	Person	System assit person	Person assit system	System	System
	Task G:Solution evaluation and decision-making	Person	Person	System assit person	Person assit system	System	System
Execution	Task H: Recovery solution implementation	Person	System assit person	System	System	System	System
	Task I:Service verification	Person	System assit person	Person assit system	System	System	System
Scenario applicability		Selected Fault Scenarios					All Fault Scenarios

For example, the red box indicates the task assessment of the current situation.

Table 4 Evaluate the level of each task for monitoring and troubleshooting

Operation action of task	Task	AN Level of tasks
design alarm handling rules and policies	Task A： Intent Translation	1
Alarm generate, filter, and report	Task B： Fault identification	4
Alarm parse, standardize, and alarm associate		
None	Task C: Potential Risk Prediction	1

Operation action of task	Task	AN Level of tasks
Problem analysis (demarcating NEs, boards, and ports)	Task D: Problem Demarcation	4
Fault analysis (for example, power failure or fiber cut)	Task E: Root cause Location	3
Design recovery solution.	Task F: Recovery Solution generation	1
Recovery Solution Select	Task G： Solution evaluation and decision-making	1
Fault rectification	Task H： Recovery solution implementation	1
Confirm the Repair Result		
Service test verification	Task I： Service verification	1

4.1.3 Example of evaluation object AN level

In step 3, the task level is evaluated. Based on the average method, the autonomous level of the monitoring and troubleshooting of the IPRAN network of mobile 2C service is 1.9. The Problem identification task and Problem Demarcation task are highly automated. The system collects network alarm, performance, and topology data and automatically aggregates and analyzes the data to accurately identify and demarcate problems.

4.2 Level Evaluation for HBB Intelligent O&M

This section selects Monitoring and troubleshooting of the Home & Access & Metro network for home broadband service (HBB O&M) as an example to describe the Autonomous Network Level. The HBB O&M analysis, task description, task capability criteria, etc. are for reference, and some need to be further researched.

Home broadband (HBB) maintenance is to ensure the voice, Internet, video services, etc., which are carried by the HBB network, it involves fault reporting, network monitoring, network fault handling, network risk check, and potential risk elimination, etc. The following shows the requirement architecture of home broadband O&M.

Network-based complaints rising generally go through three phases: Network Risk/Degradation, Network fault, and User complaint. Customers' requirements and network maintenance focus vary across those phases.

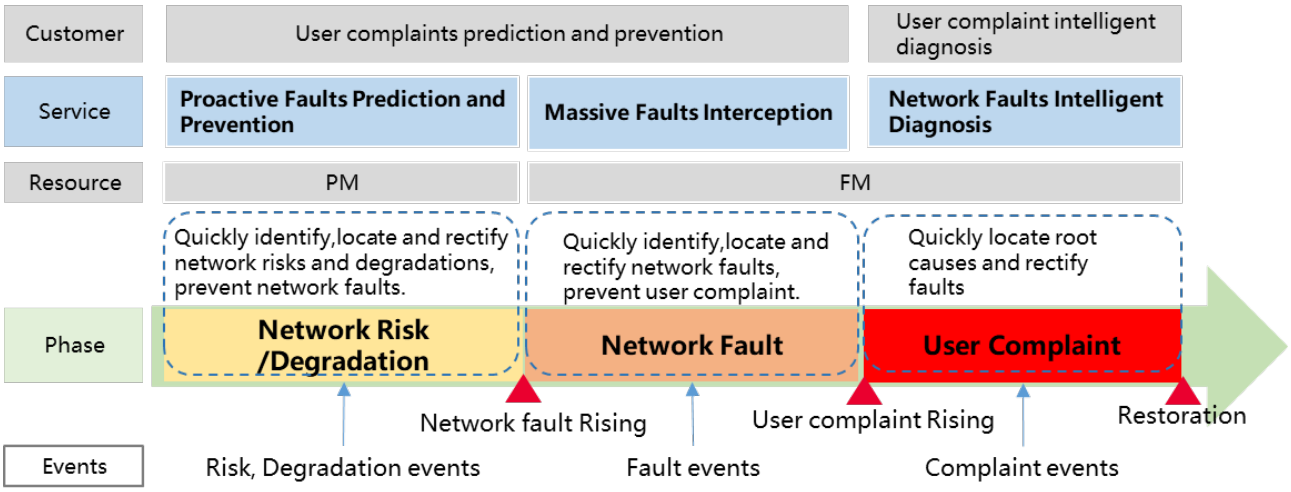

Figure 4-1 Home broadband O&M requirements architecture

4.2.1 Operation process and operation tasks

Base on the 3 phases and service layer described above, there are 3 user cases: Proactive Faults Prediction and Prevention, Massive fault interception, and Network fault intelligent diagnosis.

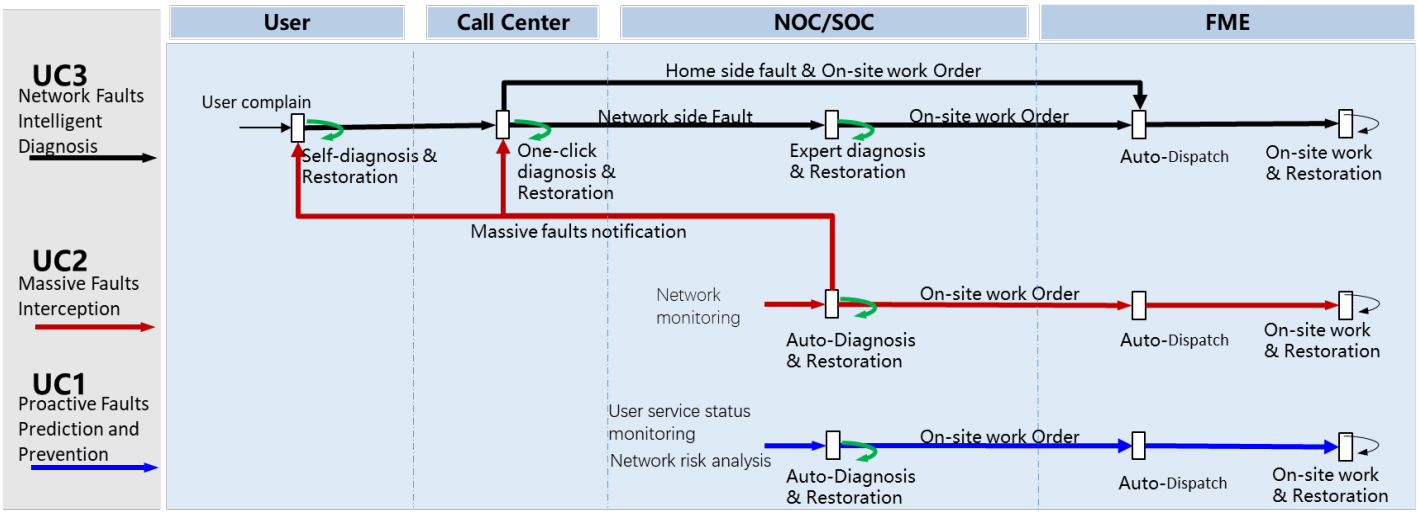

Figure 4-2 Operational processes home broadband O&M use cases

We take UC1 to describe the evaluation method in detail.

Note: UC1 focuses on phase 1 based on Figure - Home broadband O&M requirements architecture, so there is no task - Fault identification in “Awareness”.

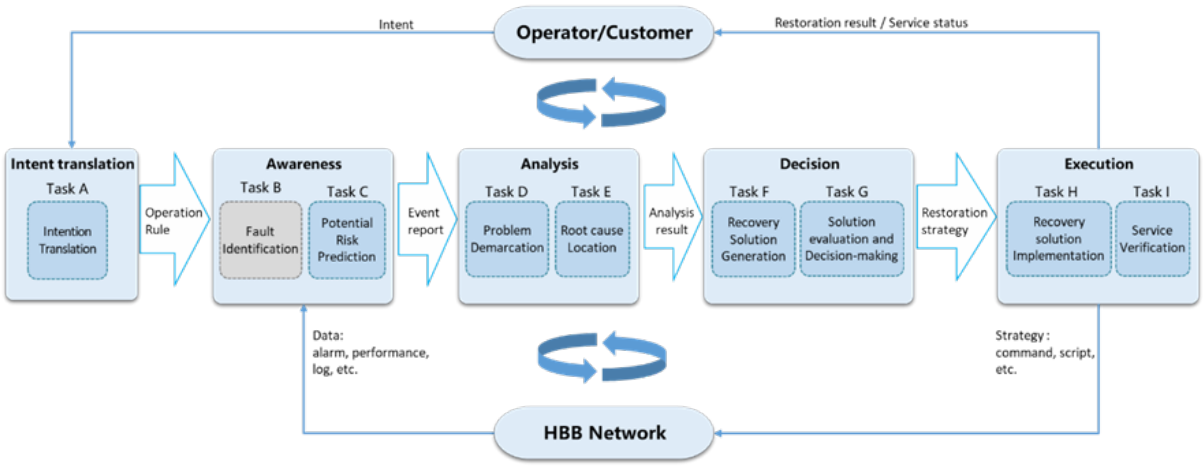

Figure 4-3 Fault Prediction and Prevention workflow

The workflow of proactive faults prediction and prevention use case begins with operation intent. The system receives operation intent from the human operator and translates it into operational rules. These rules specify how the system runs to achieve the goal of operation intent. And the system organizes serial tasks to implement the operation rules. Typically, the tasks can be classified into 4 types: *Awareness, Analysis, Decision, and Execution* as shown in Figure 4-3. The tasks form a closed control loop with network devices to continuously ensure the achievement of operation intent. The tasks of this use case are listed as follows:

Table 5 Task of UC1-"HBB Fault Prediction and Prevention"

Task	Name	Function description for UC1
Task A	Intention Translation	Based on the monitoring and assurance requirements and SLA assurance policies, determine network monitoring rules, such as the monitored area, monitored object (such as NEs or services), alarm type, alarm severity, KPI type, and alarm reporting policy for KPI exceptions. The system monitors the network based on the network monitoring rules.
Task B	Fault Identification	Not Applicable. This UC is for phase 1 which before network fault rising based on the Figure - Home broadband O&M requirements architecture.
Task C	Potential risk Prediction	Detection and data collection: Detects network and home broadband service risks and degradations, and collects related data, such as alarms, performance, configurations, logs, and STB probes. Potential risk identification: Predicts the trend of network software and hardware status and identifies the potential risk of HBB service. Exception event filtering: Removes noises. For example, filter out abnormal events caused by normal user behaviors.
Task D	Problem Demarcation	Demarcate the risk and degradation event to a specific technical domain, for HBB network should be Terminals, Home network, Access network, Metro network, CDN network.
Task E	Root cause Location	Based on the problem demarcation result, further locate the specific software and hardware causes (such as configurations, boards, and optical modules) of the problem to support the generation of recovery solutions.

Task	Name	Function description for UC1
Task F	Recovery Solution Generation	Based on the root causes analysis result, output a feasible recovery solution. Multiple recovery solutions are available, such as remote configuration modification, remote reset, and onsite component replacement.
Task G	Solution evaluation and Decision-making	Evaluate the repair solution (such as whether the solution can solve the problem, whether the repair cost is acceptable, and the extra impact on the network), and provide the optimal solution.
Task H	Recovery solution Implementation	Implement the recovery solution to eliminate potential network risks. For operations that cannot be automatically rectified by the system, manual rectification is needed.
Task I	Service Verification	After the solution is performed, verify and confirm the execution results, such as whether service interruption, quality deterioration, and alarms and KPI exceptions are cleared.

4.2.2 Metrics and Capabilities criteria

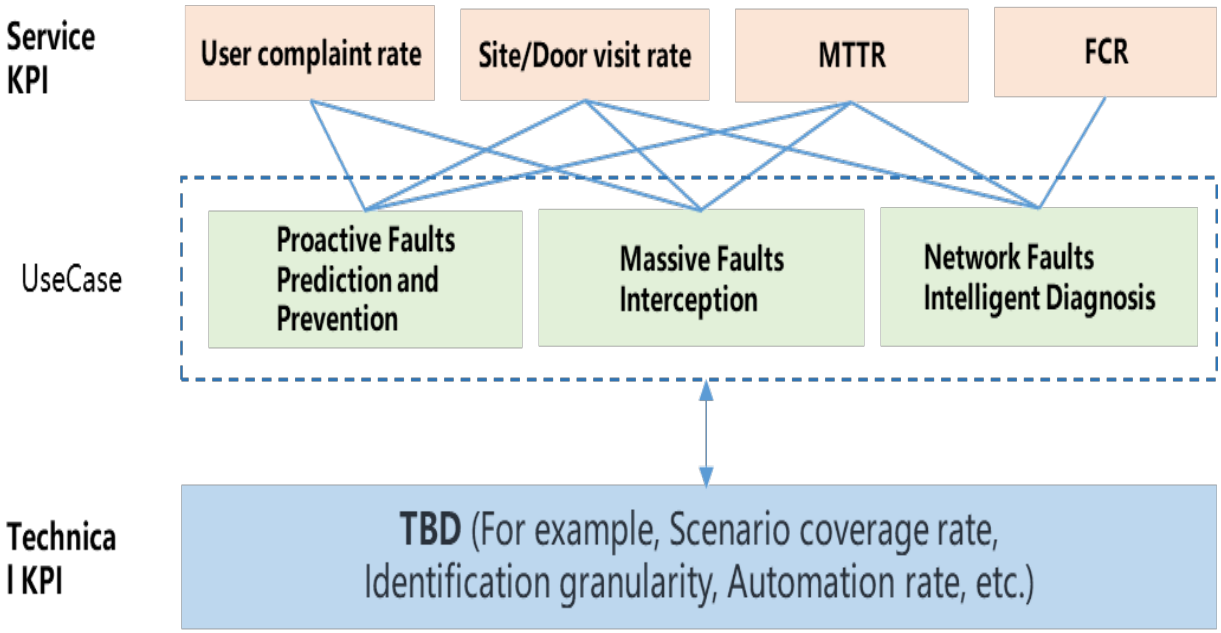

Figure 4-4 Relationship between service KPI, use cases, and technical KPI

Service KPI: Used by most CSP to measure the performance of home broadband O&M. It is not only related to technical KPI but also related to the customer's organization, manpower, and network resource performance, etc.

Technical KPI: To support service KPI, some technical indicators reflect the system capability, we named them Technical KPI. It is the system specifications that dictate the maximum capability of the system under certain conditions. For example, Scenario coverage rate, Identification granularity (like network/port level, service level, application-level), Automation rate, etc. It needs to be further researched.

Capabilities criteria based on task for AN level of HBB Proactive Faults Prediction and Prevention is as below in Table 6 Task level evaluation reference criteria for AN level of “HBB Proactive Faults Prediction and Prevention".

Table 6 Task level evaluation reference criteria for AN level of "HBB Proactive Faults Prediction and Prevention"

Cognitive Workflow	Task	L0	L1	L2	L3	L4	L5
Intent	Task A:Intent Translation	Person	Person	System assit person	System assit person	Person assit system	System
Awareness	Task B:Fault Identification	N/A	N/A	N/A	N/A	N/A	N/A
	Task C: Potential risk Prediction	Person	Person	System assit person	Person assit system	System	System
Analysis	Task D:Problem Demarcation	Person	System assit person	Person assit system	System	System	System
	Task E:Root cause Location	Person	System assit person	Person assit system	Person assit system	System	System
Decision	Task F:Recovery solution Generation	Person	System assit person	Person assit system	System	System	System
	Task G:Solution evaluation and Decision-making	Person	Person	System assit person	Person assit system	System	System
Execution	Task H: Recovery solution Implementation	Person	System assit person	System	System	System	System
	Task I:Service Verification	Person	System assit person	Person assit system	Person assit system	System	System
Scenario applicability		Selected Scenarios					All Scenarios

4.2.3 Evaluation Method

Evaluate the level of each task based on the task criteria above and automation capabilities in practice. Based on the average method, calculate the AN level of "HBB Proactive Faults Prediction and Prevention".

5. Administrative

5.1 Document History

5.1.1 Version History

Version Number	Date Modified	Modified by:	Description of changes
0.1	20-Aug-2020	Kevin McDonnell	Initial Draft.
0.24	18-Sep-2020	James O'Sullivan Kevin McDonnell	Use Cases from Catalysts added
0.36	04-Oct 2020	Kevin McDonnell	Final draft for team review
1.0.0	23-Nov 2020	Alan Pope	Final edits before publication
1.0.1	28-Apr-2021	Kevin McDonnell	IG1230A Guide draft
1.1.0	28-May-2021	Alan Pope	Final edits before publication

5.1.2 Release History

Release Status	Date Modified	Modified by:	Description of changes
Pre-production	25th May 2021	Kevin McDonnell	IG1230A Guide Team Approved
Production	26-Jul-2021	Adrienne Walcott	Updated to reflect TM Forum Approved Status

5.2 Acknowledgments

This document was prepared by members of the TM Forum Autonomous Networks project.

5.2.1 Guide Lead & Author

Member	Title	Company
Kevin McDonnell	Senior Director, Intelligent Automation	Huawei

5.2.2 Main Contributors

Member	Title	Company
James O'Sullivan	Product Director, Intelligent Automation	Huawei
Yuval Stein	AVP Technologies	TEOCO corporation
Wang Lei	Systems Expert	Huawei
Wang Xu	Systems Expert	Huawei

5.2.3 Additional Inputs

Member	Title	Company
Abdul Majid Hussain	Solutions Architect	Telstra
Abinash Vishwakarma	Lead Business Analyst	Netcracker
Andy Corston-Petrie	Senior Research Manager	BT Group plc
Brad Peters	Architect	NBNCo Ltd
Christian Maître	VP Smart Territories	Orange
Dong Sun	Chief Business Strategist, Digital Transformation	Futurewei Technologies
Emmanuel A. Otchere	Chief Technical Expert VP, Standards & Industry Development	Huawei
Joe Isaac	Principal Architect	Wipro Technologies
Johanne Mayer	Consultant	Ciena
Liu Hongbo	Deputy General Manager, Intelligent Network Center	China Unicom
Luigi Licciardi	Consultant, Executive Advisor	Huawei
Manoj Nair	Senior Solutions Architect, CTO Office	Netcracker
Min He	Chief Architect	Futurewei Technologies
Qiao Zizhi	Senior Engineer, Intelligent Network Center	China Unicom
Steve Iatropoulos	Client & Industry CTO	Microsoft
Tayeb Ben Meriem	Senior Standardization Manager	Orange
Thierry Reynard	OSS Consulting Manager	ETIYA
Vance Shipley	CEO	Sigscale
Xie Yuan	Systems Expert	Huawei
Zheng Guangying	Systems Expert	Huawei

5.2.4 TM Forum Staff

TM Forum	Title	Company
Aaron Boasman-Patel	Vice President, AI, Customer Experience & Data	TM Forum
Alan Pope	Collaboration Manager	TM Forum
David Milham	Chief Architect	TM Forum
Ian Turkington	VP, Architecture & APIs	TM Forum
W. George Glass	CTO	TM Forum