White Paper: Application of Artificial Intelligence to Enhanced Network Operations

OIF-ENO-Applic-AI-01.0

August 17, 2023

Technical White Paper created and approved

OIF

www.oiforum.com

The OIF is an international non profit organization with over 100 member companies, including the world's leading carriers and vendors. Being an industry group uniting representatives of the data and optical worlds, OIF's purpose is to accelerate the deployment of interoperable, cost-effective and robust optical internetworks and their associated technologies. Optical internetworks are data networks composed of routers and data switches interconnected by optical networking elements.

With the goal of promoting worldwide compatibility of optical internetworking products, the OIF actively supports and extends the work of national and international standards bodies. Working relationships or formal liaisons have been established with CFP-MSA, COBO, EA, ETSI NFV, IEEE 802.3, IETF, INCITS T11, ITU SG-15, MEF, ONF.

For additional information contact:
OIF
5177 Brandin Ct, Fremont, CA 94538
510-492-4040 ☞ info@oiforum.com

www.oiforum.com

Working Group: **Networking and Operations WG**

TITLE: **Application of Artificial Intelligence to Enhanced Network Operations**

SOURCE:

TECHNICAL EDITORS

Qian HU, Yi DING
China Telecom Beijing Research Institute
Email: huqian@chinatelecom.cn, dingy12@chinatelecom.cn

Ming WEI, Xiang YUN
China Information Communication Technologies Group
Email: mwei@fiberhome.com, yunxig@fiberhome.com

Stephen Shew
Ciena Corporation
Email: sshew@ciena.com

WORKING GROUP CHAIR

Jia HE
Huawei Technologies Co., Ltd.
Email: hejia@huawei.com

ABSTRACT: This whitepaper addresses the interoperability requirements for enhanced network functions that interact between transport networks and their management-control systems. This whitepaper identifies a collection of use cases for the application of Artificial Intelligence to guide interoperability. Along with the benefits of the use cases, the most relevant possible input data requirements, data processing requirements, output data requirements and interfaces related to the use case are provided.

Notice: This Technical Document has been created by the Optical Internetworking Forum (OIF). This document is offered to the OIF Membership solely as a basis for agreement and is not a binding proposal on the companies listed as resources above. The OIF reserves the rights to at any time to add, amend, or withdraw statements contained herein. Nothing in this document is in any way binding on the OIF or any of its members.

The user's attention is called to the possibility that implementation of the OIF implementation agreement contained herein may require the use of inventions covered by the patent rights held by third parties. By publication of this OIF implementation agreement, the OIF makes no representation or warranty whatsoever, whether expressed or implied, that implementation of the specification will not infringe any third party rights, nor does the OIF make any representation or warranty whatsoever, whether expressed or implied, with respect to any claim that has

This document and the information contained herein is provided on an “AS IS” basis and THE OIF DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE OR FITNESS FOR A PARTICULAR PURPOSE.

1. Table of Contents

2. List of Figures

3. List of Tables

4. Abbreviations and acronyms

The following abbreviations and acronyms are used in this whitepaper:

A-CPI	Application CPI
AI	Artificial Intelligence
AI/ML	Artificial Intelligence/Machine learning
API	Application Program Interface
ASON	Architecture for the automatically switched optical network
CPI	Control Programming Interface
EDFA	Erbium-Doped Fibre Amplifier
ENNI	External Network to Network Interface
EMS	Element Management System
ETSI	European Telecommunications Standards Institute
FCAPS	Fault Configuration Accounting Performance Security
IMT	International Mobile Telecommunications
IP	Internet Protocol
ISG	Industry Specification Group
ITU	International Telecommunications Union
ITU-T	ITU Telecommunications Standardization Sector
LSO	Lifecycle Service Orchestration
MC	Management/Control
MEF	MEF Forum
MEP	Maintenance entity group End Point
MIP	Maintenance entity group Intermediate Point
ML	Machine Learning
ND	Neighbor Discovery
NMS	Network Management System
ODU	Optical Data Unit
ONF	Open Networking Foundation
OTDR	Optical Time Domain Reflectometer
OSNR	Optical Signal to Noise Ratio
OTN	Optical Transport Network

PCE	Path Computation Engine
SDN	Software Defined Networking
SDO	Standards Development Organization
TAPI	Transport API
UNI	User to Network Interface

5. Introduction

5.1. Problem Statement

AI/ML based techniques have been applied to many problem spaces including aspects of transport networks. The benefits of big data analysis and extraction of results from seemingly unrelated data sets can assist operators in transport network operations and maintenance.

Standardization of the use of AI/ML techniques for networks is still early. Some examples are:

- Recommendation ITU-T Y.3172 (2019) "Architectural framework for machine learning in future networks including IMT-2020"
- Recommendation ITU-T Y.3177 (2021) "Architectural framework for artificial intelligence-based network automation for resource and fault management in future networks including IMT-2020"

The descriptions in these Recommendations are high level with processes, management, and AI/ML functions identified. The detailed specifications of reference points, functions and associated data required to enable independently developed implementations for the same application is not provided.

To date there has been no activity to standardize AI/ML algorithms in other SDOs.

There is consensus that the *data* on which those algorithms operate is appropriate for standardization and that is under study in at least one SDO (ITU-T).

This Whitepaper addresses the function requirements as well as data requirements to support interoperability when applying artificial intelligence to enhanced network operations.

5.2. Relationship to Other Standards Bodies

This document will analyze available standards to determine any gaps and missing pieces from solution point of view and develop or work with other standard bodies to address them.

Following is the list of SDOs and their corresponding areas/projects that are candidates for co-operation/reuse.

1) ITU-T SG15

2) ONF OIMT and OTCC

5.3. Scope

This whitepaper identifies the functions, interfaces, and associated data required to support development of AI/ML to enhance network operations. Detailed specifications are beyond the scope of this whitepaper. We seek to identify the needed specifications (a gap analysis) and thereby provide a roadmap or requirements to motivate development of those specifications in OIF or some other appropriate body e.g., ITU-T, ONF, MEF.

The artificial intelligence use cases in this document are designed to illustrate only some of the possible applications of artificial intelligence to enhanced network operations. The list is not exhaustive or final; there are many other possible applications and more may be investigated in the future.

The AI use cases include: Intelligent Network Traffic Prediction, Intelligent Maintenance of Packet/optical Network, Intelligent OSNR Prediction, Intelligent Deployment & Optimization of Packet/optical Network and Fibre Cable Pre-warning and Fault Localization. There are many other possible applications and more may be investigated in the future.

5.4. List of Contributors

We acknowledge and thank the work from the following contributors.

Company	Contributors
China Telecom	Qian HU, Yi DING, Yan LIU, Xin QIN
CICT	Ming WEI, Xiang YUN, Kam LAM, Zhiyong HU, Zhiyong TAO
Ciena	Stephen Shew, Lyndon Ong
Huawei	Jia He
Infinera	Jonathan Sadler, Paul Doolan
Nokia	Dave Brown

6. Management and Operations – lifecycles of control

Networks are subject to multiple lifecycles of control. One such lifecycle involves design and installation of equipment and fibres, their maintenance, and ongoing changes (adds/moves etc). A second lifecycle involves configuration and instantiation of services, calls, and connections. Ongoing actions to these include teardown, modification, and response to disruptions and degradation. A third lifecycle includes the actions of monitoring, optimizing, and upgrading the network.

The OIF networking IAs (UNI, ENNI, ND, PCE) and the ITU-T SG15 management and control Recommendations ([ITU-T G.7701], [ITU-T G.7702], [ITU-T G.7703], and work on information modeling) describe functions and applications that are largely associated with the second lifecycle that provides services from the network. In addition to these, network operators use applications that assist with the other two lifecycles. For example, planning applications that optimize equipment placement/configuration, where to put fibre routes, accommodates for growth, and assists with technology selection. Once a network is installed and providing services, applications outside of those used in the second lifecycle could include monitoring based on various sensor and alarm/performance data, predicting traffic growth, and predicting faults. In this whitepaper, these applications are called Enhanced Network Operations, and are positioned as complementary to the management/control functions associated with the second lifecycle. Technologies for Enhanced Network Operations have included optimization techniques like multi-commodity flow solutions (e.g., linear programming), simulation, genetic algorithms, and statistical analysis.

6.1. ITU-T Architecture of management-control for transport networks

ITU-T SG15 has been studying management and control architectures for transport networks for many years. The OIF UNI, ENNI, and PCE Implementation Agreements specify details that may be used to implement the reference points and functions in the [ITU-T G.8080] “Architecture for the automatically switched optical network (ASON)”. When SDN was studied for transport networks, common functions with ASON were identified and described in ITU-T G.7701 [1]. Applying SDN architecture was then described in ITU-T Recommendation G.7702 [2] and ASON architecture described in ITU-T G.7703 [3] (which superseded [ITU-T G.8080]). The distinction between what were known as the control plane and management plane has disappeared in the later Recommendations as the same functions often appeared in both. Those functions are now called Management and Control (MC) functions in the ITU-T G.770x series Recommendations and can be applied in SDN and ASON architectures. Other systems such as NMS/EMS that include FCAPS functions can also implement MC functions. They then become another type of MC system as are SDN MC systems and ASON MC systems.

Figure 1 is from ITU-T G.7703 [3] and shows MC components, management of MC components, and how they can be used in various types of MC systems. As mentioned above, OIF IAs fit into the ASON MC system architecture and specifically:

- OIF UNI 2.0 – specifies protocols for the ASON UNI (signaling)
- OIF ENNI 2.0 – specifies protocols for the ASON ENNI (signaling, routing, multilayer, recovery)
- OIF ND – specifies protocols for the ASON discovery component

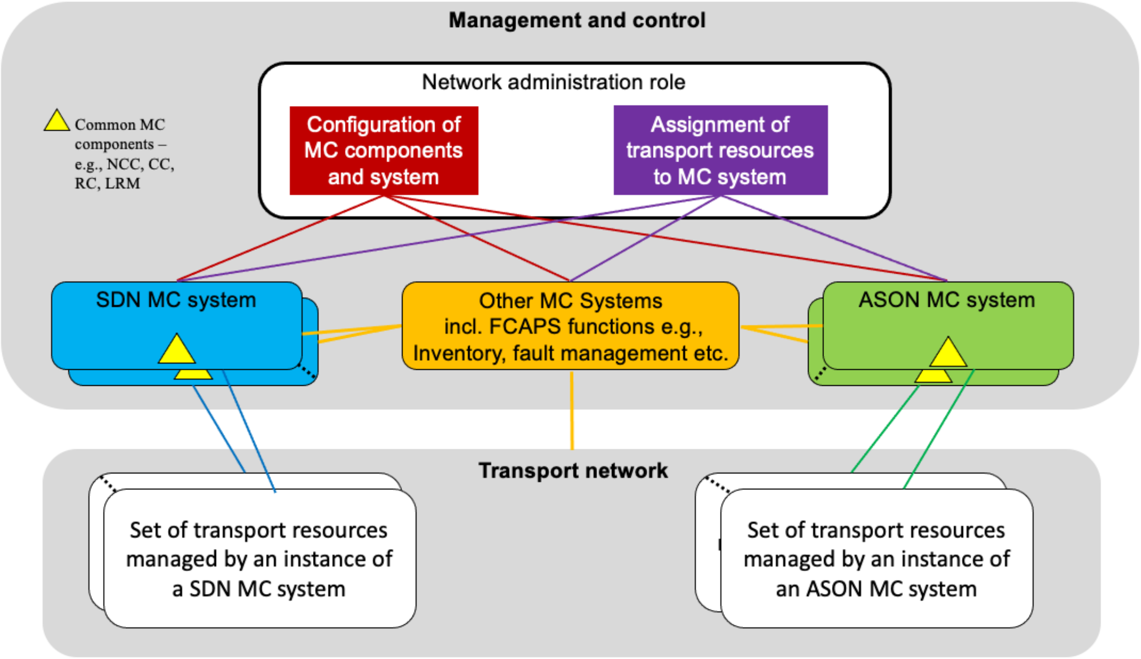
Management and control
Network administration role
Configuration of MC components and system
Assignment of transport resources to MC system
Common MC components – e.g., NCC, CC, RC, LRM
SDN MC system
Other MC Systems incl. FCAPS functions e.g., Inventory, fault management etc.
ASON MC system
Transport network
Set of transport resources managed by an instance of a SDN MC system
Set of transport resources managed by an instance of an ASON MC system

Figure 1 Architecture of management-control for transport networks (from Figure 6-1/G.7703 [3]). Used by permission from the ITU-T.

Figure 1 is an architectural view of management and control, and does not specify where its functions reside. The transport network box represents resources that transfer information (the forwarding "plane") only and these include [ITU-T G.800] layer networks as well as [ITU-T G.807] media networks. Network equipment is a packaging of MC functions and transport network resources. For example, an Ethernet NE contains one or more Ethernet switches and MAC forwarding functions (typically in network processors) which are in the transport network box of Figure 1. It would also have various functions shown in the Management and control box of Figure 1 including discovery, monitoring (e.g., [ITU-T Y.1731] MEPs/MIPs), distributed routing (IEEE 802.1aq), alarm generation, configuration, and provisioning. An ONF TAPI attached to an NE is essentially in the management and control box and its function residing on the NE is in close proximity to the switching function found in the transport network box in Figure 1, i.e., running over the blue line connecting an SDN MC System to transport networks in that figure could be an instance of the ONF TAPI.

In the SDN architecture, SDN controllers have a northbound and southbound interface to transport resources and to other SDN controllers. The ONF TAPI ([6]) is an instance of these interfaces and has been used in previous OIF network interoperability demonstration (see OIF

2020 Transport SDN API Interop Demo White Paper). In Figure 1, the blue line connecting an SDN MC Systems to transport networks could use the ONF TAPI.

6.2. Enhanced network operations

There is a common understanding in the Standards/Fora ecosystem that applications are distinct from MC systems but use interfaces exposed by the MC systems to interact with transport networks. Examples of these application/MC system relationships are:

- Business applications as depicted in OIF-FD-Transport-SDN-01-0 “Framework for Transport SDN: Components and APIs”
- The applications plane and the A-CPI in ONF TR-521 “SDN Architecture 1.1”
- Customer and operator applications in Figure 6-3 of ITU-T G.7702 [2]
- Applications that use the user side of the UNI in ITU-T G.7703 [3] “Architecture for the automatically switched optical network”

Service providers would typically use applications to configure services, for example, an ODU3 service over an OIF UNI interface.

In addition to configuring services, providers use other applications for network planning, forecasting demand, predicting errors and faults, monitoring alarms and error conditions, and optimization. These do not setup calls/connections, but are needed for example, to understand when it may be necessary to modify capacity and to understand reliability levels within transport networks. Such applications may employ techniques such as simulation, statistical analysis, linear programming, and modelling.

Enhanced network operations are external to MC systems as shown in Figure 2 and examples of data to/from those operations are in Table 1.

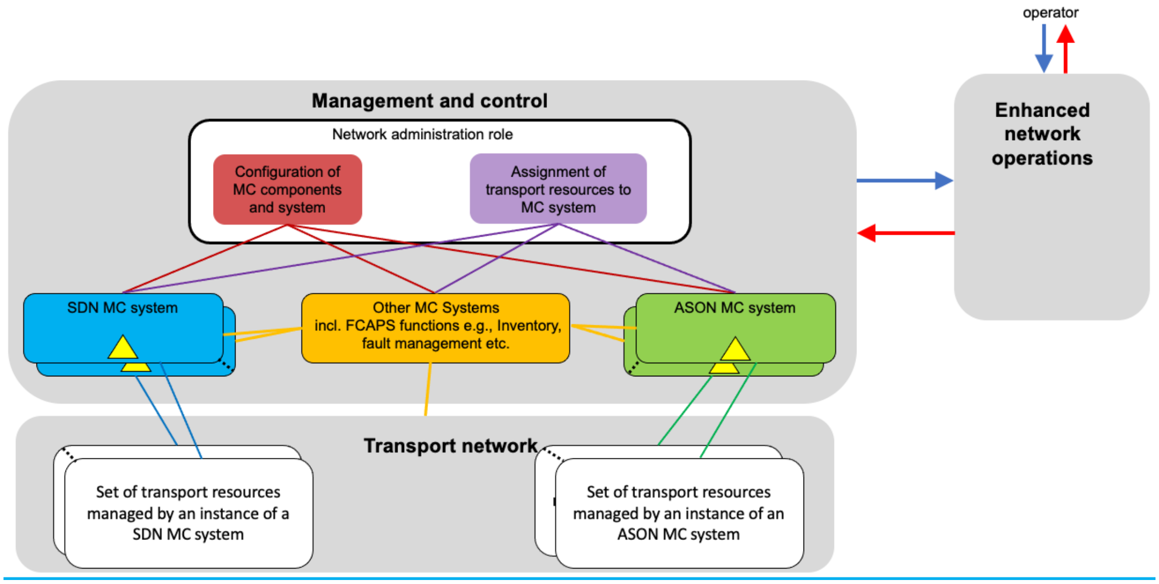
operator
Enhanced network operations
Management and control
Network administration role
Configuration of MC components and system
Assignment of transport resources to MC system
SDN MC system
Other MC Systems incl. FCAPS functions e.g., Inventory, fault management etc.
ASON MC system
Transport network
Set of transport resources managed by an instance of a SDN MC system
Set of transport resources managed by an instance of an ASON MC system

Figure 2 Enhanced network operations and MC systems

Table 1 Reference point – example data

Example Inputs	Example Outputs
• Network topology • Utilization • equipment state • alarms, logs • weather • time series	• Equipment activation/deactivation/ordering • Connection changes • Traffic forwarding changes • Network configuration changes

From the transport network, information such as alarms and utilization can pass to MC systems, which can then pass them to enhanced network operations. The SDN CPI is an example interface that could be used by an enhanced network operation. Input to enhanced network operations may also come from an operator. For example, anticipated capacity changes due to services that are pending activation.

Outputs of enhanced network operations could include reconfiguration of traffic forwarding functions that result from traffic optimization. It could also include changes in transport resources such as installing additional hardware. Commands to MC systems may also be an output. For example, setting up and tearing down connections as part of network defragmentation.

6.3. AI based enhanced network operations

Enhanced network operations may be implemented using AI/ML based techniques. Use of AI/ML based enhanced network operations can improve operational efficiency compared to manual operation and maintenance procedures. They can be integrated with MC systems (e.g., SDN controllers) by adhering to the architecture shown in Figure 2.

A specific example of an AI-based enhanced network operations application is network traffic prediction and is shown in Figure 3. Data from the transport network could include time series of link utilization and protection/restoration events. Outputs could include operations to optimize the traffic such as re-configuring forwarding functions and adding/moving connections. Equipment change orders are depicted as a type of input (the dashed line) and are meant to represent changes/upgrades to equipment. They would typically involve physical equipment installation/removal followed by requests to management and control to configure MC systems. As utilization in the network changes, the traffic predictor can predict future utilization and suggest actions to optimize for future loads.

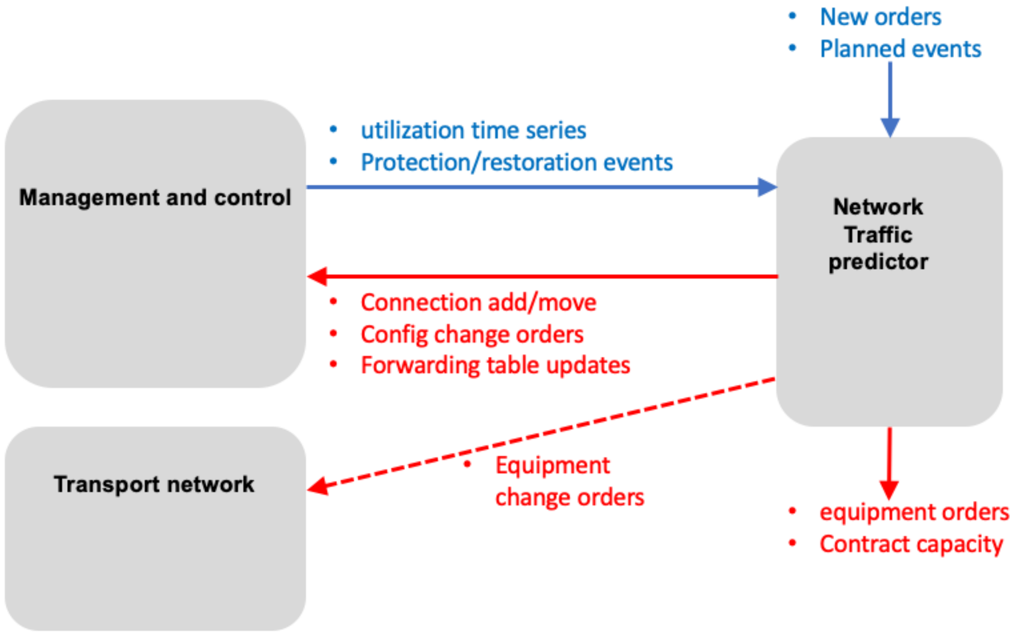

Figure 3 Example of traffic predictor enhanced network operation

6.4. Interoperability Goals

To date there has been no activity to standardize AI/ML algorithms in other SDOs.

There is consensus that the *data* on which those algorithms operate is appropriate for standardization and is under study in at least one SDO (ITU-T).

The development of interoperable AI/ML applications requires definition of inputs to and outputs from enhanced network operations. Descriptions of interoperable AI/ML applications should include the specification of interfaces, data, and descriptions of some enhanced network operations that can be used with management-control systems. These could be the subject of an interoperability demo.

Figure 4 illustrates interoperability points between MC systems, transport networks, and enhanced network operations. Inputs are shown as blue arrows, and outputs as red arrows. Inputs include formats, interface types, and parameters. Outputs include formats, interface types, and network instructions.

Data from transport network functions flow to MC functions that would typically be co-located. For example, they may be with the same OTN NE. If for example, a link fails, a hardware condition is detected in the TN function and reported to link management and alarm generation software running on the MC functions of NE.

Between the transport network and MC systems, the interfaces tend to be defined in SDOs that study MC systems. For example, the ONF TAPI and MEF LSO Adagio interface reference point.

Data such as faults would typically start in the transport network and be passed to an MC system over some notification interface, before being sent to an enhanced network operation.

The description of an enhanced network operation should be independent of implementation and should not depend on specific instances of data inputs.

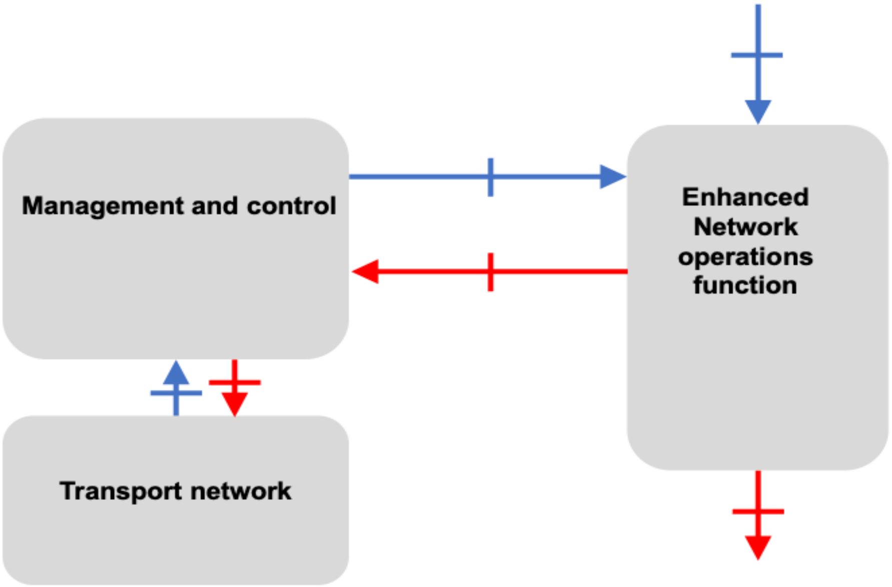

Figure 4 Interoperability points

From an operator’s perspective, specification of inputs, outputs, and type of enhanced network operation allows the operator to select different vendors for the transport network, MC system, and enhanced network operation. For example, an IP network with routers from one or more vendors, an SDN controller for an IP router network, and an IP traffic prediction function based on AI technology.

7. Enhanced network operations

7.1. Reference point to MC systems

The reference point between MC systems and enhanced network operations is an SDN CPI [2, 3, 5]. It is capable of passing data specified in 7.2 and 7.3, and is illustrated in Figure 5 which simply adds the reference point to Figure 2.

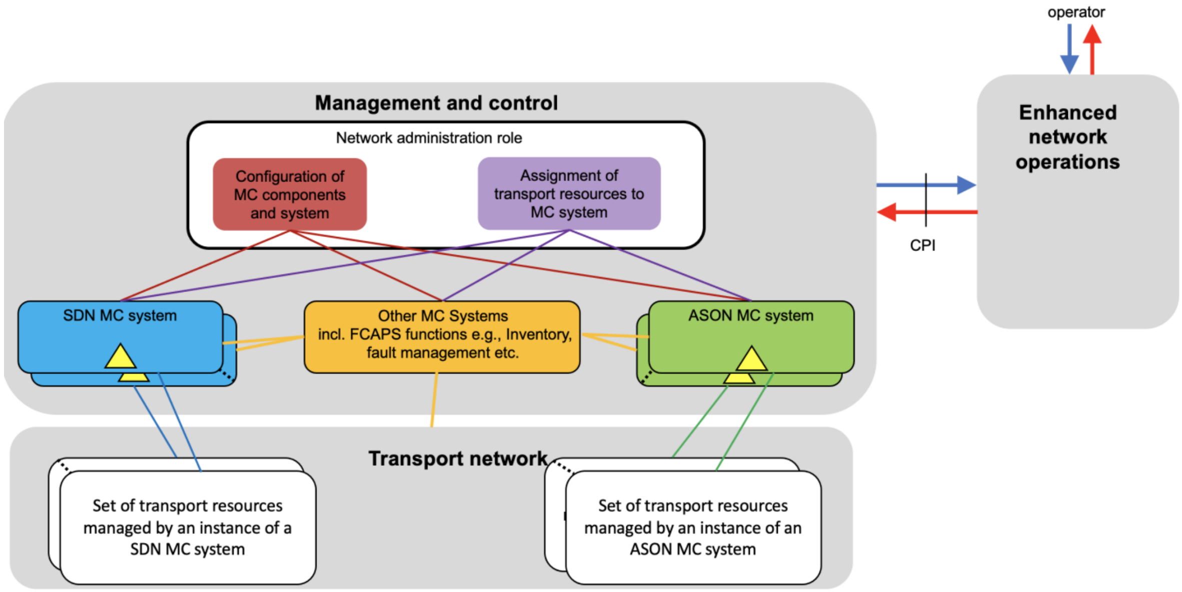
operator
Management and control
Network administration role
Configuration of MC components and system
Assignment of transport resources to MC system
Enhanced network operations
CPI
SDN MC system
Other MC Systems incl. FCAPS functions e.g., Inventory, fault management etc.
ASON MC system
Transport network
Set of transport resources managed by an instance of a SDN MC system
Set of transport resources managed by an instance of an ASON MC system

Figure 5 Reference point between enhanced network operations and MC systems

Any MC system could support an SDN CPI to an enhanced network operation function and a specific example of this is shown in Figure 6. CPIs may be arranged hierarchically and Figure 6 shows two CPIs supporting the same enhanced network operations interaction with transport resources. One place is between resources and a server context of an SDN Controller and the second place is between the client context of the same controller and an enhanced network operation function. The network administration role in Figure 6 is the same as that in Figure 5 but with less detail.

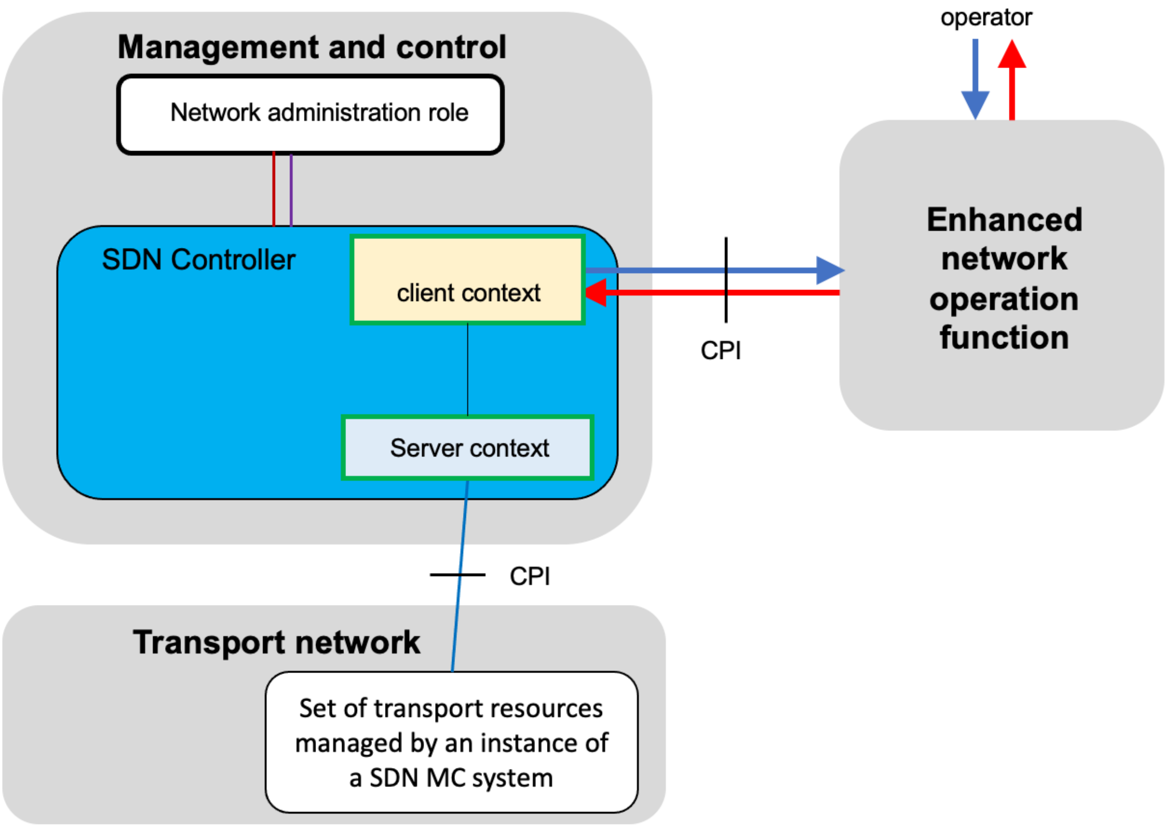
operator
Management and control
Network administration role
SDN Controller
client context
Server context
CPI
Enhanced network operation function
CPI
Transport network
Set of transport resources managed by an instance of a SDN MC system

Figure 6 Supporting an SDN CPI from a client context

7.2. SDN CPI to/from enhanced network operations

At a high level, inputs to enhanced network operations from management and control systems may include:

- Topology. Topology may be single or multi-layer. It supports standardized layer networks and includes nodal and link parameters. Resources represented by the topology may be detailed and/or abstracted (virtual).
- NE configuration. Equipment parameters include chassis, slot, cards, ports, etc. as well as device lists and physical-context (get physical span, physical span list).
- Active connections
- Resource utilization. This includes link utilization (port level), total-potential-capacity, available-capacity, cost-characteristic, and latency-characteristic (fixed latency, queueing latency, jitter, wander).
- Optical link performance (bit errors, EDFA performance)
- Forwarding performance
- Alarms, logs. These include detail alarm info, perceived severity type, probable cause, and if it is service affecting. Measurements such as loss, delay, unavailable time, jitter

can be passed. A notification subscription procedure to enable receipt of performance and alarms may be supported.

At a high level, outputs from enhanced network operations to management and control systems may include:

- Configuration
- Updated forwarding tables
- Granularity, Tolerance Rate

The inputs and outputs listed are examples of possible data. Sets of data are specific to an enhanced network operation.

7.3. Operator interface to/from enhanced network operations

Inputs from an operator may include:

- Granularity, Tolerance Rate
- Adjustment Period
- Environmental data such as weather
- OSNR parameters
- Power curve of OTDR
- Fault localization information, service update requirements and resource optimization requirements

Outputs to an operator may include:

- Predicted loads
- Root cause, maintenance actions
- OSNR prediction
- Optimization suggestions. The enhanced network operation sends recommendations and/or management instructions to improve decisions that configure transport network (e.g., change some statically defined parameters to improve resource utilization).
- Fibre warning, fault location, and trouble tickets
- Resource requests. These include additional resources, and re-deployment of resources.

The inputs and outputs listed are examples of possible data. Sets of data are specific to an enhanced network operation.

8. Use Cases

This Section provides use cases of artificial intelligence to enhanced network operations.

The interoperability requirements (Input/output data, interfaces, functions) are specified.

8.1. Use Case #1: Intelligent Network Traffic Prediction

1. Overview

In the traditional operation & maintenance and construction methods the service bandwidth carried by the optical network is generally determined by the upper application requirements, the number of device nodes and the configuration of capacity need to be planned before the construction, and then to be modified as needs change. This method generally has the disadvantages of long expansion cycle and poor customer service experience. Especially in the case the optical network directly provides private line services to customers, the expansion period often lags customer demands.

Introducing AI into the traffic prediction of optical network is helpful to optimize the network resource allocation, reduce the network operation cost, locate and predict traffic abnormal conditions, reduce network congestion, and improve the quality of user experience. As an example, intelligent network traffic prediction can provide a way to predict Ethernet network traffic in Ethernet layer over OTN in the future just based on historical traffic data and related configuration parameters. Prediction and decision results can be used to plan network expansions or optimize network traffic routing effectively.

2. Interaction with enhanced network operations

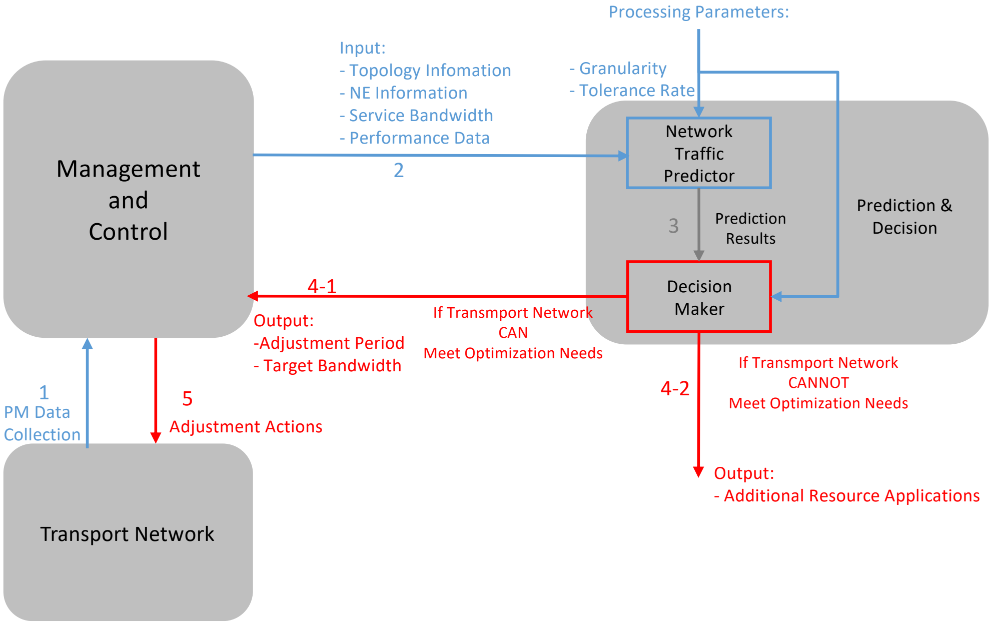

Figure 7 Interaction with Network Traffic Prediction

In step 1, Management & Control system gets PM data from transport network by a collection method such as Telemetry.

In step 2, Management & Control system provides some data (e.g. Topology Information, NE Information, Service Bandwidth, and Performance Data) as input of Network Traffic Predictor. At the same time, processing parameters are input into Network Traffic Predictor (e.g. Granularity, Tolerance Rate) and Decision Maker (e.g. Adjustment Period).

In step 3, Network Traffic Predictor provides prediction results for Decision Maker, which will draw a conclusion of bandwidth adjustments or resource applications according to Transport Network capacities. If the transport network can meet the adjustment need, then it goes to step 4-1. Otherwise, it goes to step 4-2.

In step 4-1, Decision Maker outputs the adjustment period and target bandwidth for Management & Control system, which can take some adjustment actions to optimize the Transport Network as shown in step 5.

In step 4-2, Decision Maker outputs additional resource applications in order to get additional resources for the Transport Network.

In step 5, Management & Control system takes some adjustment actions to optimize the Transport Network.

3. Use Case driven requirements

- Input data requirements

a) Require traffic consumption data which is labeled according to the application, protocol type, and location.

b) Bandwidth utilization data is collected for each port.

c) Bandwidth utilization data can be collected at second/minute/hour/day level.

d) Previous 1-60 months data is used for prediction.

e) Require continuous collection of traffic consumption data at port level.

f) Require tagging timing and location information of the collected data.

g) Require storing the collected traffic consumption data for a sufficiently long duration up to 60 months.

Data format as follows.

Table 2 Input of Network Traffic Predictor

Data	Description
Topology ID	Topology represents link and subnetwork (switching) resources. These resources may be abstract or supported by software and hardware implementations.

	The topology identifier is unique in the context of some scope which could be global.
Port ID	The port can perform the termination and adaptation functions of one or more transport layers. It supports all transport protocols including circuit and packet forms. The port identifier is unique in the context of some scope.
Line Card ID	The line card may plug into equipment. The line card identifier is unique in the context of some scope.
Network Element ID	The identifier of Network Element.
Location ID	Location represents where the equipment is. It could be geographical location.
Time Index	At the end of the measurement interval, the timestamp is reported.
RX_BYTES (average)	per port/time cycle Average bytes received per port during measurement duration.
TX_BYTES(average)	per port/time cycle Average bytes transmitted per port during measurement duration.
RX_BYTES (peak)	per port/time cycle Maximum bytes received per port during measurement duration.
TX_BYTES(peak)	per port/time cycle Maximum bytes received per port during measurement duration.
Service Bandwidth	The bandwidth allocated to the service.
Processing Parameters	measurement duration, performance throughput

- Processing requirements

a) Require training traffic forecast model based on the collected data.

b) Require the capability of adding factors such as holidays to get the final traffic prediction result.

c) Require the real-time flexible traffic prediction at different time granularities.

d) Forecast type: Offline forecast, online (real-time) forecast.

e) Granularity: Data Collection Cycle (1s, 30s, 1min, 15min, 24h), Data Storage Cycle (1 month, 3 months, 6 months, 1 year, 3 years, 5 years).

f) Tolerance Rate makes an allowance for the prediction, which can be formulated as Target Bandwidth = Predicted Throughput * (1 + Tolerance Rate). Suggested Tolerance Rate is 0.2.

g) Effective Period (1 day, 1 month, 3 months, 1 year or permanent) provides a duration after each adjustment action to the transport network.

- Output data requirements

a) Require the output from Network Traffic Predictor as the internal input of Decision Maker, not for the external presentation.

b) Require the decision result from Prediction and Decision as the only external presentation.

Data format as follows.

Table 3 Output of Network Traffic Predictor

Data	**Description**
Time Index	At the end of the measurement interval, the timestamp is reported.
Predicted Throughput	The predicted throughput of Network Traffic Predictor

Table 4 Output of Decision Maker

Data	**Condition**	**Description**
Adjustment Period	the transport network CAN meet the need of target bandwidth	the duration after each adjustment action to the transport network, e.g. 1 day, 1 month, 1 year, permanent
Target Bandwidth	the transport network CAN meet the need of target bandwidth	target bandwidth = predicted throughput * (1+tolerance rate)
Resource Application	the transport network CANNOT meet optimization needs	additional resource application

- Interface and function requirements

a) Get topology information.

b) Get NE information.

c) Get performance data.

MC system can get performance data from transport network through streaming or traditional performance collecting.

8.2. Use Case #2: Intelligent Maintenance of Packet/optical Network

1. Overview

With the gradual growth of network traffic, services are becoming more and more complex and diverse, and the complexity of technology is growing exponentially. These challenges make network operation and maintenance increasingly difficult, and maintenance staff have to face a huge amount of real-time and historical data generated by various devices. The existing network management systems and technical means do not have sufficient support for maintenance staff, resulting in many problems not being detected and solved in time, and faults continue to propagate and escalate until they affect customer experience.

Based on rich data generated in the network and the experience of experts , applying AI to packet/optical network is helpful to analyze the correlation between alarms, find out the relationship between network conditions and the root cause of faults. Therefore, AI provides a way to achieve intelligent network maintenance, which can locate the root alarm, find the root cause, and provide maintenance suggestions automatically. In this way, the efficiency of operation & maintenance can be improved.

2. Interaction with enhanced network operations

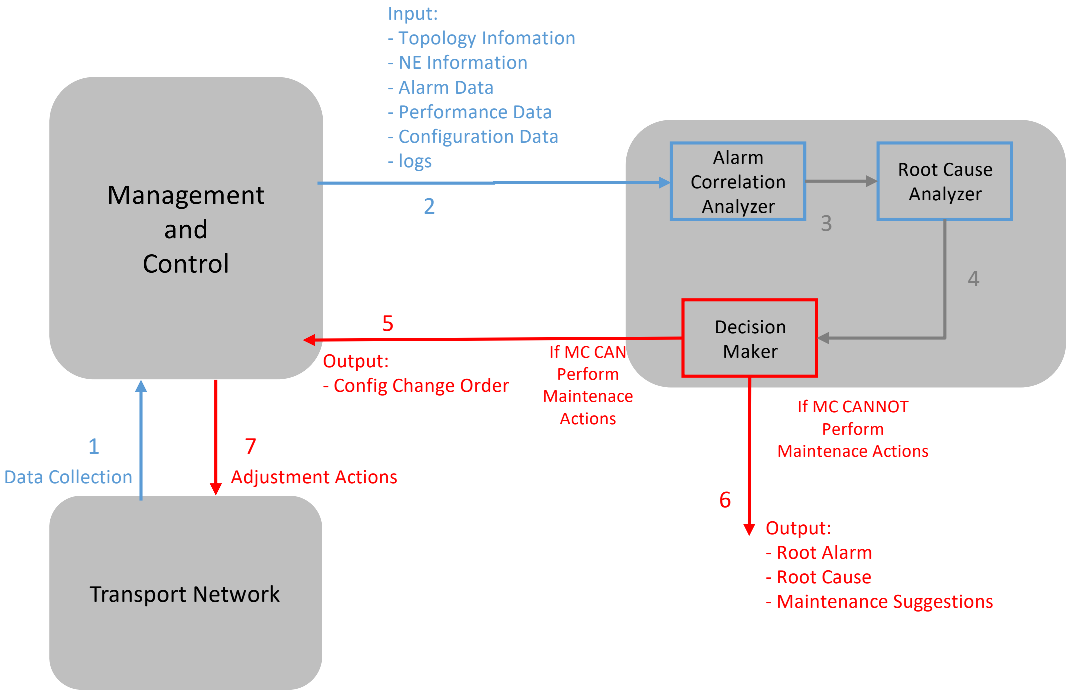

Figure 8 Interaction with Intelligent Maintenance of Packet/Optical Network

In step 1, Management & Control system collects necessary data from transport network by a collection method.

In step 2, Management & Control system provides some data (e.g., Topology Information, NE Information, Alarm Data, Performance Data, Configuration Data, and logs) as input of Alarm Correlation Analyzer.

In step 3, the result from Alarm Correlation Analyzer are input to the Root Cause Analyzer.

In step 4, Root Cause Analyzer provides analysis results for the Decision Maker, which will draw a conclusion of maintenance actions or maintenance suggestions according to the root cause of the fault. If the Management & Control system can perform the maintenance actions, then it goes to step 6. Otherwise, it goes to step 7.

In step 5, the Decision Maker outputs the Configuration Change Orders for the Management & Control system, which can take some adjustment actions to repair the fault as shown in step 5.

In step 6, the Decision Maker outputs maintenance suggestions for maintenance staff.

In step 7, the Management & Control system takes some adjustment actions to repair the fault.

3. Use Cases driven requirements

- Input data requirement

a) Require collect topology, NE information, alarms, performance, equipment states, configurations, and logs.

b) Require the time stamp of collected alarms should be at millisecond level.

c) Require alarms include the location information from which the network element, card, port information can be extracted.

d) Require network topology data include the connection information.

Data format as follows.

Table 5 Input of Alarm Correlation Analyzer

Data		Description
Topology ID		Topology represents link and subnetwork (switching) resources. These resources may be abstract or supported by software and hardware implementations. The topology identifier is unique in the context of some scope which could be global.
Alarm Data	Alarm ID	Indexed sequence number in time order.
	Alarm Level	The alarm severity assigned to the service affecting.
	Alarm Type	It identifies the active probable causes (failure) of the object.
	Alarm Name	The problem description for the entity.
	Alarm Code	It identifies the active probable causes (failure) of the object.
	Service Layer	The layer at which the network enables potential service forwarding.
	Flashing Alarm	It is used to indicate that whether the alarm is flashing.
	Network Element ID	The identifier of Network Element.
	Object ID	The identifier of the object.
	Card ID	The line card may plug into equipment. The line card identifier is unique in the context of some scope.
	Port ID	could be Null The port can perform the termination and adaptation functions of one or more transport layers. It supports all transport protocols including circuit and packet forms. The port identifier is unique in the context of some scope
	Start Time	At the time the alarm is reported.
	End Time	At the end of time the alarm is cleared.
	Repeat Times	The repeat occurrence of the alarm.
	Last Occurrence Time	The last activity date and time the alarm occurred.

Performance Data	Performance Type ID	the layer-specific Performance Data type.
	Network Element ID	The identifier of Network Element.
	Card ID	The line card may plug into equipment. The line card identifier is unique in the context of some scope.
	Port ID	The port can perform the termination and adaptation functions of one or more transport layers. It supports all transport protocols including circuit and packet forms. The port identifier is unique in the context of some scope.
	Performance Data Value	It contains the values of the PM parameters.
Configurations		It should include connection information
Logs		It is a record of events during a particular time period.

- Output data requirements

a) Require the output from Alarm Correlation Analyzer as the internal input of the Root Cause Analyzer.

b) Require the output from Root Cause Analyzer as the internal input of Decision Maker.

c) Require the decision result from Prediction and Decision as the only external presentation.

Table 6 Output of Alarm Correlation Analyzer

Data	**Description**
Root Alarm ID	The sequence number of root alarm.
Root Alarm Confidence	Statistics the probability that the root alarm falls within a specified range of value.
Root Alarm Level	The alarm severity of root alarm
Root Alarm Name	The problems description of root alarm.
Network Element ID	The identifier of Network Element.
Card ID	The line card may plug into equipment. The line card identifier is unique in the context of some scope.
Port ID	The port can perform the termination and adaptation functions of one or more transport layers. It supports all transport protocols including circuit and packet forms. The port identifier is unique in the context of some scope.
Last Occurrence Time	The last activity date and time the alarm occurred.

End Time	At the end of time the alarm is cleared.
Root Alarm State	0-Clear, 1-Not Clear
Derived Alarms	The alarms caused by root alarm.
Number of Alarms	The volume of alarms.
Number of Affected Connections	The amount connections affected by root alarm.

Table 7 Output of Root Cause Analyzer

Data	Description
Root Alarm ID	The identifier of root alarm.
Root Alarm Confidence	Statistics the probability that the root alarm falls within a specified range of value.
Root Alarm Level	The alarm severity of root alarm,
Root Alarm Name	The problems description of root alarm.
Network Element ID	The identifier of Network Element.
Card ID	The line card may plug into equipment. The line card identifier is unique in the context of some scope.
Port ID	The port identifier is unique in the context of some scope.
Last Occurrence Time	The last activity date and time the alarm occurred.
End Time	At the end of time the alarm is cleared.
Root Alarm State	0-Clear, 1-Not Clear
Derived Alarms	The alarms caused by root alarm.
Number of Alarms	The volume of alarms.
Number of Affected Connections	The amount connections affected by root alarm.
Root Cause	The cause of the root alarm.
Root Cause Confidence	Statistics the probability that the root alarm cause falls within a specified range of value.

Table 8 Output of Decision Maker

Data	Condition	Description
Configuration Change Orders	If MC CAN Perform Maintenance Actions	According to the configuration change orders, the MC can take some adjustment actions to repair the fault .
Root Alarm	If MC CANNOT Perform Maintenance Actions	The root alarm may cause many derived alarms.
Root Cause		The cause of the root alarm.
Maintenance Suggestions		Since the MC is unable to perform maintenance actions to correct the root alarm, it can give some maintenance suggestions to maintenance staff.

- Interface and function requirements：

a) Get topology information.

b) Get NE information.

c) Get alarm data.

d) Get performance data.

e) Get configuration data.

f) Get logs.

MC system can get performance data from transport network through streaming or traditional performance collecting.

8.3. Use Case #3: Intelligent OSNR Prediction

1. Overview

It is difficult to predict OSNR in traditional optical network. If an optical cable line is changed, it can be hard to detect the variation of OSNR and determine whether the changed OSNR will meet the network’s requirements. Long time aging of fibre cable and components bring unpredicable OSNR. Traditional network operations do not provide a predictive capability for OSNR to maintenance staff.

When introducing AI to optical network, the OSNR can be predicable. It helps to find the potential risks, reduce network alarms and improve the maintenance efficiency.

Based on history performance and configuration parameters, introducing intelligent OSNR prediction will help to reduce potential alarms and less failures. Prediction and decision-making can eliminate network risk and evaluate the feasibility of network capacity expansion .

2. Interaction with enhanced network operations

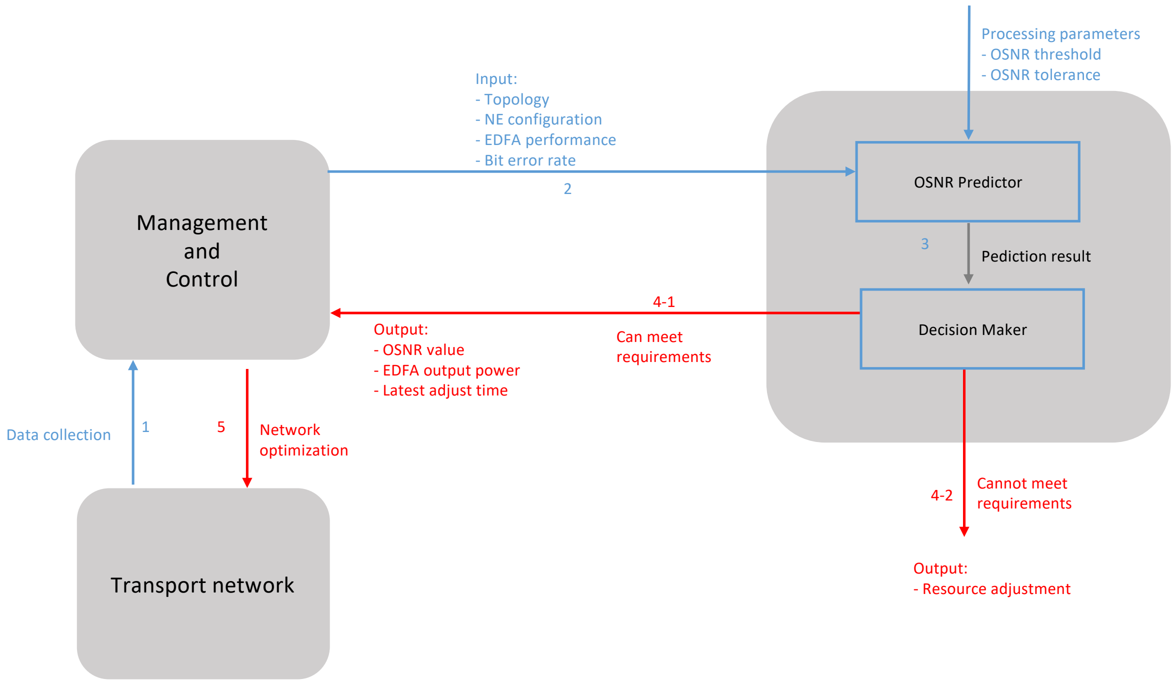

Figure 9 Interaction with Intelligent OSNR Prediction

In step 1, the Management & Control system gets performance data from optical transport network by a collection method such as Telemetry.

In step 2, the Management & Control system provides some data (e.g. Topology Information, NE configuration, EDFA performance) as input of the Network OSNR Predictor. At the same time, processing parameters are input into the Network OSNR Predictor (e.g. OSNR threshold, OSNR tolerance).

In step 3, the Network OSNR Predictor provides prediction results for the Decision Maker. Based on the VOA of EDFA, It will draw a conclusion of optical power adjustment and resource re-schedule requirements (e.g. replace cable, replace amplifier, introduce new repeater). If the transport network can meet the adjustment need, then it goes to step 4-1. Otherwise, it goes to step 4-2.

In step 4-1, the Decision Maker outputs the adjustment OSNR value and the latest action time for the Management & Control system, which can take some adjustment actions to optimize the Transport Network as shown in step 5.

In step 4-2, the Decision Maker outputs additional resource applications in order to get expansions for the Transport Network.

In step 5, the Management & Control system takes some adjustment actions to optimize the Transport Network.

3. Use Case driven requirements

- Input data requirements:

a) Requirements of collecting topology, NE configuration and performance.

b) Requires the time granularity of collected performance should be at 15 minutes and 24 hours granularity.

c) Requires Data Storage Cycle (24 months).

Table 9 Input of OSNR Predictor

Data	Description
Topology ID	Topology represents link and subnetwork (switching) resources. These resources may be abstract or supported by software and hardware implementations. The topology identifier is unique in the context of some scope which could be global.
Port ID	The port can perform the termination and adaptation functions of one or more transport layers. It supports all transport protocols including circuit and packet forms. The port identifier is unique in the context of some scope.
Line Card ID	The line card may plug into equipment. The line card identifier is unique in the context of some scope.
Network Element ID	The identifier of Network Element.
EDFA parameters	Gain
	Gain range
	noise factor
	Saturated output optical power
	input optical power
	output optical power
Performance	bit error rate

- Processing requirements

a) Providing OSNR tolerance with FEC characteristics.

b) Providing OSRN tolerance with guaranteed bit error rate.

- Output data requirements

a) Requires the output from OSNR Predictor as the internal input of OSNR Predictor.

Table 10 Output of OSNR Predictor

Data	Description
Time stamp	At the end of the measurement interval, the timestamp is reported.
Predicted OSNR	dB

Table 11 Output of Decision Maker

Data	Condition	Description
Target OSNR		
Target output power of EDFA	To meet the requirement of OSRN, the output power of EDFA can be adjusted	The target value of EDFA output power.
The latest adjust time	the transport network CAN meet the need of target bit error rate	the duration after each adjustment action to the transport network, e.g., 1 day, 1 month, 1 year, permanent
Resource Application	the transport network CANNOT meet optimization needs	additional resource application

- Interface and function requirements

a) Get topology information.

b) Get NE information.

c) Get alarm data.

d) Get performance data.

e) Get configuration data.

8.4. Use Case #4: Intelligent Deployment & Optimization of Packet/optical Network

1. Overview

For complex optical network topologies, such as mesh networks and ring networks, various services have different requirements for transmission links. The customer's Ethernet service configuration needs to be planned over the best match of service route according to the SLA level and QoS requirements of the service to complete the deployment of service configuration parameters. The traditional service configuration method requires manual route planning (or planning a single cost) and manual deployment of service parameters, which has low efficiency and cannot meet the requirements of rapid service response. With the introduction of AI functions, it is expected that the service deployment can automatically select the route based on the network state, implement intelligent service parameters configuration, and achieve the intelligent goal of end-to-end service intelligent configuration.

2. Interaction with enhanced network operations

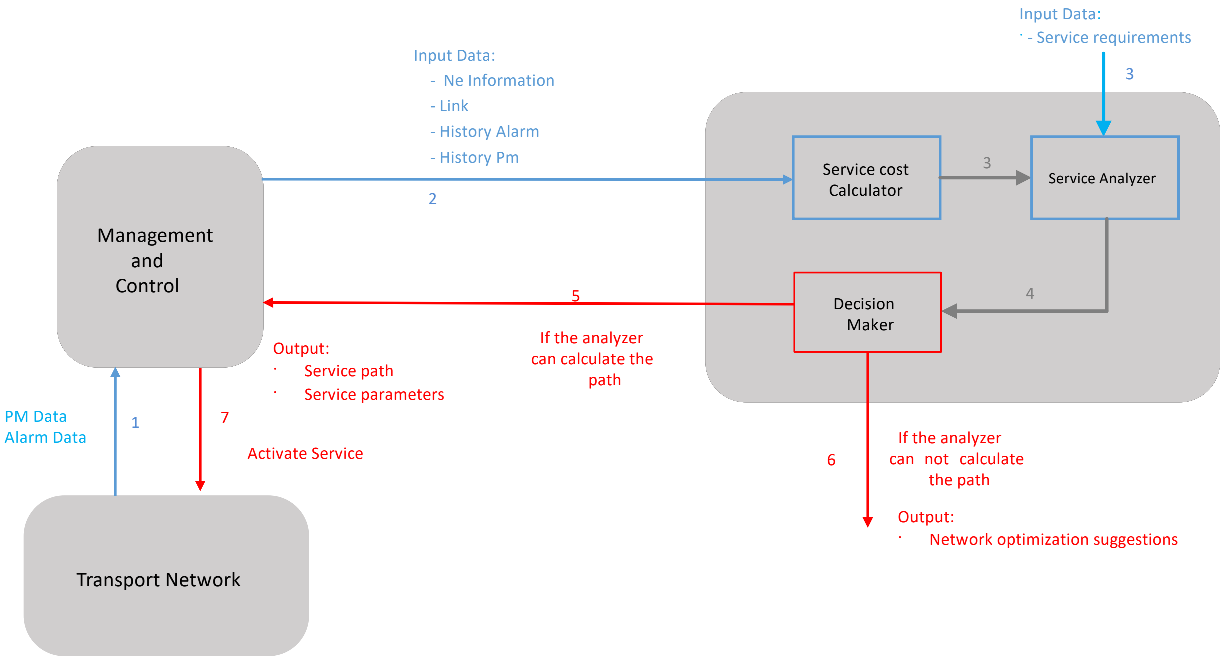

Figure 10 Interaction with Intelligent Deployment & Optimization of Packet/optical Network

In step 1, the Management and Control system gets performance data and alarm data from optical transport network by a collection method such as Telemetry.

In step 2, The Service cost calculator collects the network element information, link information, historical traffic performance and historical alarm information from Management and Control system(s).

In step 3, The Service cost calculator analyzes the cost values of each link in the network according to the collected data, and calculates the cost of each link, including bandwidth utilization, link delay, link unavailable time, link packet loss rate, etc., and then marks the cost value of each link according to the calculation results. At the same time, input the service requirements information to the Service analyzer.

In step 4, The service analyzer automatically or manually selects a routing strategy according to the service requirements and the link cost values output from the Service cost calculator. This strategy can be one of the best cost, the shortest path, the lowest link unavailable time, the least packet loss, the least delay and the lowest bandwidth utilization, or any combination of various methods. For example, the service is a voice service with the highest delay requirements, Then the most appropriate service path can be calculated based on the combination of minimum delay and cost optimal routing mode, and enter step 5; If the path cannot meet the service requirements, proceed to step 6

In step 5, Output the calculated service path to meet the SLA requirements to the Management Control system.

In step 6, the decision maker output network optimization suggestion.

In step 7, Management & Control system active optimized service with configuration parameter.

3. Use Case driven requirements

- Input data requirements:

a) Requirements of collecting NE configuration, link, history performance and history alarm.

b) Requires the time granularity of collected performance should be at 15 minutes and 24 hours granularity.

c) Requires Data Storage of history alarm Cycle (12 months), Data Storage of history performance Cycle (1 month).

d) Service requirements with service type, SLA parameter

Table 12 Input of Service Cost Calculator

Data		**Description**
Network Element ID		The identifier of Network Element.
Link		The Link shows adjacency between two or more ports.
Port rate		The port carries that rate of information transfer.
Alarm	Alarm name	The problems description for the entity.
	Alarm Raised Time	At the time the alarm is reported.
	Alarm Cleared Time	At the end of time the alarm is cleared.
	Alarm Source	The identifier of the object.
	Alarm duration	The duration of the active alarm.
Performance	RX_BYTES(average)	per port/time cycle Average bytes received per port during measurement duration.
	TX_BYTES(average)	per port/time cycle Average bytes transmitted per port during measurement duration.
	RX_BYTES (peak)	per port/time cycle Maximum bytes received per port during measurement duration.
	TX_BYTES(peak)	per port/time cycle Maximum bytes received per port during measurement duration.
	Package Loss rate	The ratio of the number of data packets lost in the test to the number of data packages sent.
	Bit Error rate	The number of bit errors is the number of bits changed by the received channel data stream due to noise, interference, loss or

		bit synchronization errors. Bit error rate (BER) is the number of error bits divided by the total number of transmitted bits in a period of time.
	Latency	The time it takes for a specific package of data to rotate around to the read/write head.
Service requirements	Source NE	The A-end NE of the service.
	Sink NE	The Z-end NE of the service.
	Service type	The service type indicates how the service is used by the customer.
	SLA	A service level agreement (SLA) is a documented agreement between a service provider and a customer that identifies both the services required and the expected level of service. The agreement varies between vendors, services, and industries.

- Processing requirements

a) Based on the port traffic performance, calculating the average traffic and peak traffic in one month.

b) Based on the port history alarm, calculating the length of link unavailability within 12 months.

- Output data requirements

a) Output the cost value of each link.

b) Output the Packet loss rate of each link.

c) Output the unavailable time of each link.

d) Output the bandwidth utilization of each link.

e) Output the Latency of each link.

Table 13 Output of Service cost calculator

Data	**Description**
Network Element ID	The identifier of Network Element.
Link port	The port identifier of the link.
Service cost	Cost relates to some aspect of the service.
Package Loss rate	Marked value of Package Loss rate
Bit Error rate	Marked value of Bit Error rate

Latency	Marked value of Latency
Bandwidth utilization	Marked value of Bandwidth utilization
Unavailable Time	Marked value of Unavailable Time

Table 14 Output of Service Analyzer

Data	**Description**
Network Element ID	The identifier of Network Element.
Link port	The port identifier of the link.
PIR	Peak Information Rate
CIR	Committed Information Rate

- Interface and function requirements

  a) Get NE information.

  b) Get alarm data

  c) Get performance data

  d) Calculate the service routing information according to the service type, SLA level and other service requirements.

8.5. Use Case #5: Fibre Cable Pre-warning and Fault Localization

1. Overview

Because of the passive aspect of fibre cable, it is difficult to manage fibre cable with traditional maintenance approach of optical transport network. The traditional approach cannot monitor and pre-warn of the condition of fibre cable and facilities such as handholes, aerial fibre cable, splitters, fibre distribution cabinets. It is difficult to localize the faults when failures of fibre cable cause service alarms.

When introducing an AI approach for real-time monitoring alarm and performance of fibre cable, it can analyze the huge volume of fibre cable to implement fibre cable pre-warning and intelligent fault localization.

2. Interaction with enhanced network operations

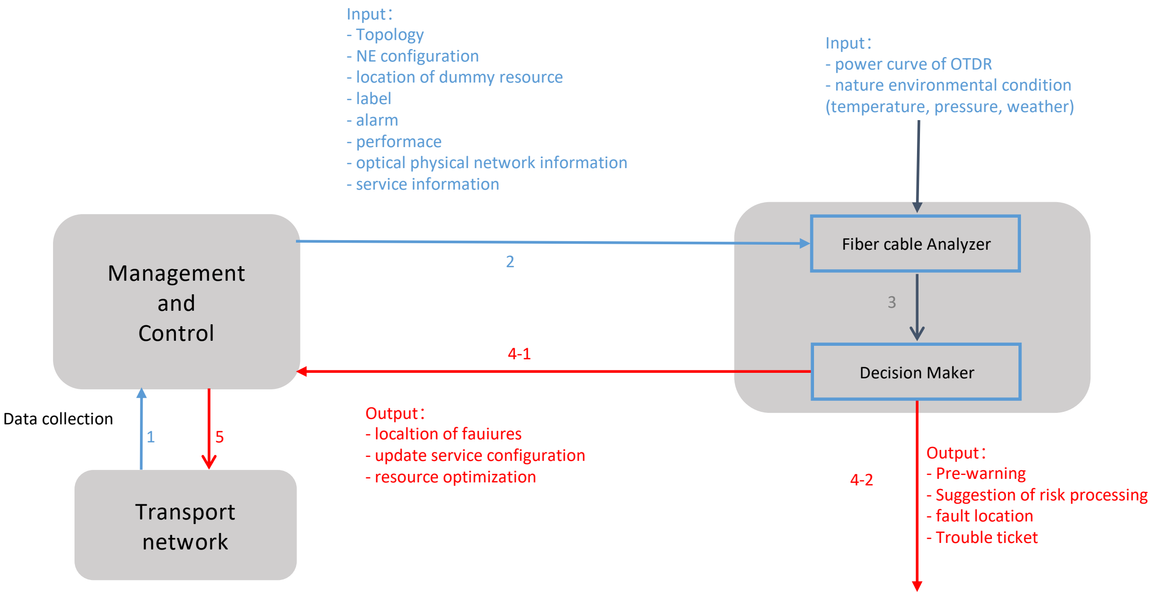

Figure 11 Interaction with fibre cable pre-warning and fault localization

In step 1: the Management & Control system gets alarm and PM data from transport network by a collection method such as Telemetry.

In step 2: the Management & Control system provides some data (e.g. topology information, NE configuration, alarm and performance Data) as input of fibre cable analyzer.

In step 3: the Fibre cable analyzer collects power curve of OTDR and some nature environmental condition (e.g. temperature, pressure, weather and camera image) to judge network risk of whether to trigger pre-warning or fault localization. If there is fibre cable cut-down, it finds the fault location and goes to step 4-1. Otherwise it goes to step 4-2.

In step 4-1, the Decision Maker outputs the fault localization information, service update requirements and resource optimization requirements to Management & Control system. The service update requirements should avoid the position of cable fault.

In step 4-2, the Decision Maker outputs the network risk information, the fault location, suggested solution, trouble ticket and additional resource applications.

In step 5: the Management & Control system takes some adjustment actions to optimize and update the optical network service.

3. Use Case driven requirements

- Input data requirements

a) Requires collection of network topology, optical physical network topology, NE configuration, fibre types and service information.

b) Requires collection of current alarms, history alarms.

c) Requires collection of optical power.

Table 15 Input of fibre cable analyzer

Data		Description
network topology	Topology ID	Topology represents link and subnetwork (switching) resources. These resources may be abstract or supported by software and hardware implementations. The topology identifier is unique in the context of some scope which could be global.
NE configuration	Location	Location represents where the equipment is. It could be geographical location.
	Port ID	The port can perform the termination and adaptation functions of one or more transport layers. It supports all transport protocols including circuit and packet forms. The port identifier is unique in the context of some scope.
	NE ID	The identifier of Network Element.
service information	Service ID	The identifier of service.
alarms	current alarms	The alarm state is cleared active.
	history alarms	The alarm state is cleared.
Optical power		
optical physical network topology	handhole ID	The identifier of handhole.
	Subduct ID	The identifier of subduct.
	Aerial fibre cable / road pole ID	The identifier of aerial fibre cable / road pole.
	Station ID	The identifier of station.
	ODF ID	The identifier of ODF.
	Fibre distribution cabinet ID	The identifier of fibre distribution cabinet.
	FDP ID	The identifier of fiber distribution point.
	Cabinet ID	The identifier of cabinet.
	Fibre type	G.652, G.653, G.654E
	Cable length	The cable length between two adjacent optical cable splice closure.
power curve of OTDR		
nature environmental condition		temperature, pressure, weather and camera image

- Processing requirements

a) Requiring risk prediction model based on the power curve of OTDR, NE configuration, location of fibre cable, nature environmental condition.

b) Requiring fault localization based on NE configuration, topology, alarms, performance, and fibre cable information.

c) Requiring on-line detection and off-line detection.

d) Data collection period: 1s, 30s, 1min, 15min, 30min, 24h. Data storage period: 1 month, 3 months, 6 months, 1 year, 2 years.

- Output data requirements

a) Pre-warning information: Resource management for cable, tunnel/hole, road poles, cabinets, location of risk.

b) Suggestion of risk processing: Suggestion of optimizing service based on cable fault location.

c) fault location information: Optical physical network resource information for cable, tunnel/hole, road poles, cabinets.

d) Trouble ticket: Decision Maker can send Trouble ticket information for maintenance staff.

e) Updating service configuration: To avoid the location of fibre cable, new path can be re-scheduled.

Table 16 Output of fibre cable Analyzer

Data		Description
Pre-warning information	Vibration curve	
	Optical Fibre loss	
	Location of risk	Location represents where the risk is. It could be geographical location.
	Nature environmental condition	The nature environmental condition includes weather, temperature.
Fault location	Location of fault	Location represents where the fault is. It could be geographical location.
	Damaged service	Service ID of the damaged service.
	Scope of damaged resource	Handholes, Aerial fibre cable, cables
	Alarm	Alarms occurred on the Fault location.

Table 17 Output of Decision maker

Data		Description
Update service configuration	re-scheduled service	
Suggestion of risk processing		
Trouble ticket		

- Interface and function requirements

a) Get topology information.

b) Get NE information.

c) Get alarm data.

d) Get performance data.

e) Get configuration data.

f) Get power curve of OTDR.

g) Nature environmental condition.

8.6. Use Case #6: intelligent detection and optimization for physical co-route cable

1. Overview

During daily maintenance of the optical network, working fiber and protection fiber may be carried over a single cable. If the single cable fails, the working path and protection path fail at the same time. Without an intelligent approach to detect co-routing of working and protection paths over a common cable, more labor is needed to eliminate the cable failure.

Co-route service could be OMSP working service/protection service, and SNCP working service/protection service. Outbound optical fibers at the same site should be optimized to avoid different direction fibers being carried over single cable.

Introducing AI approach to detect and optimize physical co-route of cable helps to predict and optimize physical optical route to reduce maintenance cost and network service risk.

When the physical optical cable deployment is unknown (for example, the physical network belongs to the third party, or the physical deployment changes), this use case can be used to solve the physical co-route cable problem.

Under some circumstance, wrong judgement of the physical co-route cable may be possible. Some enhanced AI algorithm and more data collection can help to improve the analysis results of correlation and clustering.

2. Interaction with enhanced network operations

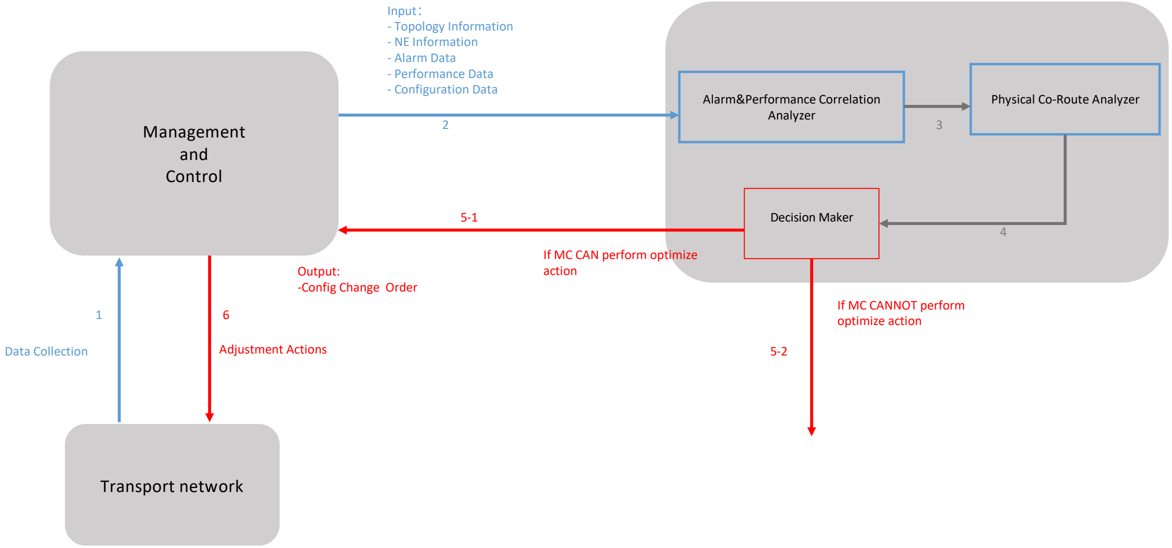

Figure 12 Interaction with intelligent detection and optimization for physical co-route cable

In step 1, the Management & Control system gets necessary data from the transport network by a collection method such as Telemetry.

In step 2, the Management & Control system provides some data (e.g., Topology Information, NE Information, Alarm Data, Performance Data, Configuration Data, and service Data) as input of the Alarm & Performance Correlation Analyzer.

In step 3， the cluster result from the Alarm & Performance Correlation Analyzer are input to the Root Cause Analyzer.

In step 4, combined with topology and service data, the Physical Co-route Analyzer provides analysis results for Decision Maker. If there are different physical route available, then it goes to step 5-1 to deploy optimization and avoid co-route. Otherwise, it goes to Step 5-2.

In step 5-1， the Decision Maker outputs the Configuration Change Orders for Management & Control system, which can adjustment service to avoid physical co-route cable.

In step 5-2, the Decision Maker outputs information of physical co-route cable and maintenance priority suggestions for maintenance staff.

In step 6, the Management & Control system takes some adjustment actions.

3. Use Case driven requirements

- Input data requirements

a) Requires collect topology, NE information and service information.

b) Requires history alarms of optical port.

c) Requires history performance of optical port.

d) Requires storing the collected alarm data and performance data for a sufficiently long duration up to 24 months.

Table 18 Input of Alarm & Performance Correlation Analyzer

Data	**Description**
Topology ID	Topology represents link and subnetwork (switching) resources. These resources may be abstract or supported by software and hardware implementations. The topology identifier is unique in the context of some scope which could be global.
NE ID	The identifier of Network Element.
Optical port ID	The port can perform the termination and adaptation functions of one or more transport layers. It supports all transport protocols including circuit and packet forms. The port identifier is unique in the context of some scope.
LINK ID	The identifier of link.
Service information	The links supporting the service.
Service SLA	/
Time Index	At the end of the measurement interval, the timestamp is reported.
History alarm	
History performance	
Optical power	
Bit error rate	
Power loss curve of optical path	

- Processing requirements

a) Requires physical co-route model based on alarm and variation of optical power.

b) Requires physical co-route analysis based on alarm, optical power, bit error rate and variation of Power loss curve of optical path.

c) Granularity: Data Collection Cycle (1s, 30s, 1min, 15min, 24h) Data Storage Cycle (1 month, 3 months, 6 months, 1 year, 3 years, 5 years).

- Output data requirements

a) Requires to figure out sections of physical co-route cable. Combined with affected service quantity and service SLA, it requires to give maintenance suggestion with priority.

b) Requires to adjust service path to avoid physical co-route cable.

Table 19 Output of Physical Co-route Analyzer

Data	**Description**
Physical co-route section	
Information of affected service	Service ID, service supported by NEs, ports, physical co-route section

Table 20 Output of Decision maker

Data	**Description**
Adjusted service configuration	Re-scheduled route can avoid the physical co-route cable.
Optimization suggestion of physical co-route cable	

- Interface and function requirements

a) Get topology information.

b) Get NE information.

c) Get alarm data.

d) Get performance data.

e) Get configuration data.

9. References

[1] Recommendation ITU-T G.7701 (2022), “Common control aspects”

[2] Recommendation ITU-T G.7702 (2022), “Architecture for SDN control of transport networks”

[3] Recommendation ITU-T G.7703 (2021), “Architecture of the automatically switched optical network”

[4] Recommendation ITU-T G.7711 (2022), “Generic protocol-neutral information model for transport resources”

[5] ONF TR-512, “Core Information Model (CoreModel)” v1.5 September 2021

[6] ONF TR-547, “TAPI v2.1.3 Reference Implementation Agreement” v1.0 July 2020

[7] OIF carrier network SDN requirements : http://www.oiforum.com/wp content/uploads/OIF_Carrier_WG_Requirements_on_Transport_Networks_in_SDN_Architectures_Sept 2013.pdf