ETSI GR F5G 007 V1.1.1 (2023-01)

Fifth Generation Fixed Network (F5G); F5G Industrial PON

Disclaimer

The present document has been produced and approved by the Fifth Generation Fixed Network (F5G) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGR/F5G-007 Industrial PON

Keywords

F5G, industrial, PON

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Fifth Generation Fixed Network (F5G).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document studies the application of PON systems for industrial networks, including various deployment scenarios, industrial PON system descriptions, key functions, performance recommendations, interfaces, management system, ONU with industrial interfaces and industrial environment adaptation recommendations.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR F5G 001: "Fifth Generation Fixed Network (F5G); F5G Generation Definition Release #1".

[i.2] ETSI GR F5G 008: "Fifth Generation Fixed Network (F5G); F5G Use Cases Release #2".

[i.3] ETSI GS F5G 003: "Fifth Generation Fixed Network (F5G); F5G Technology Landscape".

[i.4] ETSI GS F5G 004: "Fifth Generation Fixed Network (F5G); F5G Network Architecture".

[i.5] Recommendation ITU-T G.984.1 (2008): "Gigabit-capable passive optical networks (GPON): General characteristics".

[i.6] Recommendation ITU-T G.987 (2012): "10-Gigabit-capable passive optical network (XG-PON) systems: Definitions, abbreviations, and acronyms".

[i.7] Recommendation ITU-T G.987.1 (2016): "10-Gigabit-capable passive optical networks (XG--PON): General requirements".

[i.8] Recommendation ITU-T G. Sup74 (2021): "Network slicing in a passive optical network context".

[i.9] Recommendation E.419 (2006): "Business oriented Key Performance Indicators for management of networks and services".

[i.10] IEC 60529: "Degrees of protection provided by enclosures (IP Code)".

[i.11] ETSI EN 300 019-1-4: "Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 1-4: Classification of environmental conditions; Stationary use at non-weatherprotected locations".

[i.12] ETSI EN 300 019-2-4: "Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 2-4: Specification of environmental tests; Stationary use at non-weatherprotected locations".

[i.13] IEC 61000-4-2:2008: "Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test".

[i.14] CCSA (China Communications Standards Association) 2018-0172T-YD: "Networking Technology for Industrial Internet-General Technical Requirements for Passive Optical Network (PON)".

[i.15] IEEE 802.3ae™-2002: "IEEE Standard for Information technology - Local and metropolitan area networks - Part 3: CSMA/CD Access Method and Physical Layer Specifications - Media Access Control (MAC) Parameters, Physical Layer, and Management Parameters for 10 Gb/s Operation".

[i.16] IEEE 802.3af™-2003: "IEEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Data Terminal Equipment (DTE) Power Via Media Dependent Interface (MDI)".

[i.17] IEEE 802.3at™-2009: "IEEE Standard for Information technology - Local and metropolitan area networks - Specific requirements - Part 3: CSMA/CD Access Method and Physical Layer Specifications Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements".

[i.18] IEEE 802.3bt™-2018: "IEEE Standard for Ethernet Amendment 2: Physical Layer and Management Parameters for Power over Ethernet over 4 pairs".

[i.19] IEEE 802.3bz™-2016: "IEEE Standard for Ethernet Amendment 7: Media Access Control Parameters, Physical Layers, and Management Parameters for 2.5 Gb/s and 5 Gb/s Operation, Types 2.5GBASE-T and 5GBASE-T".

[i.20] IEEE 802.3i™-1990: "IEEE Standard for Local and Metropolitan Area Networks - System Considerations for Multi-segment 10 Mb/S Baseband Networks (Section 13) and Twisted-Pair Medium Attachment Unit (MAU) and Baseband Medium, Type 10BASE-T (Section 14)".

[i.21] IEEE 802.3u™-1995: "IEEE Standards for Local and Metropolitan Area Networks: Supplement - Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units, and Repeater for 100Mb/s Operation, Type 100BASE-T (Clauses 21-30)".

[i.22] IEEE 802.11™-2020: "IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.23] IEEE 802.11a™-1999: "IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band".

[i.24] IEEE 802.11b™-1999: "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band".

[i.25] IEEE 802.11n™-2009: "IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput".

[i.26] IEEE 802.11ac™-2013: "IEEE Standard for Information technology - Telecommunications and information exchange between systems-Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz".

[i.27] IEEE 802.11ax™-2021: "IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN".

[i.28] NIST SP 800-57 Part 1 Rev. 5: "Recommendation for Key Management: Part 1 - General".

[i.29] IEC 61158: "Industrial communication networks - Fieldbus specifications".

[i.30] Recommendation ITU-T G.987.3 (2014): "10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) layer specification".

[i.31] Recommendation ITU-T G.9804.1 (2019): "Higher speed passive optical networks - Requirements".

[i.32] Recommendation ITU-T G.9804.2 (2021): "Higher speed passive optical networks - Common transmission convergence layer specification".

[i.33] Recommendation ITU-T G.9804.3 (2021): "50-Gigabit-capable passive optical networks (50G-PON): Physical media dependent (PMD) layer specification".

[i.34] IEEE 802.1Qbv™-2015: "IEEE Standard for Local and metropolitan area networks -- Bridges and Bridged Networks - Amendment 25: Enhancements for Scheduled Traffic".

[i.35] IEEE 802.1Qch™-2017: "IEEE Standard for Local and metropolitan area networks--Bridges and Bridged Networks--Amendment 29: Cyclic Queuing and Forwarding".

[i.36] IEEE 802.11g™-2003:"IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band".

[i.37] IEEE 802.1Qbu™-2016: "IEEE Standard for Local and metropolitan area networks -- Bridges and Bridged Networks -- Amendment 26: Frame Preemption".

[i.38] IEEE 802.3br™-2016: "IEEE Standard for Ethernet Amendment 5: Specification and Management Parameters for Interspersing Express Traffic".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

industrial environment adaptation: capability of maintaining acceptable level of service within industrial environments

industrial protocol adaptation: capability to interpret and/or convert a range of industrial communication protocols

network resilience: capability of a network to protect against and maintain an acceptable level of service in the presence of network failure(s)

PON slice: group of one or more flows associated with one or more ONUs that are treated as a single entity by a hierarchical traffic scheduler

NOTE: Defined in ITU-T G. Sup74 (2021) [i.8], clause 3.2.3.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

10GE	10 Gbit/s Ethernet
10G-EPON	10 Gbit/s Ethernet PON
AES	Advanced Encryption Standard

AGV	Automated Guided Vehicles
AI	Artificial Intelligence
AN	Access Network
AP	Access Point
API	Application Programming Interface
AR	Augmented Reality
ASIC	Application Specific Integrated Circuit
BASE-T	Baseband Twisted pair cable
BE	Best Effort
BNG	Border Network Gateway
CAN	Controller Area Network
CCD	Charge Coupled Device
CMOS	Complementary Metal Oxide Semiconductor
CO	Cooperative
CPN	Customer Premise Network
CPU	Central Processing Unit
CQF	Cyclic Queing and Forwarding
CX	short-haul Copper
DBA	Dynamic Bandwidth Allocation
DC	Data Centre
DevOp	Development and Operation
DHCP	Dynamic Host Configuration Protocol
DI/DO	Digital Input/Digital Output
DSP	Digital Signal Processing
DU	Distributed Unit
E2E	End to End
EC	Edge Computing
EMC	ElectroMagnetic Compatibility
EMI	Electro-Magnetic Interference
EMS	Electro-Magnetic Susceptibility
EPON	Ethernet PON
ER	Extended Range
ERP	Enterprise Resource Planning
ETH	Ethernet
F5G	Fifth Generation Fixed Network
FE	Fast Ethernet
FEC	Forward Error Correction
FOCAS	Flight Operations, Compliance and Safety
FPGA	Field Programmable Gate Array
FTTx	Fiber To The x
FTTX	Fibre To The X
GE	Gigabit Ethernet
GPON	Gigabit PON
GPU	Graphical Processing Unit
GTC	Gigabit-capable passive optical network Transmission Convergence
HD	High Definition
HMEE	Hardware-Mediated Execution Enclave
HSP	Higher Speed PON
HTTP	HyperText Transfer Protocol
IaaS	Infrastructure as a Service
ID	Identification
IEEE	Institute of Electrical and Electronic Engineers
IIoT	Industrial IoT
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
LAG	Link Aggregation
LLS-FH	Low-Layer Split mobile Fronthaul
LOSi	Loss Of Signal for ONUi
LR	Long Range
LRM	Long Reach Multimode
LX	Long-haul fibre

M&C	Management & Control
MAC	Media Access Control
MCA	Management, Control & Analytics
MES	Manufacturing Execution System
MITM	Man-In-The-Middle
MQ	Message Queue
MQTT	Message Queue Telemetry Transport
MS	Management System
NAND	Not-And
NBI	Northbound Interface
NMS	Network Management System
O&M	Operation & Management
OAM	Operation Administration and Maintenance
ODN	Optical Distribution Network
OLT	Optical Line Termination
OMCI	ONU Management and Control Interface
ONU	Optical Network Unit
ONUi	Optical Network Unit No. i
OPC UA	Object linking and embedding for Process Control - Unified Architecture
OPC-UA	Open Platform Communications Unified Architecture
OS	Operating System
OT	Operational Technology
P2MP	Point to Multipoint
PaaS	Platform as a Service
PC	Personal Computer
PLC	Programmable Logic Controller
PMD	Physical Media Dependent
PoE	Power over Ethernet
PON	Passive Optical Network
POTS	Plain Old Telephone Service
QBV	802.1Qbv
QoS	Quality of Service
RFID	Radio Frequency Identification
RS	Recommended Standards
RTOS	Real-Time Operating System
RTT	Round-trip Time
SAP	Service Access Point
SCADA	Supervisory Control And Data Acquisition
SDi	Signal Degraded of ONUi
SDN	Software-Defined Network
SFi	Signal Fail of ONUi
SN	Serial Number
SPP	Service Processing Point
SR	Short Range
SR-DBA	Status Reporting DBA
SSD	Solid-State Drive
SX	Short-haul fibre
TC	Transmission Convergence
T-CONT	Transmission Container
TDM	Time-Division-Multiplex
TDMA	Time-Division-Multiple Access
TF	Transmitter Failure
TL1	Transaction Language 1
TM	Traffic Management
TSN	Time Sensitive Network
TTE	Time Triggered Ethernet
UART	Universal Asynchronous Receiver-Transmitter
UE	User Equipment
UNI	User Network Interface
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VM	Virtual Machine

VR	Virtual Reality
Wi-Fi®	Wireless Fidelity
XG	10 Gbps
XG-PON	10-Gigabit-capable Passive Optical Network
XGS	10 Gbps Symetrical
XGS-PON	10-Gigabit-capable Symmetric Passive Optical Network
XML	eXtensible Markup Language
YANG	Yet Another Next Generation
ZTP	Zero Touching Provisioning

4 Overview

Industrial networks are designed to connect and control devices, systems, machines, and other assets within the industrial environment. With digital transformation, remote control machinery and sensors are deployed to automate the process of production, monitoring, and management. Industrial networks are extended to include facilities related to the business, such as R&D centres, warehouses, administrative offices, and customer service branches.

Industrial PON, inherited a mature PON technology from residential access network (see [i.5], [i.6] and [i.7]), and enhances it to include functions required by the industrial customers. Industrial PON needs to support high quality connectivity to communicate between sensors, devices machines, and people within the industrial parks, see ETSI GR F5G 001 [i.1] and ETSI GS F5G 003 [i.3].

In the present document, typical industrial PON deployment scenarios, the architecture, the key functions and interfaces of the industrial PON system are described. These include the management system; the ONUs used in industrial scenarios and addresses industrial environmental recommendations.

5 Typical scenarios

5.1 Overview

There are three typical main deployment scenarios for industrial PON, which are illustrated as a complete overview in Figure 1. These scenarios have been included in F5G use cases (see ETSI GR F5G 008 [i.2]), and there follows a brief overview of these scenarios.

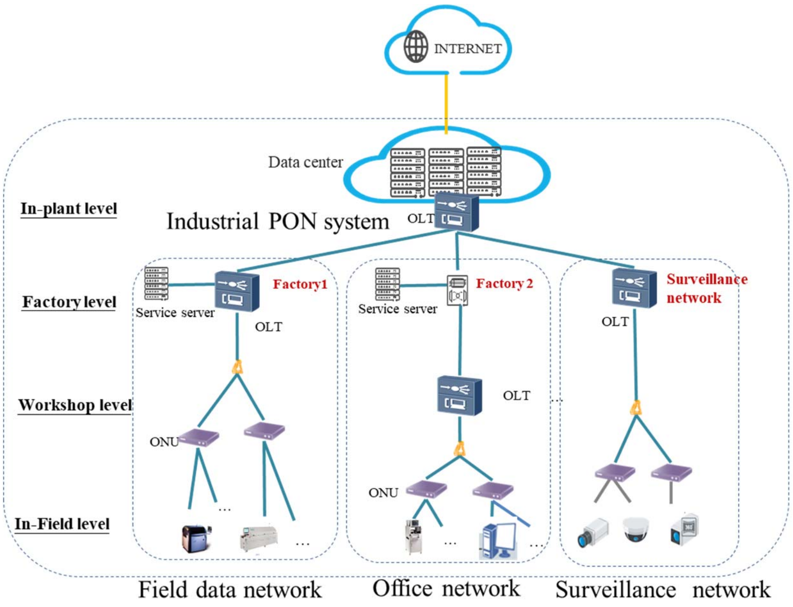


Figure 1: Overview of the industrial PON with typical connectivity scenarios within the factory

The industrial PON system is comprised of three main area (see ETSI GR F5G 008 [i.2]):

1) The field data network which is primarily the industrial environment, described in clause 5.2.

2) The office network including sales, marketing, finance and managerial staff areas, described in clause 5.3.

3) The surveillance network including internal and external video surveillance, alarms sensors and machine monitoring, described in clause 5.4.

5.2 Field Data Network

One major application in industrial PON is the transport of factory intra-plant industrial field level services. Industrial PON serves as a connection and convergence network for the machines within the factory, because the field data from the product line process is carried by the industrial PON.

There are several industrial field level interfaces and protocols defined in the IEC 61158 series [i.29]. Therefore, the industrial PON ONUs need to support the corresponding physical interfaces and the built-in protocol-related functions, or provide connectivity to existing industrial gateways, to support the communications among PLCs, other gateways, production management systems, etc.

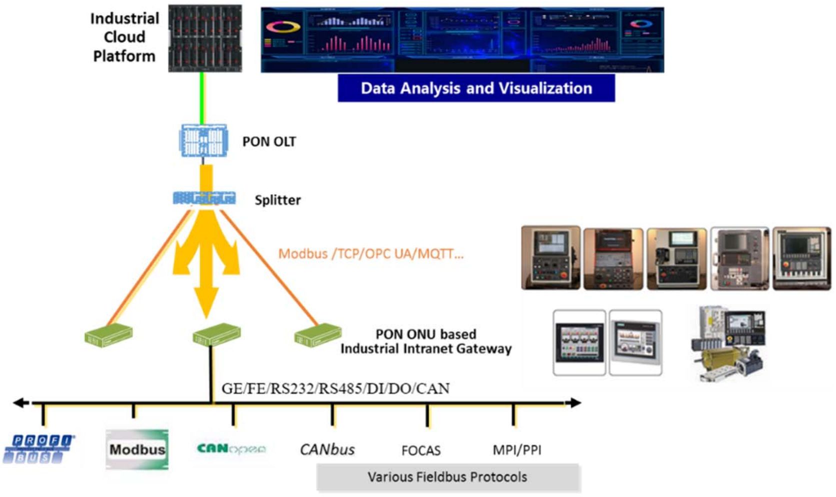

Industrial Cloud Platform
Data Analysis and Visualization
PON OLT
Splitter
Modbus /TCP/OPC UA/MQTT...
PON ONU based Industrial Intranet Gateway
GE/FE/RS232/RS485/DI/DO/CAN
PROFI BUS
Modbus
CANopen
CANbus
FOCAS
MPI/PPI
Various Fieldbus Protocols

Figure 2: Fieldbus connection and converge network overview

5.3 Office network

The Industrial network supports the transport of traffic from the office area of a factory as internet/intranet surfing, telephony and Wi-Fi® APs traffic, etc. As the PON system is one of the dominant solutions for the fixed network in the public access network, it is an ideal candidate to transport these office network services in the factory.

By replacing existing copper-wire based network with fibre, higher access bandwidth can be available, and a single fibre can transport all the network services within the office. In addition, by using an industrial PON solution, the conventional copper cables can be replaced, the duct resources within the buildings are freed up and the duct space is available for future network expansion or network scaling.

By achieving a single converged PON network solution for both the factory workshop and office area, the services configurations and managements can be unified, and faster troubleshooting can be achieved.

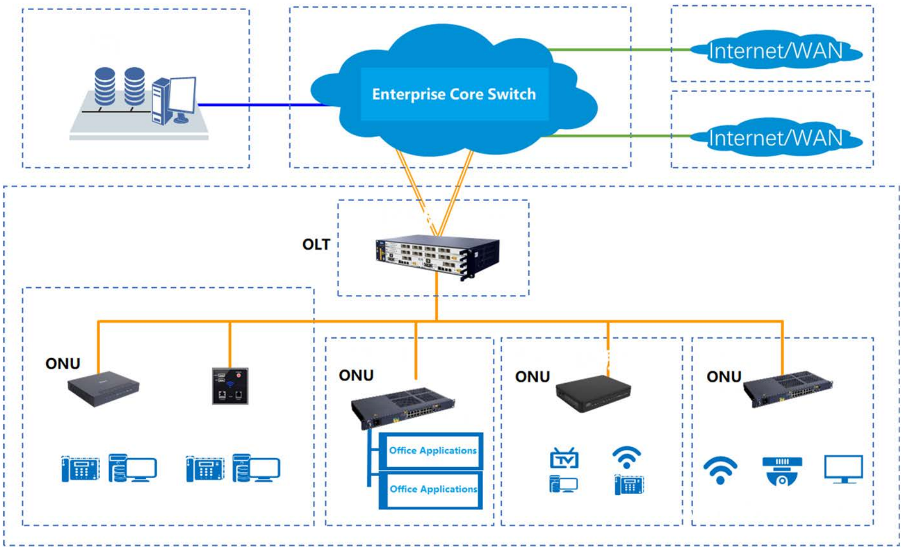


Figure 3: Office network connection via Industrial PON overview

5.4 Surveillance network

Beside the field level network and the office network, other major industrial network scenarios are the video surveillance networks and environment sensing networks around the factory. The industrial PON can fully support sensing services. A PON ONU needs to be capable of supporting Power over Ethernet (PoE) functionality when necessary to provide both network connectivity and electricity supply for remote video monitoring cameras. Other capabilities like Wi-Fi® AP, small cellular cells can also be embedded to the industrial PON ONU to realize the data transmission for several kinds of sensors.

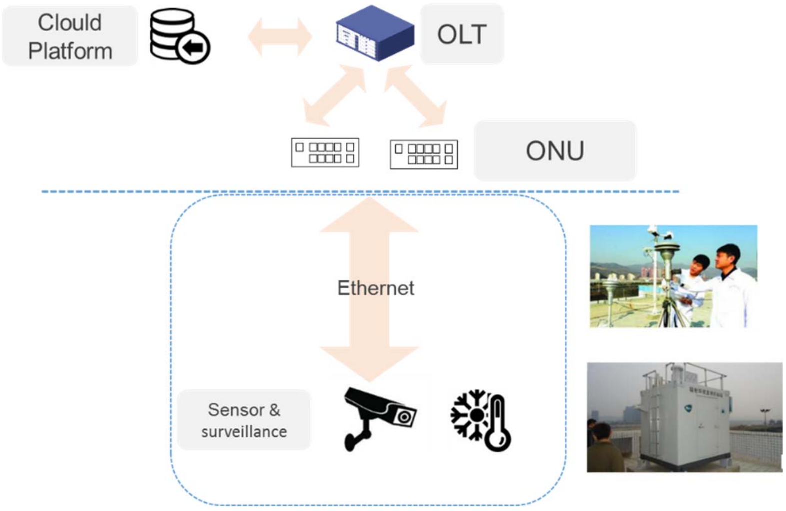


Figure 4: Industrial PON for sensor & surveillance network overview

In the intelligent factory, there are more and more machine vision applications being deployed. High-resolution image/video cameras are installed on the production lines to capture high-definition images or video streams for further AI-based analysis and recognitions, which can quickly locate defective production and products.

Such applications need very large upstream bandwidth on the network, as the traffic could be in the order of tens of gigabits per production line. 10G industrial PON systems, such as 10G-EPON and XGS-PON can be used to satisfy these bandwidth needs and future 50G PON system can further provide 5 times more bandwidth.

6 Industrial PON system description

6.1 System overview

6.1.1 Typical system architecture

The industrial PON system is within the scope of the F5G network architecture defined in ETSI GR F5G 004 [i.4], and it includes both the CPN (Customer Premises Network) and AN (Access Network) segments of the underlay plane.

The industrial PON system provides service connectivity for the users and devices in the industrial area. The major protocols used in the industrial scenarios are supported by the industrial PON system. The ONUs performs the SAP (Service Access Point) functions and the OLTs performs the SPP (Service Processing Point) functions.

As the industrial PON system is the underlying network of the industrial factory intranet, the factory intranet may be self-contained depending on the network scale and security considerations of the customers. The aggregation edge functions such as BNGs are optional for the OLT uplinks. The industrial PON can either be connected to higher level network elements or be stand-alone.

The industrial PON system supports the MCA (Management, Control & Analytics) plane interfaces and related operation and management functions. Conventional network management protocols such as TL1 and SDN based protocols such as NETCONF/YANG are supported by the industrial PON, and advanced functions such as AI analyser can also be deployed in the industrial PON system, see Figure 6.

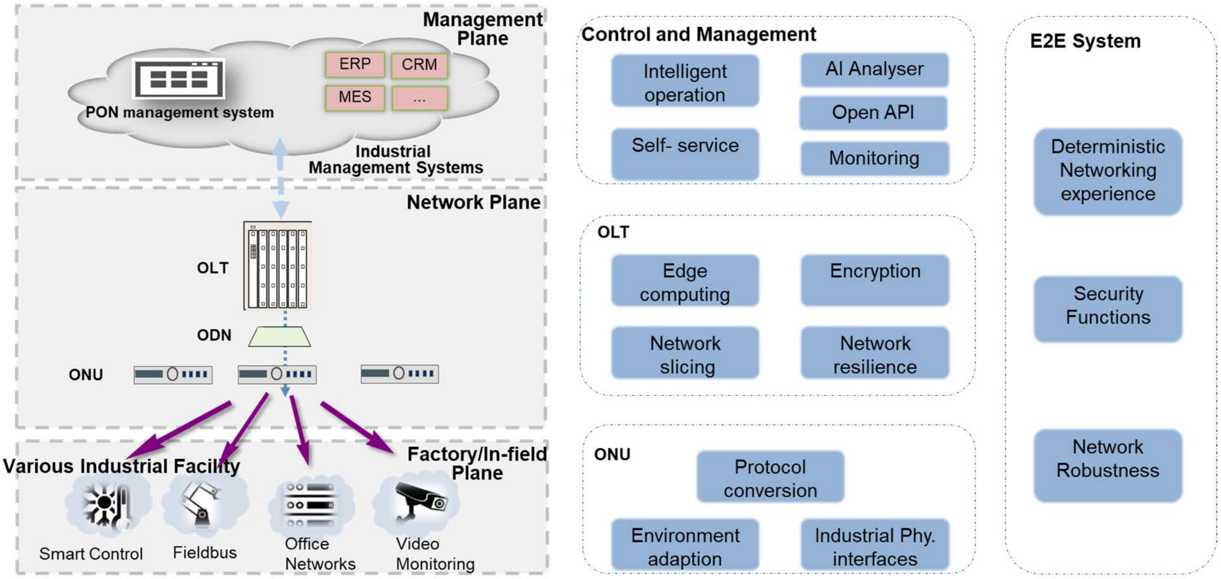


Figure 6: Industrial PON system architecture overview

As shown in Figure 6, the industrial PON system acts as the intra-plant communication hub. The Industrial ONUs provide the interconnection capability and various industrial physical interfaces and protocol conversion capabilities. Various factory facilities, office and surveillance services can easily be connected. The Industrial ONUs are optimized for operations in harsh environments, which may include very high temperature and/or complexelectro-magnetic issues.

The OLT has enhanced capabilities including network slicing, network resilience, encryption and edge computing to fulfil the services for industrial applications. OLTs with built-in open computation platforms can realize essential edge computing functions, to satisfy the local data processing in the factory, and can further cooperate with higher layer cloud computing facilities to provide dedicated cloud and IT services for industrial customers.

The industrial PON control and management system support conventional and SDN-based intelligent operation and management. The industrial PON control and management system can provide open API to other existing manufacture management system within the factory, and can lead to IT and OT convergence.

6.1.2 An alternative system architecture

6.1.2.1 Alternative spine-leaf architecture for large-scale industrial park scenarios

For a large industrial plant or a possible expanded industrial park, several OLTs need to be deployed in the factory to transport extensive east-west traffic traversing across the distributed plant.

The conventional architecture and management method mentioned in the previous clause may not be fully suitable for such large scale PON scenarios, as it may lead to issues of high operation and maintenance cost.

To address these issues for large-scale industrial park scenarios, an alternative architecture using a spine-leaf architecture, is shown in Figure 7.

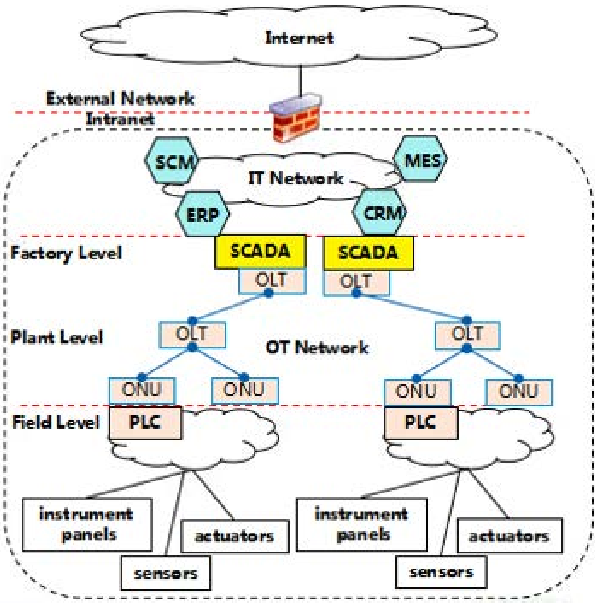


Figure 7: An alternative spine-leaf architecture for industrial PON within the scenario of large-scale industrial park

It is an alternative to the system architecture documented in clause 6.1.1.

6.1.2.2 Overview of the alternative spine-leaf industrial PON Architecture

The detailed architecture of the spine leaf industrial PON OLT extension is illustrated in Figure 8.

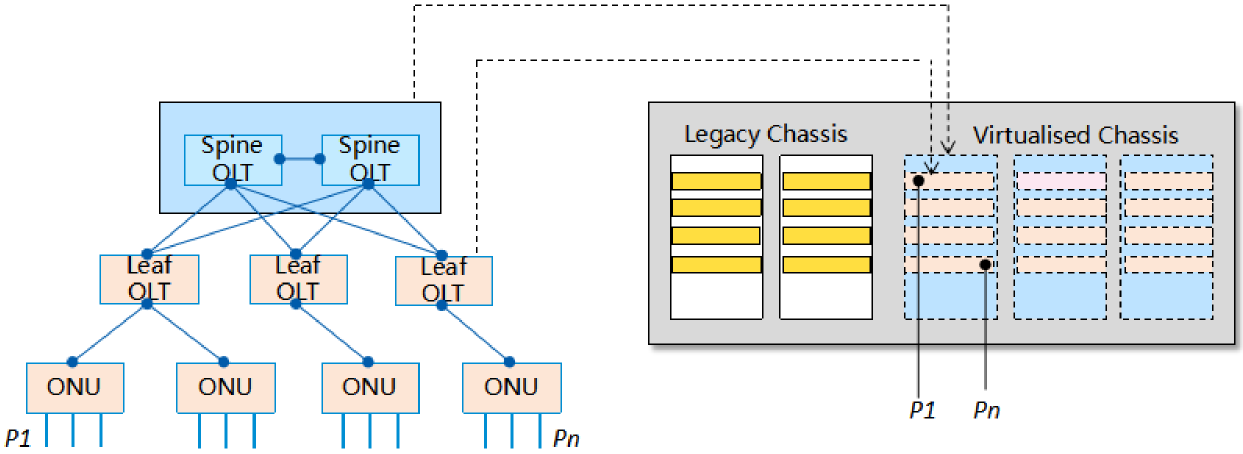


Figure 8: Management of the physical spine leaf Industrial PON OLTs and ONUs Controller

The physical spine OLT referenced in Figure 8 could be a physical core switch supporting PON interface board, located between the industry external network and the intranet. These spine nodes (whether spine OLTs or core switches) on the top of leaf OLTs are required to support the traffic from multiple plants.

The leaf OLTs and the distributed ONUs are deployed close to the plant and field network for dense coverage purpose. Although one single PON trunk fibre connection from one leaf node to the above spine node functions correctly, it is recommended to make these fully meshed connections between leaf nodes and spine nodes to improve system resilience and robustness, as shown in Figure 8.

The spine OLTs and leaf OLTs maybe differ in chassis size and total number of ports, but there are no fundamental differences between the OLTs in clauses 6.1.1 and 6.1.2, and no specific functional OLT requirements.

The datacentre-like spine-leaf switching architecture is easy to manage and expand. Because of virtualization and DC technologies that are rapidly growing in the IT world, the industrial park can also deploy the virtualization concepts into the management of the OT network.

The management of this core switch chassis assumes a northbound M&C PON controller to manage these PON extension devices in the industrial park network. From the perspective of the PON controller of this industrial park network, the spine OLTs considered a single virtualized L2 & L3 integrated virtualized switch chassis, and the virtualized chassis manages the two-levels of OLTs in the factory. That is one leaf OLT is virtualized as a service board on the chassis, the ONU UNIs connected to this OLT are virtualized as the customer interfaces on the service board.

This virtualization approach on the PON controller simplifies the management of the PON extension network:

- making it easier for operation and maintenance;
- reducing the cost; and
- smoother process for the future escalation and migration of the controller (potential future updating the version of PON controller itself, and/or migration to faster and lager scale cloud platforms).

Another benefit is, that the SCADA (Supervisory Control and Data Acquisition) system, the PON controller, and industrial management systems can share the DC environment.

6.1.2.3 Alternative spine-leaf industrial PON deployment scheme

The common functions of the OLT and the PON layer can be separated. The common functions can be abstracted and moved to the spine nodes or the chassis, while the low-cost leaf OLTs, take the role of the PON layer that extends PON P2MP branches to those industrial ONUs for field network operation.

The OLT-C (OLT Control) function in the PON controller is responsible for translating a data model-based input received via the M&C NBI to PON message interface (e.g. OMCI primitives). It includes the transmission of the M&C messages in sequence to the dedicated service board, PON port and the target ONUs. It is also responsible for the response collection received on a request, and for notifications of events, which are received from the industrial plant deployed ONUs.

The OLT-C is centrally located on the PON controller is also a hub to other dedicated control functions. These functions include traffic steering and zero-deployment control. The AI assisted traffic flow diagnostics are decoupled and modularized in software, which contribute to easy service deploy and expansion.

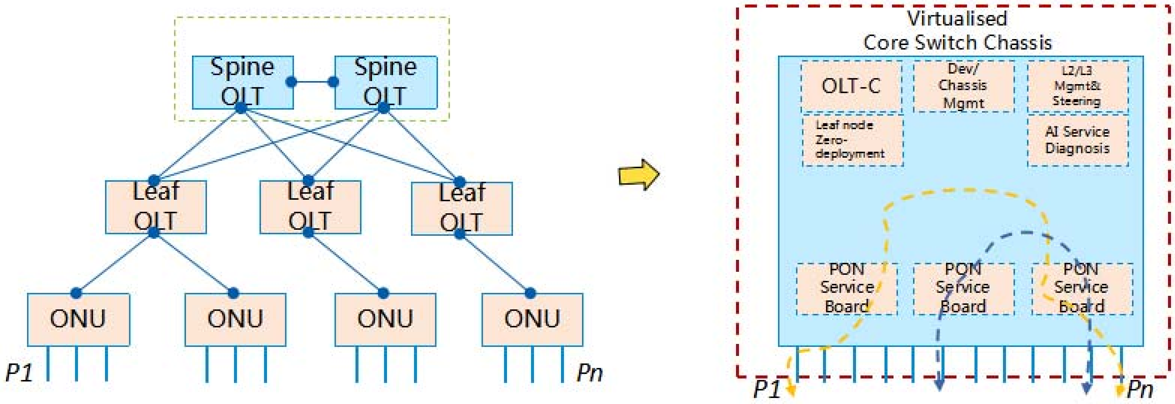


Figure 9: Existing Functions of Leaf OLTs and Attached ONUs are abstracted as Decoupled Modules

This architecture facilitates the high-density coverage extension of the industrial PON network and associated management, and enables the smooth upgrade of bandwidth and devices.

6.2 Overview of the ONU in the industrial scenarios

Industrial scenarios impose new demands to PON ONUs as used in today's residential markets.

The PON ONUs deployed in a residential scenario are used to connect subscribers' computers, mobile devices, set top boxes and intelligent devices. In residential scenarios, the ONUs support IEEE 802.3 (see [i.15]) to [i.21]) to Ethernet interfaces and IEEE 802.11 Wi-Fi® AP modules at the UNI (see [i.22]) to [i.27]).

However, in the industrial scenarios, the machines/devices in the industrial networks maybe very different from those used in residential scenarios. Some legacy or specific machines/devices may not support standard Ethernet interfaces, instead they may be equipped with industrial field level interfaces such as RS-232/485, CAN, DI/DO interfaces, and related protocols running over these physical interfaces. The ONUs used to connect to these machines/devices need to support these interfaces in addition to standard IEEE 802.3 Ethernet and IEEE 802.11 Wi-Fi® interfaces.

The industrial ONUs need to function correctly in very harsh environment. Another significant difference between industrial PON ONUs and residential ONUs is that they need to adapt to industrial environment conditions such as temperature, humidity, electromagnetic fields and water/dust, etc.

The main differences are summarized in Table 1.

Table 1: Comparison of major differences between industrial PON ONUs and residential ONUs

ONU Type	Industrial PON ONUs	Conventional residential ONUs
User network interface	RJ45, Wi-Fi® RS-232, RS-485, CAN, DI/DO etc.	RJ45, Wi-Fi®, POTS etc.
Environment conditions	Wider working temperature range: -40 °C to 70 °C (see note) Humidity Water/dust Electro-magnetic fields	Room temperature
NOTE: For conventional industrial grade network device the temperature range is -40 °C to 70 °C, while the upper limit could be as high as 85 °C in some scenarios, such as the metallurgy industry, etc.		

There are multiple types of machines/devices in the industrial PON networks as illustrated in Figure 10.

For the office network and video monitoring scenario, the ONUs will support standard IEEE 802.3 Ethernet and IEEE 802.11 Wi-Fi® interfaces. PoE (Power over Ethernet) support is needed for connecting devices currently powered with PoE, such as surveillance cameras or standalone Wi-Fi® Aps.

For the machines/devices with specific industrial interfaces mentioned above, there are two approaches to connecting them with industrial PON ONUs:

1) Use an industrial gateway, which will provide the specific industrial interfaces to the machines/devices, and support a standard Ethernet interface to be connected to the ONUs. These gateways act as an interworking function between the legacy industrial machines/devices and the ONUs. They may also have the capability to interpret specific industrial protocols.

2) Use ONUs with the specific industrial interfaces build-in, these ONUs can be seen as a combination of PON ONU and industrial gateways. These ONUs can have additional capabilities such as to transform/interpret industrial protocols/data.

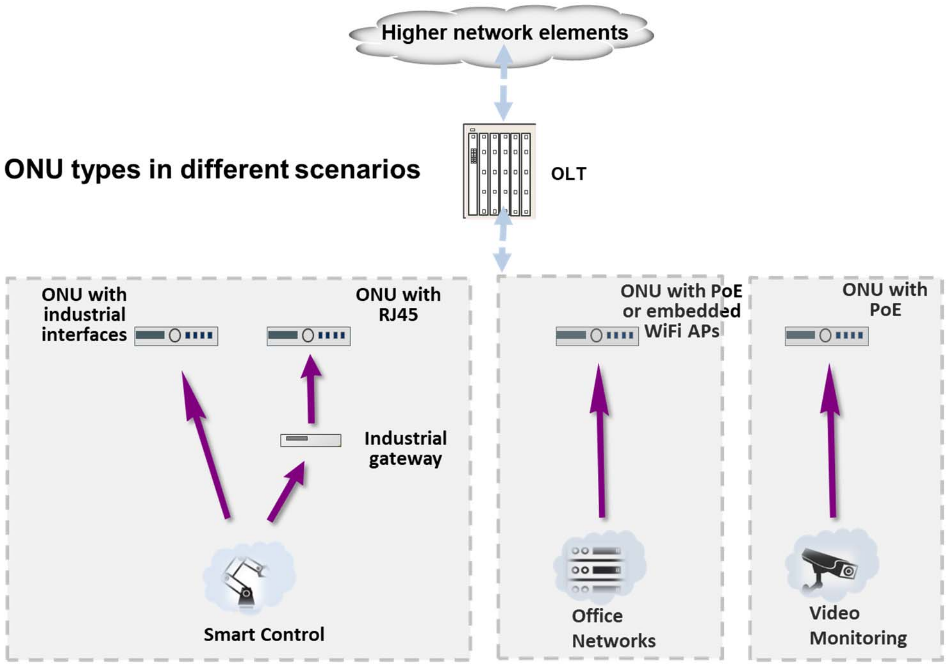


Figure 10: Illustration of ONU types in different scenarios in the industrial

The environmental recommendations for the industrial PON ONUs can be found in clause 7.4 of the present document.

6.3 Industrial PON management system overview

6.3.1 Industrial PON Management Needs

The current PON management systems are designed for public access networks, and these systems have a complete set of network management functions, which cover all aspects of the public access network control and management. Thus, these systems are complex, require extensive server hardware resources, and need specially trained personnel to operate them, which implies very high investment and human resource costs. These facts could possibly reduce the interest of the industrial customers to choose industrial PON solutions for their factories.

On the other hand, as industrial PON system is deployed within the factory intra-networks, the deployment scale and service characteristics are very different from conventional public access network scenarios. Industrial customers have specific industrial functional requirements and have greater demand on the PON management systems for interaction with their existing manufacturing systems, which have not yet been realized by current PON management systems.

6.3.2 Management System architecture

Figure 11 shows a typical system architecture of the industrial PON management systems. The system has three main layers:

1) **Management & Orchestration Layer:**

   - This layer provides APIs and function modules related to other existing manufacturing system, as MES (Manufacturing Execution System), ERP (Enterprise Resource Planning) etc., hence the industrial PON system can provide solid linkages with other corresponding systems within the factory supporting smart factory and intelligent manufacturing demands.

2) **Function Platform Layer:**

   - This layer contains all the function modules capable of converting factory network administrator's objectives into commands to configure the underlying PON equipment:

     a) Management modules: these modules provide the fundamental network management functions for the PON system in the industrial scenarios, including network elements access control and authentication, configuration editing and distribution, fault locating and diagnosis, etc.

     b) Service modules: these modules support functional management other than fundamental network management functions, including edge computing, container-based industrial application management.

     c) Analysis modules: these modules provide network status analysis, fault analysis and network landscape overviews based on artificial intelligence.

3) **Network Configuration Layer:**

   - This layer provides southbound interfaces, using standard the NETCONF/YANG scheme to directly manage underlying PON devices, including both OLT and ONU. One main stream scheme is using NETCONF/YANG to manage and configure OLTs, while the ONUs are managed with standard OMCI schemes by the OLTs, but other alternative schemes can be used.

   - Telemetry-based function module is also included in this layer, and real-time and high precision performance data collecting can be realized by this module.

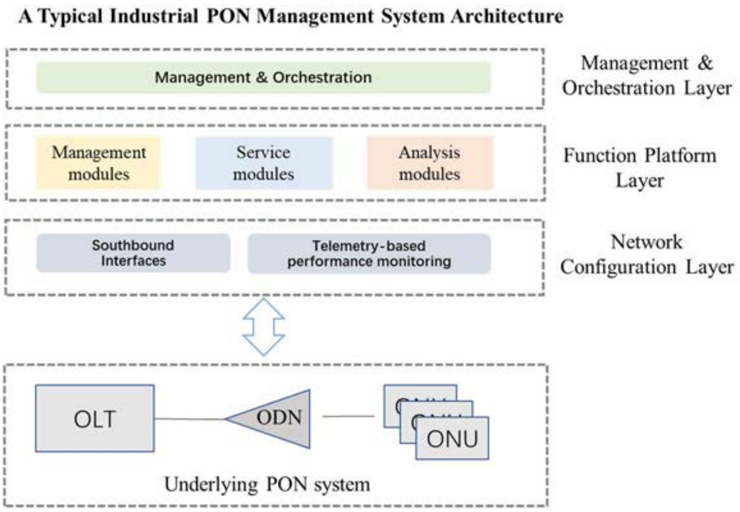

A Typical Industrial PON Management System Architecture
Management & Orchestration
Management & Orchestration Layer
Management modules
Service modules
Analysis modules
Function Platform Layer
Southbound Interfaces
Telemetry-based performance monitoring
Network Configuration Layer
OLT
ODN
ONU
Underlying PON system

Figure 11: Typical industrial PON management system architecture overview

7 Key function and performance recommendations

7.1 Industrial PON features

7.1.1 PON slicing

7.1.1.1 PON slicing application scenarios

As the manufacturing factory expands, and the intra-network reaches more zones within the factory, the industrial PON OLT acts as a convergence hub within the factory. It could be used to carry more and more sub-networks, such as, but not limited to, the manufacturing management network, the manufacturing control network in the field, the office network and the video surveillance network around the factory, as shown in Figure 12.

However, if every sub-network connects directly to an OLT without any physical or logical isolation, there may be potential service and security issues.

For the service aspect, as different sub-networks are carrying different network elements, their requirements on the network performance could be diverse. So running all the sub-networks within a single network may cause unexpected service degradation, such as larger latency/jitter, unexpected packet loss. These degradations are unacceptable for some critical applications within the factory, and may cause potential production downtime or low production efficiency.

For the security aspect, certain sub-networks are not authorized to visiting public internet sites, while others may needs to. Putting all the sub-networks together may cause security issues such as sensitive client information may be hacked by intruders from the public internet.

One solution to overcome these issues is to have a dedicated OLT for every sub-network, so that they have no potential service conflicts and security issues. However, the hardware and management cost could be very high if the number of sub-networks is large while number of users within a single sub-network is small.

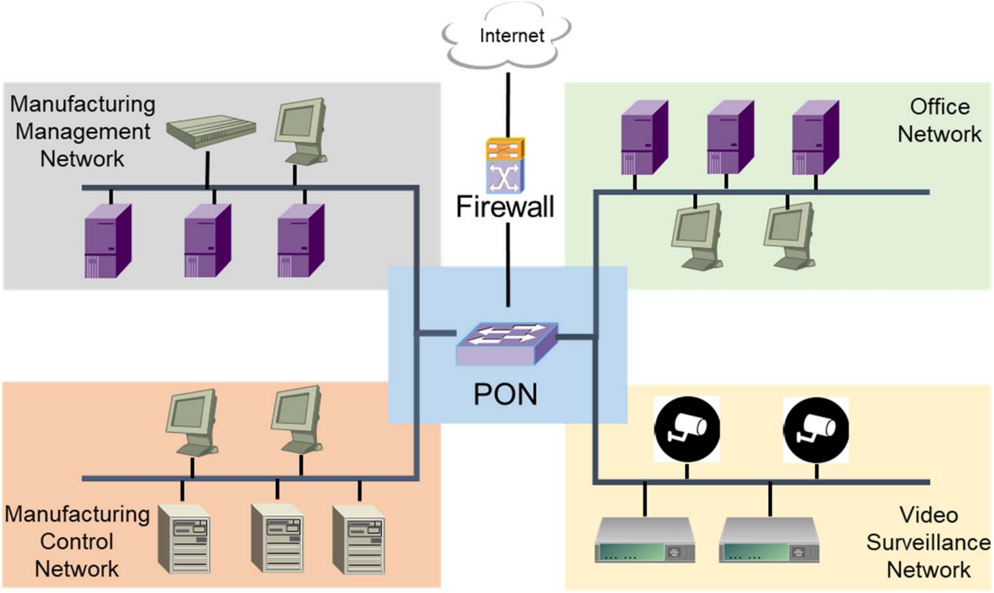

Internet
Manufacturing Management Network
Firewall
Office Network
PON
Manufacturing Control Network
Video Surveillance Network

Figure 12: illustration of multiple sub-network within a factory

A better solution to these problems is to implement PON slicing techniques, so that a single physical OLT is located within the factory, and different slices are used to carry different sub-networks. Each slice is isolated from each other with respect to the service and security issues, and can be individually managed.

7.1.1.2 PON slicing architecture

The system architecture for PON slicing within industrial scenarios is illustrated in Figure 13. The service is independent for every slice, users within a single sub-network are unaware of the existence of user from other sub-networks, and the physical OLT appears to be dedicated to a given user group in a sub-network.

On the management level, network administrators from one sub-network can only see and manage their own slice, and any customized configuration on the slice has no effect on other slices within the same physical OLT.

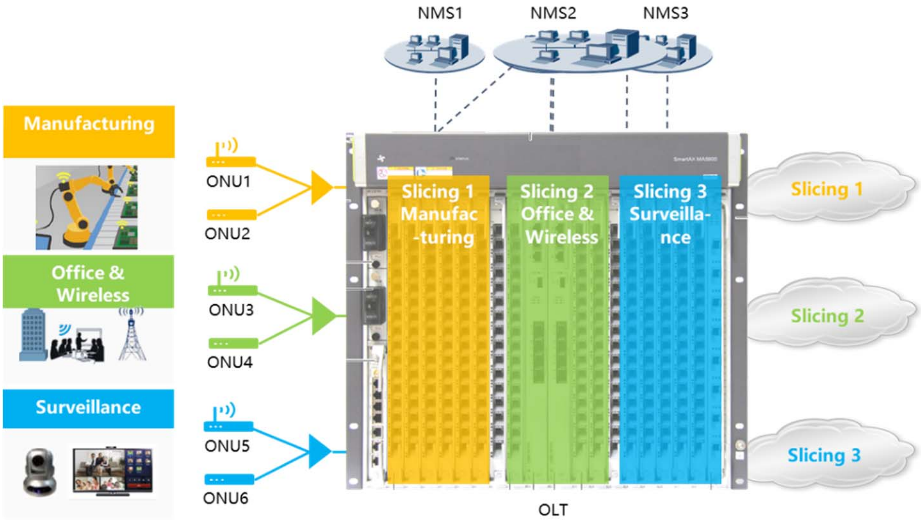


Figure 13: The system architecture of the PON slicing

7.1.1.3 PON slicing deployment scheme

7.1.1.3.1 PON slicing granularities

There are three main granularities for PON slicing:

- OLT line card slicing.
- OLT port slicing.
- ONU slicing.

7.1.1.3.2 OLT line card slicing

As shown in Figure 14, the PON slicing is on the line card level, different line cards could be configured as different slice within the physical OLT. This is the coarsest level of slicing allocation. It is suitable for large scale intra-factory networks with hundreds of network elements in one sub-network.

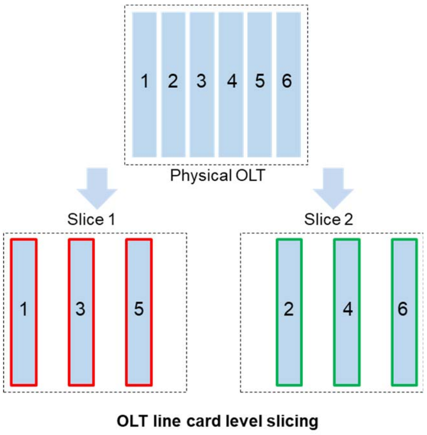


Figure 14: PON slicing on the line card level

7.1.1.3.3 OLT port slicing

As shown in Figure 15, the PON slicing is on the PON UNI port level, different UNI ports on the OLT could be configured as different slice within the physical OLT, different ports on the same line card can be allocated to different slice. This is a medium level of slicing allocation. It is suitable for medium scale intra-factory network with tens to hundreds of network elements in one sub-network.

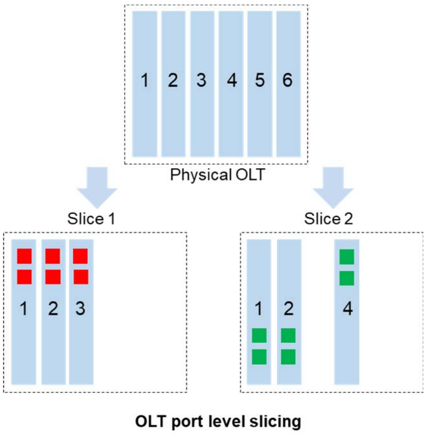


Figure 15: PON slicing on the OLT port level

7.1.1.3.4 ONU slicing

As shown in Figure 16, the PON slicing is on the PON ONU level, different ONUs could be configured as different slices within the physical OLT, and various slices can co-existed on the same OLT PON UNI port. This is the finest level of slicing allocation. It is suitable for small scale intra-factory network with several to tens of network elements in one sub-network.

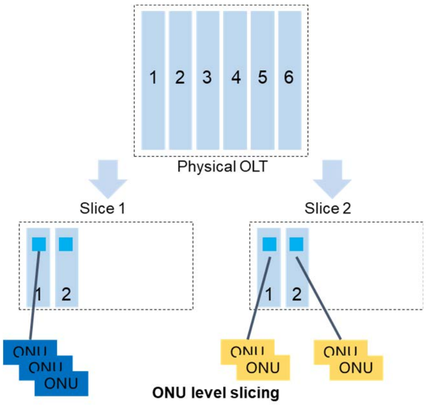


Figure 16: PON slicing on the ONU level

7.1.1.4 PON slicing relevance in Industrial PON

PON slicing is an essential function for industrial PON, as it can carry multiple sub-networks within the factory with fewer physical OLTs, while keeping each sub-network isolated from the service, security and management point of view.

7.1.2 Edge computing

7.1.2.1 General architecture and recommendations

Edge computing is a core function of industrial PON scenarios. It is defined as a universal, distributed and open computing platform that provides limited compute, network, and storage resources. It can be deployed in industry devices, such as ONUs, OLTs, or edge data centres which are close to data sources, in cooperation with a centralized cloud computing entity to provide dedicated cloud and IT services for industrial customers. Industry devices and gateways with built-in open computing platforms are called on-site edge computing. OLTs and edge data centres with built-in open computing platforms are called network edge computing.

Edge computing applied toindustrial scenarios, include the following major features:

- Located in an edge environment, on the first hop of either network or data from the end user's perspective.
- Distributed deployment.
- Provides dedicated applications on a universal platform.
- Operate in cooperation with cloud computing.

The main drivers to deploy edge computing in industrial scenarios are:

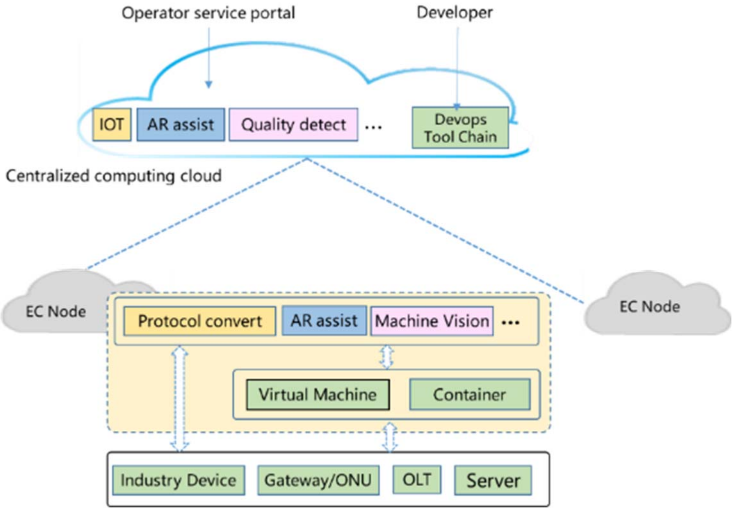
- to meet privacy needs by keeping the owner's data inside owner's campus;
- to terminate a large number of IIoT links locally, reducing the pressure on the bearer network and the centralized Data Centre;
- to terminate a large volume of data uplink, avoiding impact on the bearer network and centralized Datacentre;
- to support real-time decisions, control and self-optimization;
- to support the service continuity needs. Edge computing needs to function normally even in case that the bearer network or centralized Datacentre are out of service;
- to Support data optimization needs. Edge computing may perform conversion of a variety of industrial protocols to standard IP/Ethernet protocol; Add labels of location and time to the data; Pre-process data to reduce pressure on cloud processing (format conversion, structuration, data cleaning).

The following applications may be supported by universal edge computing:

- Traffic distribution in campus: A traffic distribution application is deployed in network edge computing to identify industrial application traffic and forward the traffic to the local campus server.
- Industrial IoT data protocol conversion: An industry application is deployed on the industry gateway (ONU) to convert various protocols such as CAN-BUS (Controller Area Network Bus), UART (Universal Asynchronous Receiver-Transmitter).
- Industrial machine vision data processing: A machine vision processing application is deployed on the edge computing platform to process images captured by industrial cameras to monitor quality of manufacturing and detect defective products.
- Process video or image data captured by surveillance cameras on campus: An image processing module is deployed on the edge computing platform to process images from campus cameras for vehicle flow analysis, facial recognition, vehicle license plate recognition, intrusion detection and fire detection.
- AR (Augmented Reality) assisted rendering and alignment: For example, to use AR assisted assembly in a complex assembly process. AR assisted assembly applications may be deployed on the edge computing platform, and virtual content (such as assembly tips) that needs to be projected on the AR glasses is rendered in real time based on the position of the eyeball sensor, and focus on the real-time images in spatial-time wise, and display them on AR glasses.
- For campus IIoT processing: For example, in warehouses, docks, and stations, logistics monitoring applications can be deployed on the edge computing platform to collect statistics on the number of categories based on the RFID information attached on the surface of incoming and outgoing objects and perform real-time control (categorized storage location guidance and abnormal object interception).

The Above applications are only some of the application cases of edge computing in industrial scenarios. With the development of AI, sensing, and control technologies, more application use cases will be developed in the future.

Universal edge computing does not need to deploy a complete heavyweight cloud architecture or provide capabilities in normal cloud computing, including elastic computing, unlimited resource pools, dynamic expansion, and data sharing. It encompasses reasonable hardware capabilities and security requirements with cost constrains and engineering deployment conditions. It provides comprehensive IaaS (Infrastructure-as-a-Service) and PaaS (Platform-as-a-Service) platforms and tool chains to reduce application development and deployment difficulties and cloud-network collaboration. Figure 17 illustrates the functional architecture of edge computing.



NOTE: Gateway function may be embedded in the ONU in some cases.

Figure 17: Architecture of industry edge computing

According to the architecture of industrial PON edge computing shown in Figure 17, it is recommended that edge computing has the following characteristics:

- General computing and storage capabilities:
  - The basic hardware platform needs to provide integer, floating point, hash, and vector computing capabilities that meet corresponding scenario requirements. It may be based on CPU, GPU, AI ASIC, FPGA, DSP, or a combination of these electronic devices (heterogeneous computing resources). To provide persistent storage capabilities that meet scenario requirements, the storage hardware may be SSDs, mechanical hard disks, and NAND/NOR flash memory.
  - The basic hardware platform for computing and storage may be located in Industry Devices, Gateways, ONUs with embedded gateway functionality, and OLTs, or universal servers in the campus.
- Network connection and acceleration capability:
  - Basic hardware needs to support user specific applications such as protocol conversion, AR assistance and machine vision which cooperates with applications located in the centralized cloud. Basic hardware may also provide Layer 2 and Layer 3 network connections for Containers and VMs (Virtual Machine) which are either standalone or on the IaaS layer if IaaS is deployed.
- Engineering aspects of hardware deployment:
  - The industrial environment has many special environmental requirements. The edge computing hardware on industry gateways and devices need to meet engineering deployment requirements, such as electromagnetic compatibility, temperature, humidity, power supply, noise, vibration and reliability. The edge computing card on the OLT and the integrated or universal server of the edge datacentre needs to meet the mechanical, electrical, temperature, and heat dissipation requirements of the deployment environment.
- Open edge computing IaaS platform:
  - An optional open IaaS foundation may be provided in the form of containers or VMs at the edge, combined with the centralized edge computing IaaS management portal on the cloud, to implement lightweight container/VM unified O&M and automatic lifecycle management, multi-type PaaS hosting, on-demand usage and billing. In addition, the underlying hardware capabilities can be encapsulated into specific APIs (such as GPU for video processing) to support hardware-assisted acceleration.
- Edge computing PaaS platform:
  - An optional distributed lightweight PaaS platform is provided on edge computing nodes, together with the centralized management platform of edge computing PaaS on the cloud, to provide some encapsulated value-added services for third-party developers, simplifying application development and rollout. The PaaS platform needs to encapsulate network capabilities such as QoS, location sensing, time service, network security, user identifier, and terminal identifier and open to third-party developers. Besides this, platform management openness is also required, by using APIs to encapsulate the running environment, the life cycle management, the configuration, the computing, and storage capabilities. Furthermore, the PaaS platform may provide some open and differentiated services, for example, providing services such as the AI inference framework, AI model and algorithm library, graphics and image processing, knowledge graph, and speech recognition.
  - Complete tool chain for development, commissioning, release, provisioning, and maintenance to automate operations.
  - To enable third-party developers to use edge computing at a "zero" cost, a complete tool chain needs to be provided based on the cloud environment to implement the DevOps (Development and operation) process, and automatic release, deployment, provisioning, and maintenance need to be supported.
- Complete security mechanism:
  - Physical security, IaaS/PaaS platform (if applied) security, application security, and network capability openness security need to be considered for edge computing nodes.

- Cloud-Edge synergy:
  - Edge computing is an extension of cloud computing. The management of service portals, hardware platforms, IaaS and PaaS platforms (if applied), DevOps tool chain, and security mechanisms all need to be synergized between the cloud and edge.

7.1.2.2 Typical edge compute scenarios

In an industrial PON campus, unmanaged, unauthorized industrial terminals in all forms and scales may connect to network at any time. These terminals are invisible to most underlay networks and their private access and spoofing is a challenge to the existing access control systems. Beside the authentication and admittance functions, other functions such as connection management, network topology update, device status monitoring, real time data collection of these terminals, also pose challenges for the existing management and control systems.

These industrial terminals include industrial IoT devices such as environmental humidity sensors, temperature sensors, and vision & surveillance monitors, field machinery actuators like PLC machines, or even PC and telephone smart devices but for industrial purpose. Managing these various terminals introduces complexity to the existing management system, given the fact that data collection approach and standard management protocol varies for the different terminal types. Therefore, the mechanism of managing large number of industrial terminals in an edge compute oriented industrial campus needs to be refined to solve these problems.

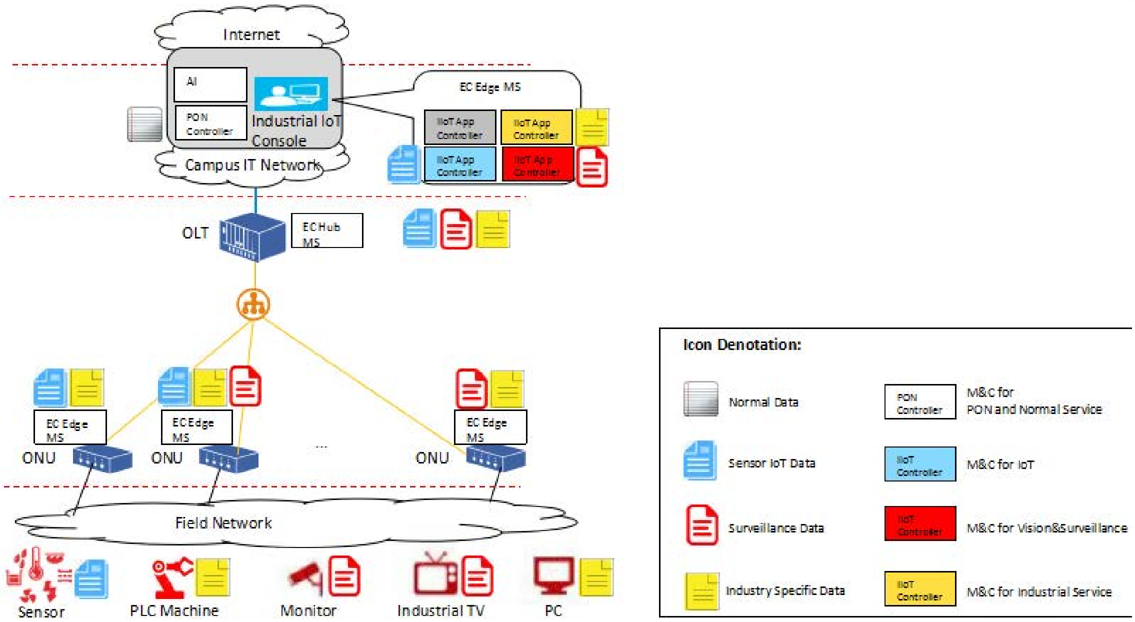


Figure 18: IIoT Controllers for Managing Dedicated Types of Terminals and Their Data in the Industrial Campus

The management of industrial field machinery actuators, together with Industrial Internet of Things (IIoT) devices, requires deeper integration between IT, OT, cloud, and industrial PON campus networks. Thus the industrial field machinery actuators management systems are frequently merged with industry IT/OT and industrial PON network management systems which were already deployed by Centralized Computing Cloud.

The Industrial IoT (IIoT) management, illustrated in Figure 17 on Architecture of industry edge computing, is a set of future IIoT applications or controllers which have complete view of all connected IP addressed industrial terminals and provide an integrated, real-time access control and management system for them.

Access control of the system can sense the terminal access, block and isolate the unauthorized terminal access to make industrial campus access more reliable and safer. Data collected from the IIoT devices such as sensors and monitors are recommended to follow publish and subscribe processes on the edge applications, from which the subscribed data are forwarded to the target IIoT app (illustrated in Figure 18 and highlight as blue app, red app) for final data analysis and control decision. Similarly, data capturing and forwarding of the field machinery actuators follows OPC-UA industry standard to its target IIoT app (illustrated in Figure 18 and highlight as yellow app). These IIoT apps provide a visionary approach to the routine terminal administrating, connection status monitoring, terminal lifecycle management, and topology map on-plan periodical maintenance. If AI is desired, it can be introduced as an optional management module per operator requirements to aid high-level decision making to the field machinery actuators.

The PON controller ensures the management of underlay network to the industrial terminals, and is co-located with the IIoT apps in the centralized computing cloud. The PON controller is responsible for PON asset discovery, PON associated connection update, topology map maintenance, device status and alarm monitoring, imposing role-based access control, terminal access and authentication policy on the gateway etc. Besides, the Plug-and-Play the server is either build-in or collaborate with the PON controller for zero-touch commissioning of PON devices in the network, such as OLTs and ONUs (industrial PON gateway). NETCONF is a widely accepted protocol for network configuration communicating between the system and the target devices, while YANG informs how to encode the configuration in XML.

In Figure 18, Edge Computing Edge Management System (EC Edge MS) and Edge Computing Hub Management System (EC Hub MS) are IIoT data orchestration platforms to host IIoT apps and help deliver the data from industrial terminals to the centralized compute cloud. Deploying the EC Edge MS platform on Industrial PON gateway and the EC Hub MS on OLT. This approach offers an efficient assistance to improve the cooperations between edge applications and those in centralized compute cloud.

Industrial PON gateway in the campus is proposed to be an edge-compute enabled network devices. EC Edge MS can configure and manage edge applications for large numbers of industrial terminals from centralized compute cloud to edge compute nodes. Two-level EC Edge MS at gateway and centralized compute cloud are for different application purposes. Time critical and on-premises terminal information associated edge applications are suitable to be installed on the EC Edge MS near to the gateway, while EC Edge MS at the central cloud is a better choice to host versatile applications for terminal information processing, diagnosis, data analysis, predicting future trends, and enables intelligent close-loop control. The application of process and analysis hierarchically is a widely accepted deployment method in cloud compute environment for IIoT.

The EC Edge MS provides web-based user interfaces for both on-premises and central cloud-based management, and especially DevOps tools to build, distribute edge applications to the Industrial PON gateway.

The edge applications for industrial terminals includes:

1) Processing high volumes of data at the edge and deliver a real time closed loop control.

2) Introduces appropriate execution application at the edge from the industrial partnership ecosystem.

3) Increases the speed of industrial production deployment with edge application management and execution to allow to scaling-up of IIoT deployments.

4) Scan and discover the industrial terminals, collect and build-up databases of terminal information. Popular scan tool e.g. nmap (Network Mapper is a free and open source utility for network discovery and security auditing) is an option for fingerprint info gathering, while OPC-UA technology is preferred for industrial data collection from the machinery actuators. They are deployable to edge-compute enabled industrial PON gateway.

An extra compute-capable platform deployed in the form of OLT line card, can act as a hub and middle layer between the edge computing cloud and the centralized compute cloud, and can shadow the details of the elements within the edge computing cloud. The upstream information from IIoT apps can be interpreted by this hub, and reducing the direct data interactions between centralized computing cloud and the edge computing cloud nodes.

7.1.3 Industrial interfaces and protocol adaptation

7.1.3.1 Interface types for the industry

Industrial PON is supposed to replace the current point-to-point Ethernet based network, to provide a simpler and cheaper connections for industrial equipment from multiple vendors. In such a system, the OLT provides access, aggregation, switching, and edge computing. The uplink interface of an OLT typically connects to a datacentre in the factory or in a private Cloud. ONUs, as terminals of the system with imbedded industry gateway functions, connect to the OLT and provide User-Network-Interfaces (UNI) to end users with various user interfaces for different industrial services.

7.1.3.2 OLT Ethernet interface

The Ethernet interface of an industrial PON OLT can provide several types of Ethernet interfaces, including FE, GE, 10GE, and higher-speed interfaces. In the case a GE interface is used, 10M/100M/1000M auto-negotiation needs to be supported. 10GE interfaces can be one or more 10GBASE-SR, 10GBASE-LR, 10GBASE-ER and 10GBASE-LRM interfaces [i.13].

7.1.3.3 User-Network Interface (UNI)

Three types of UNI need to be supported by an industrial ONU: wireline Ethernet interface, wireless interfaces and industrial interfaces. Industry network gateway converts industry protocols and connect them via any of these interfaces:

1) The UNI needs to provide Ethernet interfaces, including FE, GE, 10GE and higher-speed interfaces in the future. A GE port can be either one of followings: 1000BASE-LX, 1000BASE-SX, 1000BASE-CX, and 10/100/1000BASE-T. To adapt to the evolution of Ethernet technology, 2,5G/5G BASE-T, which is standardized by IEEE 802.3bz-2016, needs to be supported by the ONU UNI. Power over Ethernet functions defined by IEEE 802.3af-2003, IEEE 802.3at-2009, IEEE 802.3bt-2018 may be optionally supported by ONU UNI interface including FE, GE, 2,5GE or 5GE BASE- T, see [i.13], [i.14], [i.15], [i.16], [i.17], [i.18],[i.19].

2) The UNI needs to provide wireless interfaces defined by following standards: IEEE 802.11a [i.23], IEEE 802.11b [i.24], IEEE 802.11g [i.36], IEEE 802.11n [i.25], IEEE 802.11ac [i.26], IEEE 802.11ax [i.27], and see also [i.20], [i.21], [i.22].

3) The UNI could provide industrial interfaces as needed, such as a Universal Asynchronous Receiver-Transmitter (UART), including RS485, RS232, and RS-422. Even though industrial PON is a common transport plane between industrial equipment and DC, providing industrial interfaces on UNI allows industrial PON to be applicable to more scenarios. In a real deployment scenario, an ONU may only support a limited number of industrial interface types and as such there may be multiple types of industrial ONUs.

Nowadays, there are quite a number of widely used industrial interfaces and protocols, such as Profinet, Profibus, CClink, Modbus, FOCAS, etc. In order to provide connections to industrial equipment with these interfaces, the industrial PON ONU with gateway function needs to provide corresponding physical interfaces and be able to transparently forward the industrial protocols or analyse the data. There is also a trend in the manufacturing industry to use OPC UA as a unified protocol to replace current fieldbus protocols. With the widespread application of industrial Ethernet interface technologies in industrial control scenarios, for example the deployment of TSN in the industry, these traditional industrial field bus protocols may be gradually unified to an industrial Ethernet interface.

By supporting industrial interfaces on the ONU, device data, production information and environmental data can be collected through these industrial interfaces, and then sent to the DC or Cloud with a unified protocol that is different from industrial protocols on the UNI.

Industrial PON ONU with gateway function could support built-in OPC UA server, MQTT (MQ Telemetry Transport) broker (a server that routes published messages to subscribers), HTTP communication with a web server. It also collects data from the industrial interfaces and real-time Ethernet protocol to be analysed.

7.1.4 Access security

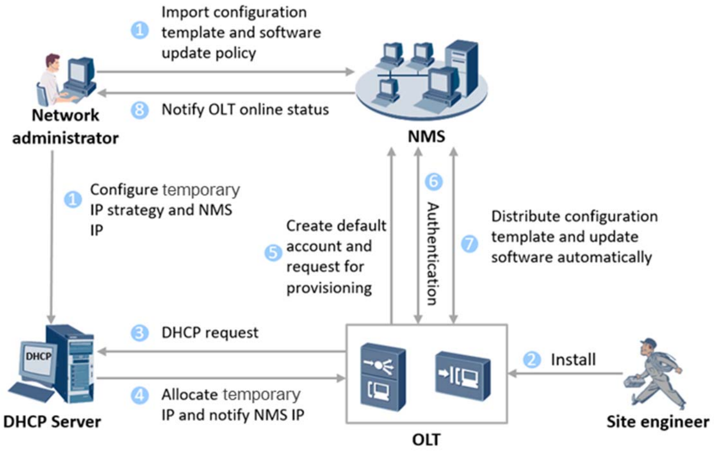
7.1.4.1 Overview

Access security for industrial PON needs security improvements and authentication optimization, ONU service activation and connection management of network elements, which connect to the ONU and OLT.

7.1.4.2 Security of Provisioning

Currently, ONU or OLT deployment and provisioning is usually performed manually by authorized technicians. However, manual configuration is slow and error prone. For F5G industrial PON devices a simpler and more efficient provisioning and configuration scheme is required, such as ZTP (Zero Touching Provisioning) for automatic provisioning and configuration.

ZTP removes the need for IT personnel to manually provisioned and configure hardware devices and reduces the risk caused by human error. It automates the process of system configuration, installing patches, etc. Figure 19 provides an example of ZTP functionality in OLT deployment scenarios.



1 Import configuration template and software update policy
8 Notify OLT online status
Network administrator
NMS
1 Configure temporary IP strategy and NMS IP
5 Create default account and request for provisioning
6 Authentication
7 Distribute configuration template and update software automatically
3 DHCP request
4 Allocate temporary IP and notify NMS IP
DHCP
DHCP Server
OLT
2 Install
Site engineer

NOTE: The ZTP function is secure with the assumptions that the DHCP server is protected with security functions like firewall and strong authentication mechanism for the administrator.

Figure 19: An example of ZTP function

The steps are:

Step 1: The network administrator creates a configuration on the DHCP server and NMS, and the configuration covers:

- Temporary IP allocation strategy and NMS IP address on DHCP server.
- Configuration template and software update policy on the NMS.

NOTE 1: The DHCP server verifies the identity of the network administrator using up-to-date authentication mechanism to prevent illegal access to the DHCP server.

Step 2: The site engineer installs the OLT and ensures it is powered on and connected to the network.

Step 3: The OLT sends DHCP request to DHCP server.

Step 4: The DHCP server allocates an IP address to OLT and inform the NMS of the allocated IP address.

NOTE 2: The DHCP server verifies the identity of the newly deployed OLT by factors such as MAC address or serial number.

Step 5: The OLT sends a provisioning request to NMS server.

Step 6: NMS server authenticates the identity of the OLT via the equipment serial number for example.

Step 7: Once authentication is successful, the NMS server distributes the default configurations to the OLT and starts software updating based on the policy configured in Step 1.

Step 8: The OLT report its on-line status to network administrator.

7.1.4.3 ONU access authentication

Network invasion is another major risk threatening industrial PON. An attacker may connect a malicious device to the network and perform MITM (Man-In-The-Middle) attack. To mitigate the risk, mutual authentication is required when a new device is connected to the PON network. The devices involved in the connection need to verify the identity of each other. A pre-installed certificate or pre-shared key is suggested as the factor of authentication which is defined by Recommendation ITU-T G. Sup74 [i.8]. The certificate or key used in device authentication needs to be protected from illegal access.

7.1.4.4 Security of device connected to ONU/OLTs in a PON system

In addition, the ONU and OLT need to be capable of identifying and blocking the connections of suspicious device. Features like Brute-force protection can help to identify and lock out the suspicious IP or account. Access control list based on IP, MAC, port or URL addresses can be used for connection management. Up to date technologies or schemes are need to be incorporated in the industrial PON system to ensure the security and resilience of the system.

7.1.5 Data security

7.1.5.1 Overview

Data security recommendations of industrial PON system, is mainly linked to three parts: data encryption, cryptographic key protection and data isolation.

7.1.5.2 Data encryption

Data encryption implemented in PON framing, such as AES256 or other data encryption schemes are used to protect the confidentiality of different types of data transmitted in industry PON.

Data transmission in an industrial PON network needs to be protected from eavesdropping and tampering. The industrial PON device can use best practice cryptography to communicate securely. The strength of cryptographic algorithms and primitives, defined by [i.28], used in PON frame encryption needs to be strong enough to cover the designed usage lifetime of the PON devices.

7.1.5.3 Cryptographic key protection

Protection of cryptographic keys and applications involved in service data encryption.

It is recommended that Industrial PON device support HMEE (Hardware-Mediated Execution Enclave) to prevent unauthorized access or modification of sensitive data and applications while they are in use.

EXAMPLE: Sensitive data include cryptographic keys used in data encryption and decryption, certificate used in authentication, etc. The execution of data encryption and decryption can also be secured in HMEE.

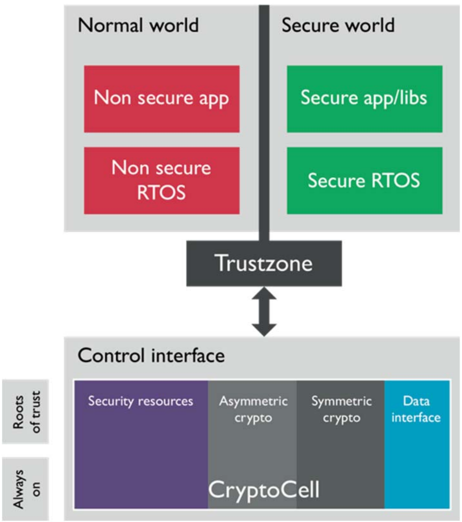


Figure 20: Trustzone-based HMEE architecture

Figure 20 shows the Trustzone-based HMEE architecture. The HMEE architecture is a general scheme which can be implemented in a CPU with different architectures such as x86/x64 and arm32/64. Different CPU vendors need to provide software, including but not limited to libraries and secure OS images, to support the HMEE architecture. With the software provided by CPU vendors, the PON equipment vendor can develop their own secure applications and deploy them into the secure world. The Trustzone isolates the system into two domains: the normal domain, where non secure app and non-secure RTOS are deployed, and secure domain, where secure app/libs and secure RTOS are deployed. The CPU works in either normal or secure domain at any time. System hardware ensures that none secure domain assets can be accessed from the normal domain. A secure design places all sensitive resources in the secure domain, and ideally has robust software running that can protect assets against a wide range of possible software attacks. In Figure 20, CryptoCell is used to provide a root of trust and a secure cryptographic mechanism.

7.1.5.4 Data isolation

Industrial PON provides services to the office, surveillance and manufacturing networks in the industrial environment. Data from different networks need to be properly isolated according to data sensitivity and QoS levels. Different networks, such as office network and manufacturing network, can be physically separated by isolating switches. Alternatively, VLAN or PON slicing can also be used to separate different data services.

7.1.6 E2E latency/jitter optimization

7.1.6.1 Overview

This clause describers the End-to-End (E2E) latency/jitter recommendations and its optimization for industrial PON networks.

7.1.6.2 E2E latency/jitter industrial needs

Industrial PON systems need to provide high-quality and deterministic network services for industrial manufacturing and production. In industrial scenarios, production networks are used for control, data collection, and connection.

Control includes remote control and field production line control. Remote control has certain requirements on network delay and network bandwidth. Field production line control mainly includes PLC, I/O, and device motion control, where network traffic is periodic and has different requirements for key indicators such as network delay and packet loss based on different control objects.

Data collection services include sensor data collection, video detection and collection.

Connectivity includes automatic device programme download, manufacturing and processing program download, wireless-based AGV navigation, and remote diagnosis and maintenance guidance.

Table 2 summarizes the quantified feature indicators and recommendations including delay, packet jitter and packet loss for each application running over industry networks.

Table 2: Industrial automation traffic types, service recommendations

Traffic types	Periodic/ Sporadic	Typical period	Data delivery guarantee	Tolerance to Jitter	Tolerance to loss	Typical data size (Byte)	Criticality
Isochronous	P	100 µs ~ 2 ms	Deadline	0	None	Fixed: 30 ~ 100	High
Cyclic Synchronous	P	500 µs ~ 1 ms	Latency bound (τ)	≤ τ	None	Fixed: 50 ~ 1 000	High
Cyclic Asynchronous	P	2 ms ~ 20 ms	Latency bound (τ)	≤ τ	1 ~ 4 Frames	Fixed: 50 ~ 1 000	High
Events: control	S	10 ms ~ 5 ms	Latency bound (τ	n.a.	Yes	Variable: 100 ~ 200	High
Events: alarm & operator commands	S	2 s	Latency bound (τ)	n.a.	Yes	Variable: 100 ~1 500	Medium
Network control	P	50 ms ~ 1 s	Throughput	Yes	Yes	Variable: 50 ~ 500	High
Configuration & diagnostics	S	n.a.	Throughput	n.a.	Yes	Variable: 500 ~ 1 500	Medium
Video	P	Frame Rate	Throughput	n.a.	Yes	Variable: 1 000 ~ 1 500	Low
Audio/Voice	P	Sample Rate	Throughput	n.a.	Yes	Variable: 1 000 ~ 1 500	Low
Best effort	S	n.a.	None	n.a.	Yes	Variable: 30 ~ 1 500	Low
NOTE: For camera-assisted control applications, camera traffic can be cyclic-asynchronous. Cameras are synchronized at the application level with a required synchronicity in the range of 1 µs - 10 µs. Camera traffic may produce higher data throughputs (e.g. 1080P/30 Hz/8-bit pixel video corresponds to 500 Mbit/s).							

7.1.6.3 Latency and jitter supported by current XGS PON standards

XGS PON is a TDMA-based system, whose end-to-end delay has the following main contributing factors:

1) The OLT system processing delay. For example, FEC encoding and decoding, data forwarding, and data traffic management, usually takes tens of microseconds.

2) The ONU system processing delay, for example, FEC encoding and decoding and data forwarding, takes around ten microseconds.

3) The delay caused by windowing for new ONU registration is about 250 ms, according to the ITU-T standard for an ODN with a maximum optical fibre length of 20 km.

4) Uplink DBA delay is usually hundreds of microseconds or even goes up to milliseconds sometimes

Table 3 illustrates factors contribute to latency in a PON system.

Table 3: Factors contribute to latency in a PON system

Factors	ONU process	Fibre (5 µs/1 km)	Discovery & Ranging	DBA	OLT	Total (Theoretical)
SR-DBA	~13 µs	~50 µs (10 km)	250 µs	~1 ms	30 µs	~1,3 ms
Fixed	~13 µs	~50 µs (10 km)	250 µs	125 µs	30 µs	468 µs
Separate Discovery & Ranging	~13 µs	~50 µs (10 km)	0	125 µs	30 µs	218 µs

7.1.6.4 Optimization for industrial PON system latency and jitter

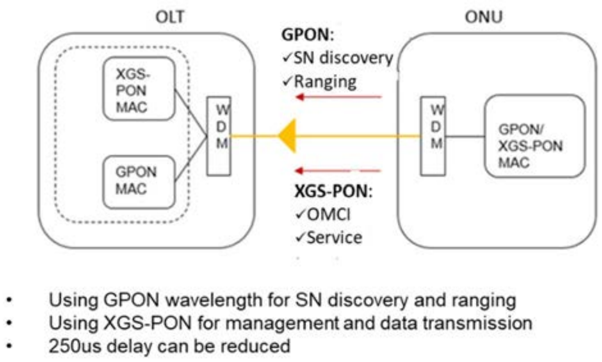
7.1.6.4.1 Overview

PON optimization in terms of latency and jitter was discussed in both industry and standards. There are several ideas addressing this topic.

7.1.6.4.2 PON link latency optimization by dual wavelengths

The main idea is to remove the impact of windowing for new ONU and DBA scheduling. Following figures illustrate one of the two ideas which were put on the table and discussed in ITU-T SG15/Q2. The idea is to use additional dedicate wavelength for windowing for new ONU registration, while the primary wavelength focuses on the data traffic, and fractional frame based burst which enables multi-DBA requests/grants in one frame, increases DBA scheduling frequency for different Alloc-ID within the same OLT channel pair, and reduces the traffic delay and jitter by corresponding times.

Because the PON system uses the time division mode in the upstream direction, it needs to periodically stop all online ONUs and open a quiet window for offline ONUs to register to the OLT. The delay is periodically 250 µs . By using two upstream wavelength channels, one wavelength is used for data transmission, and the other wavelength channel is used for registering an unregistered user, a delay of 250 µs caused by window opening can be eliminated. The principle is shown in Figure 21.



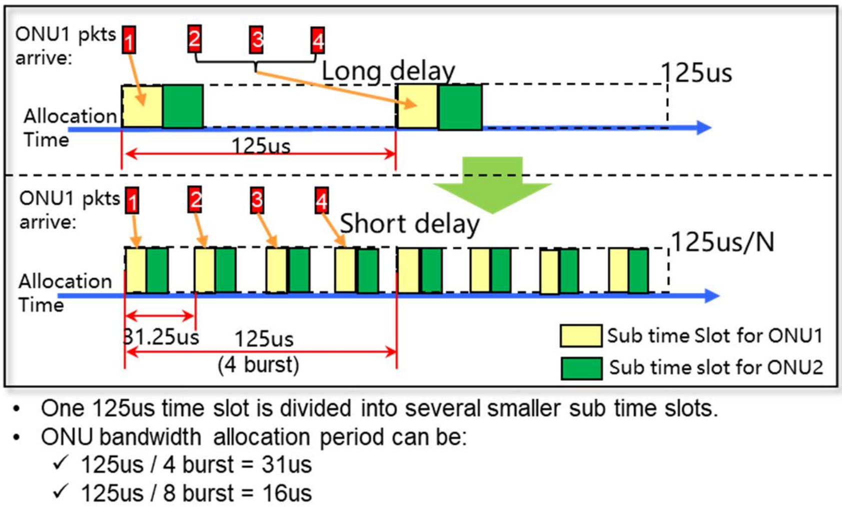
- Using GPON wavelength for SN discovery and ranging
- Using XGS-PON for management and data transmission
- 250us delay can be reduced

Figure 21: Dedicate wavelength for SN Discovery & Ranging

NOTE: The above explanation focuses on latency and jitter optimization. In some cases, the GPON channel may also be used to carry data traffic to maximize the bandwidth of PON system.

7.1.6.4.3 PON link latency optimization by means of fractional frame based burst

Another major contributor to the PON system delay is the delay caused by upstream DBA scheduling. Generally, each ONU obtains only one opportunity to send data in one grant period (equals to one frame). In a low-traffic mode, it may take several grant period for one ONU to be granted an opportunity to send data. This causes a scheduling delay of hundreds of microseconds or even greater than a 1 ms. By using fractional frame based burst technology, the OLT may allocate to an ONU, that requires low latency, multiple timeslots for sending data in one grant period. This scheme thereby reducing a scheduling delay by the corresponding times accordingly. For example, if four timeslots are allocated to a low-latency ONU in each grant period (125 µs), the scheduling delay may be reduced to 31 µs, and if 16 timeslots are allocated, the scheduling delay will be reduced to 8 µs. The principle of fractional burst frame is shown in Figure 22.



- One 125us time slot is divided into several smaller sub time slots.
- ONU bandwidth allocation period can be:
  - ✓ 125us / 4 burst = 31us
  - ✓ 125us / 8 burst = 16us

Figure 22: Fractional burst frame in one 125 µs frame

7.1.6.4.4 Cooperative DBA (CO DBA) that combines PON DBA and wireless DBA to reduce latency and buffer between these two segments

CO DBA is used to increase the PON capacity and reduce the latency of the services by tracking the real-time bandwidth requirements of service flows. The first such service type is Low-Layer Split mobile Fronthaul (LLS-FH) with variable traffic and ultra-low latency. Similar mechanism can be used in industry PON scenarios if the OLT has the information of bandwidth requirements before traffic data arrival.

An inherent feature of mobile fronthaul is that the scheduler in a DU may estimate uplink mobile fronthaul traffic load according to uplink bandwidths allocated by the scheduler to different User Equipment (UEs) in upcoming mobile timeslots. The CO DBA may use the same information to adjust the upstream timeslots of the mobile service and the corresponding ONU. The information needs to be transmitted from the DU (Distributed Unit) to the OLT.

Once the OLT receives the information, the CO DBA infers the corresponding serving T-CONT and determines the correct upstream bandwidth allocation for that T-CONT. Then it generates the start and end time for such upstream bandwidth allocation. When a new DBA cycle begins, the new allocation is sent as a bandwidth map. This differs from traditional SR-DBA cycles, which require status reporting before bandwidth allocation can be updated, and the maximum packet buffer latency can be on the order of 1 ms to 2 ms. Compared with SR-DBA, CO DBA has a shorter upstream buffering delay when the ONU waits for sufficient upstream burst bandwidth allocation. CO DBA reduces the buffer latency to tens of microseconds.

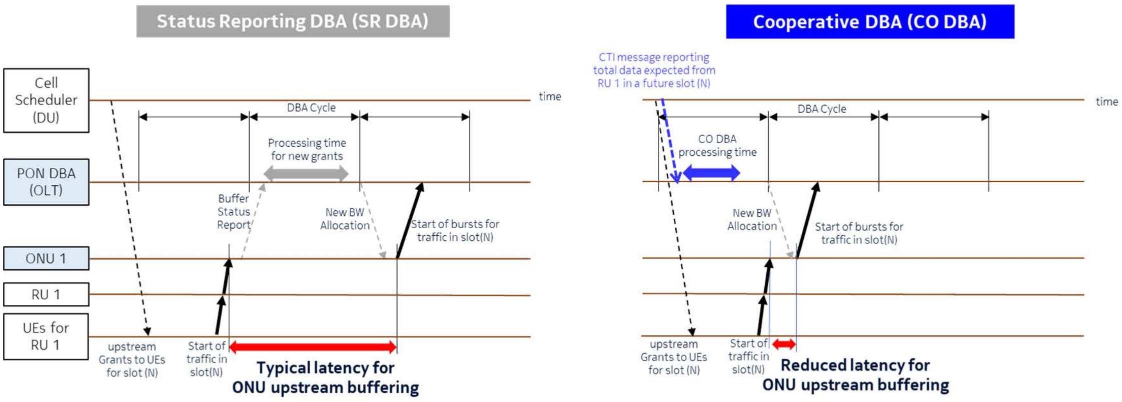

Status Reporting DBA (SR DBA)
Cooperative DBA (CO DBA)
Cell Scheduler (DU)
PON DBA (OLT)
ONU 1
RU 1
UEs for RU 1
time
DBA Cycle
Processing time for new grants
Buffer Status Report
New BW Allocation
Start of bursts for traffic in slot(N)
upstream Grants to UEs for slot (N)
Start of traffic in slot(N)
Typical latency for ONU upstream buffering
CTI message reporting total data expected from RU 1 in a future slot (N)
DBA Cycle
time
CO DBA processing time
New BW Allocation
Start of bursts for traffic in slot(N)
upstream Grants to UEs for slot (N)
Start of traffic in slot(N)
Reduced latency for ONU upstream buffering

Figure 23: Cooperative DBA

7.1.6.4.5 System level optimization such as network slicing and setting industry PON link with fixed bandwidth and high priority

For services that have higher requirements on delay and jitter, a fixed bandwidth can be used to ensure that the ONU can send data only once within a grant period, thereby reducing the delay. In a single grant period, data traffic of a fixed type is placed at a fixed position at the front of the current grant period to reduce jitter.

The hard slicing technology allocates fixed and independent bandwidth, priority, and forwarding queue resources based on PON ports or ONUs for services with higher latency and jitter requirements. This ensures that the resources of the forwarding path between the ONU and the OLT are fixed and cannot be interfered with by other services. This reduces the network delay and jitter.

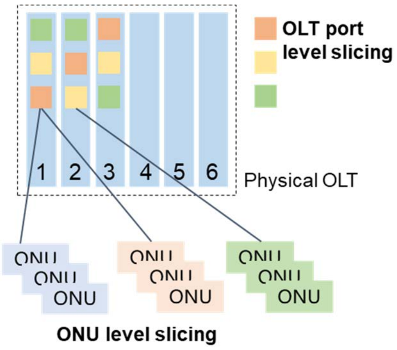


Figure 24: OLT port and ONU slicing

7.1.6.4.6 E2E latency/jitter optimization based on cooperation between PON and industrial devices

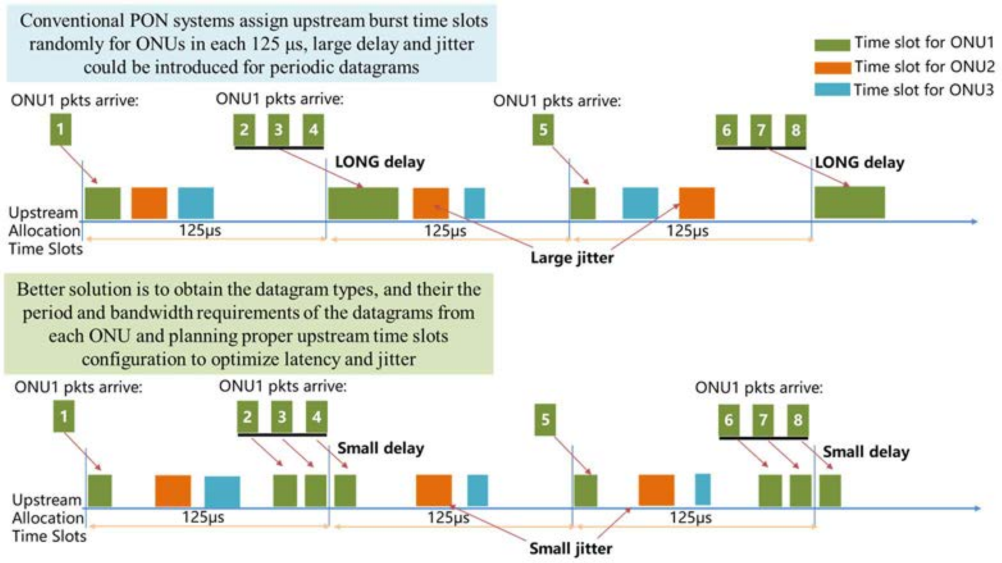
In the upstream direction, PON systems (e.g. GPON, XG(S)PON) assign upstream burst timeslots randomly to each ONU every 125 µs defined in related ITU-T PON standards. This kind of randomness makes it impossible to match the periodic nature of data in the industrial scenarios. Hence, PON systems cannot guarantee deterministic transmission capability.

On the other hand, there is strong demand from the industrial customers to optimize the upstream latency and jitter performance of the PON system. It is important to provide a better deterministic network solution for the industrial customers.

For the network within a factory workshop, in most cases, the network topology is fixed, once the network is deployed and the workshop is running.

Hence, for the industrial production elements (machines, devices for manufacturing products etc.) connected to industrial ONUs, the number and type of them would be fixed for the majority of the time. The data transmitted between the industrial production elements and upper layer manufacturing management systems usually has relatively fixed transmission period and datagram size.

These aforementioned conditions of the network dataflow characteristics within the workshops can be utilized to orchestrate the upstream timeslots for each ONU based on the periodic nature of the dataflows. By utilizing these characteristics, the E2E latency and jitter performance can be optimized and achieve deterministic network performance.



Conventional PON systems assign upstream burst time slots randomly for ONUs in each 125 μs, large delay and jitter could be introduced for periodic datagrams

Better solution is to obtain the datagram types, and their the period and bandwidth requirements of the datagrams from each ONU and planning proper upstream time slots configuration to optimize latency and jitter

Figure 25: Illustration and comparison of conventional upstream burst time slots assignment (above) and proposed solution (below) to improve deterministic network performance

With the help of ONU's localized computing capability, it is possible to achieve better latency and jitter performance in the industrial PON system. The ONU can monitor and analyse the characteristics of the datagrams passing through the ONU connected to industrial production elements, and report the characteristics parameters to the OLT. Such characteristics parameters can be processed by the OLT to adjust the burst allocations in the upstream transmission for certain ONUs.

According to ITU-T PON recommendations, ONUs' upstream transmission follows the received arrangement of the burst allocations instructed by the OLT. A typical burst allocation includes the 'StartTime' as defined in Recommendation ITU-T G.987.3 [i.30], etc., which can be used by the OLT to control the interval between the adjacent burst allocations when arranging the burst allocations.

Hence the deterministic performance of the industrial PON system can be improved by matching the above arrangement to datagrams and shortening the waiting time inside the ONU. The optimization process is realized by specific algorithms within the edge computing module in the PON system. It can provide an automatic way to optimize the deterministic performance without human intervention.

A Summary and comparison of the five latency/jitter optimization methods are tabulated in Table 4.

Table 4: Comparison of the five latency/jitter optimization methods

Approaches	Pros	Cons
PON link latency optimization by dual wavelengths	Upstream time slots for registering etc. are eliminated in the data transmission wavelength channel, latency/jitter can be reduced	Currently non-standard, and additional wavelength channel increases the total hardware cost
PON link latency optimization by means of fractional frame based burst	Being standardizing in HSP systems Latency/jitter can be reduced significantly No additional requirements on Legacy ONUs	Compromise between latency/jitter performance and total throughput of the PON port
Cooperative DBA (CO DBA) that combines PON DBA and wireless DBA to reduce latency and buffer between these two segments	Latency/jitter can be reduced significantly	Additional requirements on the industrial network elements
System level optimization such as network slicing and setting industry PON link with fixed bandwidth and high priority	No additional requirements on Legacy ONUs	Relatedly limited latency/jitter optimization
E2E latency/jitter optimization based on cooperation between PON and industrial devices	Latency/jitter can be reduced significantly	Additional requirements on the ONUs and industrial network elements

7.1.7 Evolution to higher speed PON

7.1.7.1 Evolution of service and application drivers

For industry application, there are quite different scenarios and use cases, so the bandwidth requirements for an Industrial PON system can be quite different. For traditional industry field network, the latency and jitter are quite important while the bandwidth demand is low. However, for some new video-based industry application, the bandwidth requirement is also important.

1) Video surveillance:

Video surveillance is widely used in industry scenario for the security of the factory. As video surveillance applications continue to expand, a large number of video surveillance sites will impose capacity expansion which may introduce pressure on the surveillance backhaul network deployment and O&M. The bandwidth requirement of video surveillance depends on the definition of the video. For 720P and 1080P, the typical bandwidth requirements are 20 Mbit/s and 40 Mbit/s respectively for one site. The requirement is even higher for 4K or 8K video. Table 5 shows the bandwidth requirements of 4K and 8K video.

Table 5: Bandwidth requirements of 4K and 8K video

Service type	Bandwidth	Average latency	Jitter	Package loss rate
4K video	> 54 Mbit/s	/	/	< 1,0E-5
8K video	>150 Mbit/s	/	/	< 1,0E-6

2) Machine vision:

Machine vision systems are developed through machine vision products (i.e. image capture device, CMOS and CCD) converting the captured object into an image signal, transmitting the image signal to a dedicated image processing system, obtaining the shape information of the captured object, and converting it into a digitized signal according to pixel distribution, brightness, colour, and other information. The image system can perform various operations based on these signals to extract the features of the target. The bandwidth requirement of machine vision depends on the number of images.

3) VR-based virtual manufacturing:

Currently, all manufacturing procedures are carried out step by step in sequence. From design to prototype, the front-end team needs to clearly explain and communicate the design intent to the back-end team. The back-end team needs to continuously provide feedback to the front-end design team to accurately control the project progress and direction. But the limitations of distance, time, and the current means of communication do not allow this kind of deep and efficient project collaboration. When the concept of virtual manufacturing is applied, the situation change dramatically. All stakeholders in the entire manufacturing chain can be involved in the project from the start. From the beginning of the virtual design, everyone can raise issues they will face in their own procedures, and communicate with non-engineers to understand their difficulties and provide better solutions. Through such cooperation and communication, the R&D and launch cycle of the entire product will be greatly shortened.

VR-based virtual manufacturing needs extremely high bandwidth and low latency. Table 6 shows the network performance requirements for VR service with different classes.

Table 6: Performance Requirements for VR service

Class	Class 1	Class 2	Class 3	Class 4
Video resolution	2-3 K	4K	8K	16K~
Average bitrate	≥ 40 Mbit/s	≥ 65 Mbit/s	≥ 270 Mbit/s	≥ 770 Mbit/s
Bandwidth requirement	≥ 80 Mbit/s	≥ 130 Mbit/s	≥ 540 Mbit/s	≥ 1,5 Gbit/s
E2E round-trip time (RTT)	≤ 20 ms	≤ 20 ms	≤ 10 ms	≤ 8 ms
Jitter tolerance	≤ 15 ms	≤ 15 ms	≤ 10 ms	≤ 7 ms
packet loss tolerance	$\leq 10^{-5}$	$\leq 10^{-5}$	$\leq 5\times10^{-6}$	$\leq 1\times10^{-6}$

According to the performance requirements, it is clear that both the bandwidth and latency are important for these industrial applications. For industrial PON, one OLT port may be shared by up to 64 (or 128) sites, and the services of all sites may be simultaneous. For example, if there are 64 sites with 8K video surveillance, the total bandwidth requirements will be 150 Mbit/s × 64 = 9,6 Gbit/s which exceeds the capability of 10G PON (as there are about 15 % FEC overhead for 10G PON). So new PON technology is needed to be introduced for industry application in the future.

7.1.7.2 Technology evolution

ITU-T SG15 decided to select 50 Gbit/s PON as the next generation of PON system. The recommendations series include G.9804.1 [i.31] (Higher Speed Passive Optical Networks: Requirements), G.9804.2 [i.32] (Higher Speed Passive Optical Networks: Common Transmission Convergence (TC) Layer), G.9804.3 [i.33] (Higher Speed Passive Optical Networks: 50G PMD: Physical Media Dependent (PMD) Layer Specification).

There is a strong need that 50G PON is capable of coexist with XG(S) PON or GPON. 50G PON provides various upgrade paths for legacy PON generations, such as GPON, XG-PON, XGS–PON, to evolve to higher system capabilities. Specific coexistence and upgrade evolution paths are shown in Figure 26. XG(S)–PON systems can be upgraded to 50G PON smoothly and achieve about 5 times capacity increase and low latency features. In certain cases, 10G-EPON can be also co-existed with 50G PON.

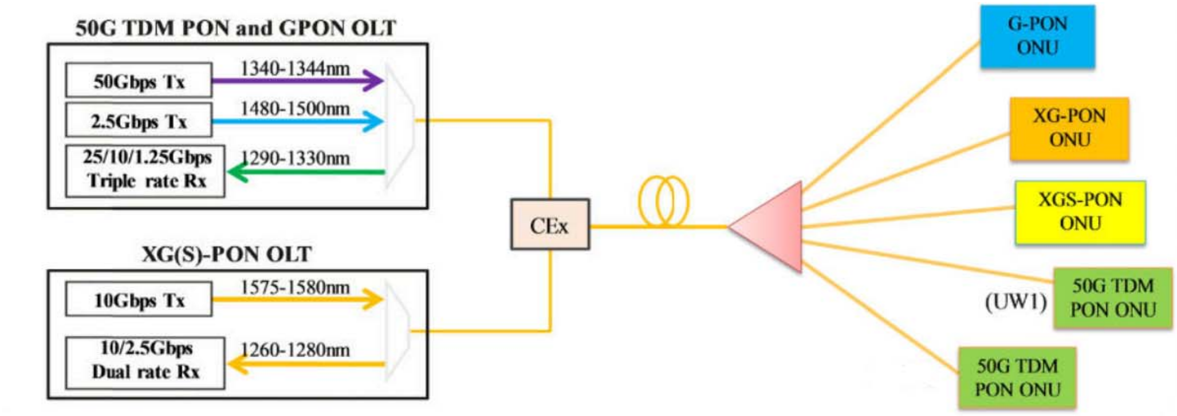


Figure 26: The co-existence of 50G TDM PON and GPON/XG(S)-PON system

Industrial scenarios are different from conventional home broadband, the demand on network bandwidth for upstream is much greater than that for downstream. For example, machine vision and video surveillance in many production lines are pure upstream traffic. For these applications, the high bandwidth and low latency requirements are mainly in the upstream, while the requirements in the downstream are much lower. It is different from traditional FTTx application whose downstream bandwidth is greater than upstream bandwidth. Currently, XGS PON is used to meet the demands of high upstream bandwidth. In the future, the network can be upgraded to symmetric 50G PON to satisfy the increased bandwidth demands of such applications.

7.1.8 TSN over PON

7.1.8.1 Background of TSN-enabled PON

Along with the evolution and upgrading of industrial production and operation system, driven by digitalization using information for smart decisions, the industrial networks are required to support interoperability, real-time operation, and reliability. In legacy Ethernet, due to its statistical multiplexing-based technology, traffic delays are accumulated hop-by-hop and packet delay variation uncertainty increases accordingly. In addition, hierarchical scheduling introduces weak isolation and cannot meet the requirements of industrial control networks. To alleviate these shortcomings, TSN (Time Sensitive Network) technology emerged. TSN complies with the standard Ethernet architecture and has precise traffic scheduling capability to ensure high-quality transmission of multiple service flows within the same network with both technical and cost advantages. It has become an important evolution direction for bearer network technologies in various fields, such as audio and video transmission, industry, mobile xHaul, and in-vehicle networks. However, TSN technology based on copper-wire Ethernet is limited by network layers and transmission distance, and may require multiple hops for E2E networking. In addition, TSN technology needs to operate under SDN controller, which adds complexity to network planning and configuration, and severely limits the adoption of the Ethernet TSN technology. Currently, factory workshop control networks are generally deployed in lightly loaded or dedicated networks in the industry. The network utilization is low and it is difficult to deploy and maintain multiple networks.

In general, a TSN-enabled PON network could take advantage of the PON network technology, enterprise-grade PON network management and native time synchronization. A TSN-enabled PON network could potentially build a simplified deterministic and low-latency industrial PON network.

7.1.8.2 TSN-related technologies which may be used in industrial PON system

7.1.8.2.1 Overview

A series of technologies are defined in IEEE TSN standards, such as IEEE 802.1Qbv [i.34], IEEE 802.1Qch [i.35], TTE (Time Triggered Ethernet) and jumbo packet fragmentation. The following sub-clauses gives a brief introduction to these functions that may be implemented in industrial PON system.

7.1.8.2.2 Time-Triggered Ethernet (TTE)

A timestamp is added to each packet and transmission of each packet is controlled by a timetable. Each packet is aware of its transmit time. The transmit time of each packet is separated on the packet egress side to ensure that packet delay and jitter meets the corresponding requirements. Figure 28 gives an example of TTE.

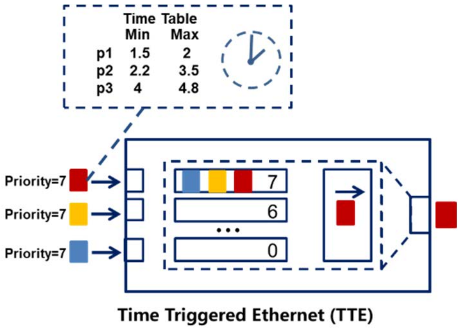


Figure 28: An example of TTE

7.1.8.2.3 Frame preemption (IEEE 802.1Qbu/IEEE 802.3br)

In order to achieve low latency for high-priority data, preemption/interruption of low-priority data packets transmission is allowed. Low-priority packets are either blocked or fragmented and transmitted later. The following bullets and Figure 29 explains the process in brief:

- While one or more-time sensitive frames are transmitted, transmission of non-time sensitive frames can be paused.

- IEEE 802.1Qbu (frame preemption) [i.37] and IEEE 802.3br [i.38] (fast traffic interspersion) defines the frame preemption function.
    - IEEE 802.1Qbu defines preemption interfaces and modules for transport devices. In frame preemption, delay-sensitive frames are called express frames, and other frames are called low-speed frames or preemptable frames.
    - IEEE 802.3br [i.38] introduces the MAC combination sublayer, and defines specific procedures of segmentation, segments restoration, and verification of frame preemption.

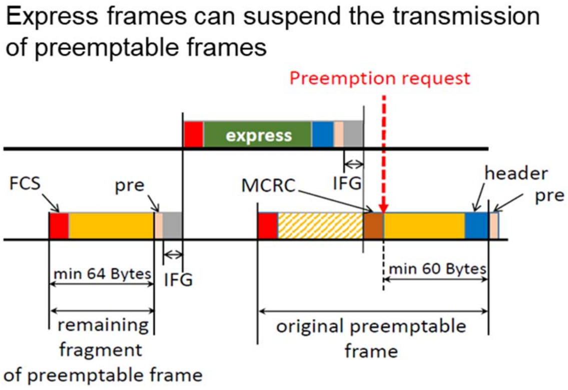

Express frames can suspend the transmission of preemptable frames
Preemption request
express
FCS
pre
MCRC
IFG
header
pre
min 64 Bytes
IFG
min 60 Bytes
remaining fragment of preemptable frame
original preemptable frame

Figure 29: Illustration of preemption

7.1.8.2.4 Proactive fragmentation of jumbo packets

The Ethernet channel is separated into two channels: one is a high-priority channel and the other one is a low-priority channel. Jumbo Ethernet packets in the low-priority channel are fragmented to achieve low packet delay and low jitter on the high-priority channel (see Figure 30).

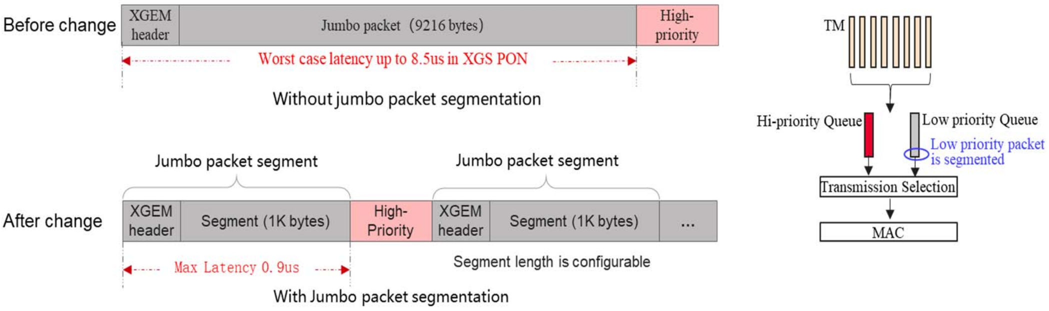


Figure 30: Segmentation of jumbo ETH packet

7.1.8.2.5 Enhancements to Traffic Scheduling (IEEE 802.1Qbv)

Ethernet data traffic are classified into different types, each of which is reserved for a specific time to access the network, thus class-specific protection "channels" are created. Each queue has a transmission gating procedure (each scheduled queue is associated to scheduling period time value). By configuring the queue transmission gating table to control the transmission of queues, each queue can then be isolated from others in time.

7.1.8.2.6 Cyclic Queuing and Forwarding (IEEE 802.1Qch)

In CQF, E2E latency is averagely divided by CQF to each hop, by controlling the transmitting time of each packet hop by hop, end-to-end latency boundary can be guaranteed. An equipment which implements CQF functionality needs to set two queues Q0 and Q1 which are controlled by a time gate for time-sensitive frames at the egress. In even timeslots Q0 buffers data frames received from the ingress, meanwhile Q1 transmits data packets buffeted during the previous odd timeslot. In odd timeslots the two queues operate in reverse, Q1 receives and buffers data packets while Q0 transmits buffered data in the previous time slot.

7.1.8.3 Integration of TSN features to enable TSN in an industrial PON system

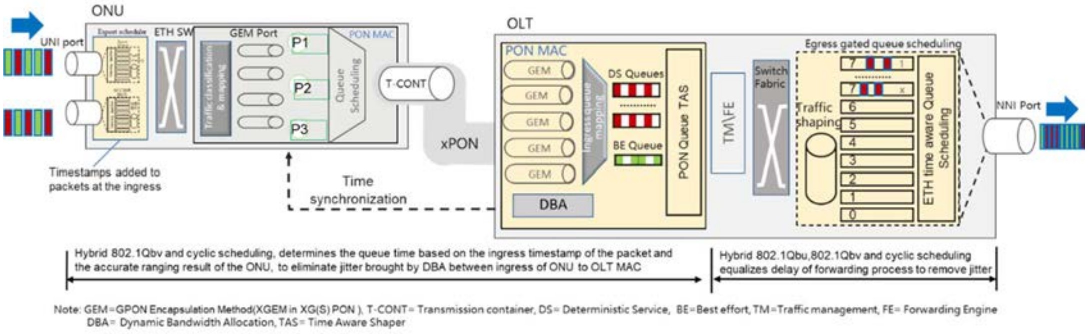
7.1.8.3.1 Overview

The OLT and ONUs are considered logically integrated. The forwarding plane uses TSN technologies such as TSN IEEE 802.1Qa/b [i.23] and [i.24], IEEE 802.1Qbu [i.37], IEEE 802.1Qch [i.35], TTE (Time Triggered Ethernet), and jumbo packet fragmentation. This is combined with low-delay and low jitter PON technologies (see clause 7.1.6) to implement segment-based deterministic jitter, and achieves end-to-end deterministic latency.

7.1.8.3.2 Upstream packet transmission over PON

7.1.8.3.2.1 Upstream data process in TSN enabled PON

IEEE 802.1Qbu [i.37] plus IEEE 802.1Qbv [i.34] plus cyclic scheduling hybrid mode is implemented to achieve the required delay jitter. Figure 31 illustrates the upstream data packet process for TSN enabled PON.


ONU
UNI port
ETH SW
GEM Port
P1
P2
P3
PON MAC
Traffic classification & mapping
Queue Scheduling
T-CONT
xPON
Timestamps added to packets at the ingress
Time synchronization
OLT
PON MAC
GEM
GEM
GEM
GEM
GEM
Ingress queue mapping
DS Queues
BE Queue
DBA
PON Queue TAS
TM\FE
Switch Fabric
Egress gated queue scheduling
Traffic shaping
7
7
6
5
4
3
2
1
0
ETH time aware Queue Scheduling
NNI Port
Hybrid 802.1Qbv and cyclic scheduling, determines the queue time based on the ingress timestamp of the packet and the accurate ranging result of the ONU, to eliminate jitter brought by DBA between ingress of ONU to OLT MAC
Hybrid 802.1Qbu,802.1Qbv and cyclic scheduling equalizes delay of forwarding process to remove jitter

Note: GEM=GPON Encapsulation Method(XGEM in XG(S) PON), T-CONT= Transmission container, DS= Deterministic Service, BE=Best effort, TM=Traffic management, FE= Forwarding Engine
DBA= Dynamic Bandwidth Allocation, TAS= Time Aware Shaper

Figure 31: Upstream data packets processing in TSN enabled PON

7.1.8.3.2.2 Segment from ONU ingress to OLT upstream PON MAC

- IEEE 802.1Qbv [i.34] plus cyclic scheduling hybrid mode may eliminate the packet jitter caused by the DBA allocation period, and may determine the queue time based on each ingress packet timestamp and the accurate ranging result of corresponding ONU.
- Multiple groups were created for deterministic and Best Effort (BE) service flows. Each service flow is mapped into a corresponding group accordingly.
- The serialized flow queue determines the time of each packet's exit from the queue based on the ONU ranging and receiving timestamp, to perform QBV scheduling.
- BE (Best Effort) packets are scheduled when queues are in idle.

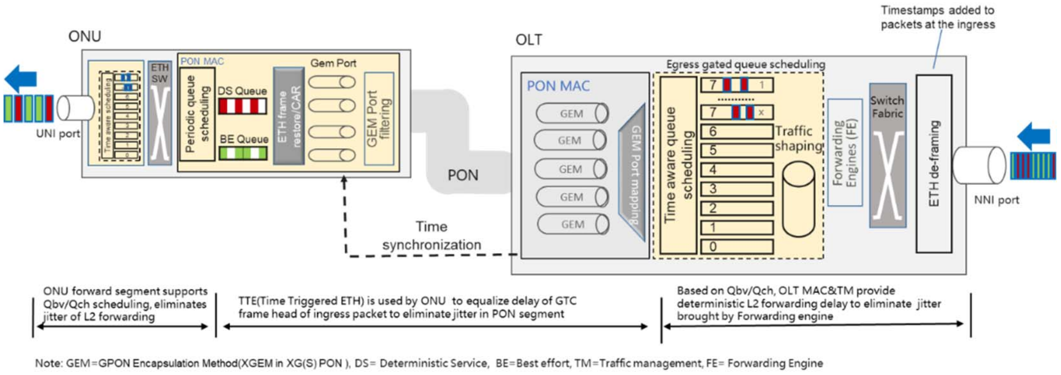
7.1.8.3.2.3 Segment from OLT upstream PON MAC to OLT uplink ETH

The hybrid mode of IEEE 802.1Qbu [i.37] plus IEEE 802.1Qbv [i.34] plus cyclic scheduling manages the packet jitter caused by the forwarding processing and eliminates packet jitter by delay equalization.

7.1.8.3.3 Downstream packet transmission over PON

7.1.8.3.3.1 Downstream data process in TSN enabled PON

TTE scheduling eliminates packet jitter in PON downstream and achieve an E2E packet jitter of less than 1 µs. Figure 32 shows the mapping and bearer of downstream data packets.


ONU
UNI port
Time aware scheduling
ETH SW
PON MAC
Periodic queue scheduling
DS Queue
BE Queue
ETH frame restore/CAR
Gem Port
GEM Port filtering
PON
Time synchronization
OLT
PON MAC
GEM
GEM
GEM
GEM
GEM
GEM Port mapping
Egress gated queue scheduling
Time aware queue scheduling
7
1
7
x
6
5
4
3
2
1
0
Traffic shaping
Forwarding Engines (FE)
Switch Fabric
ETH de-framing
Timestamps added to packets at the ingress
NNI port
ONU forward segment supports Qbv/Qch scheduling, eliminates jitter of L2 forwarding
TTE(Time Triggered ETH) is used by ONU to equalize delay of GTC frame head of ingress packet to eliminate jitter in PON segment
Based on Qbv/Qch, OLT MAC&TM provide deterministic L2 forwarding delay to eliminate jitter brought by Forwarding engine

Note: GEM=GPON Encapsulation Method(XGEM in XG(S) PON), DS= Deterministic Service, BE=Best effort, TM=Traffic management, FE= Forwarding Engine

Figure 32: Downstream data packets processing in TSN enabled PON

7.1.8.3.3.2 From OLT uplink interface (entry of OLT in downstream) to OLT downstream PON MAC

- Maximum delay caused by GTC (GPON Transmission Convergence) frames: 7 µs for GPON and 2 µs for XGS-PON.
- The cyclic scheduling queue period is designed to meet delay jitter requirement. The cyclic scheduling period eliminates the downstream jitter.
- The deterministic packets are scheduled at the egress according to the timestamp and ONU ranging result.
- BE queues are scheduled when deterministic packet queues are idle.

7.1.8.3.3.3 Segment of PON Downstream

- TTE scheduling on the ONU is introduced to equalize packet delay and to eliminate the PON link packet jitter caused by the GTC frame header.

7.1.8.3.3.4 Segment of ONU downstream forwarding

- IEEE 802.1Qbv [i.34]/IEEE 802.1Qch [i.35] scheduling are used to eliminate layer 2 forwarding packet delay jitter.

IEEE 802.1Qbv [i.34]/IEEE 802.1Qch [i.35] cyclic queue scheduling is introduced to the OLT PON MAC & TM (Traffic Management) to provide deterministic layer 2 packet forwarding delay and eliminates packet forwarding jitter caused by the forwarding engine.

7.1.8.4 Summary

This clause introduced TSN features, which are defined in IEEE standards and how these features can be adapted for a PON system to reduce latency, eliminate packet jitter and provide deterministic network latency.

7.2 ODN

7.2.1 Network topology

7.2.1.1 Application scenarios

In industrial scenarios, there are various network elements to be connected to the industrial PON system, such as the machines in the industrial field level scenarios, the computers in the office network scenarios, and cameras in the sensor & surveillance scenarios.

The major network topology of the industrial PON system is the conventional tree topology, in which even optical power splitters are used, as shown in Figure 33.

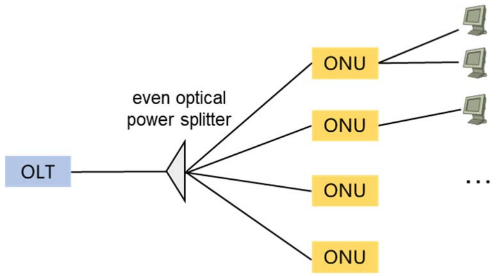


Figure 33: Illustration of the tree topology in industrial scenarios

In the industrial field level scenario, the detail distribution of the network elements depends on the layout of the factory production lines and/or the workflow of the actual manufacturing procedures. For certain use case, as shown in Figure 34, the span of the machines in the longitudinal direction can be in the order of hundred-metres, therefore the tree topology may not be a good option to connect these machines, while the chain topology based on uneven optical power splitting provides alternative an option for this scenario. The ONUs in the chain topology are connected in the cascade manner, and the uneven optical power splitters are used instead of the even optical power splitters.

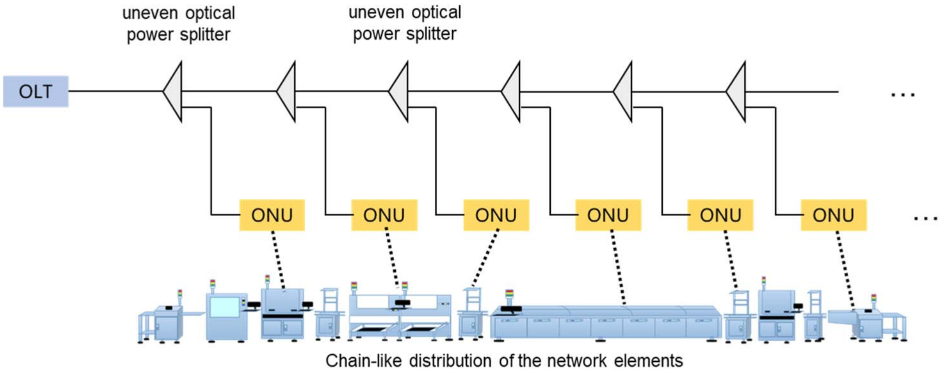


Figure 34: illustration of the chain topology in in industrial scenarios

7.2.1.2 ODN System architecture

To meet the various network topological requirements, there are two network main topologies used in industrial PON system, which are the tree topology and the chain topology, as shown in Figure 35 and Figure 36 respectively.

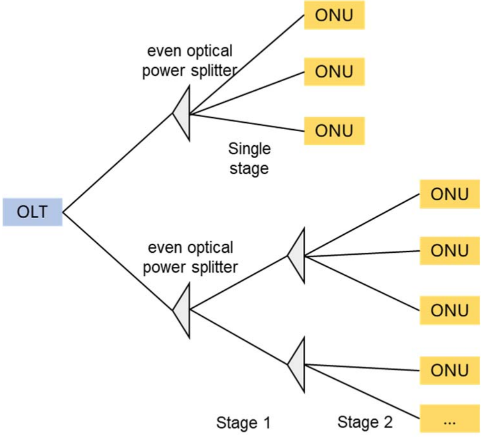


Figure 35: Industrial PON with tree topology, both the single-stage and dual-stage structures are shown

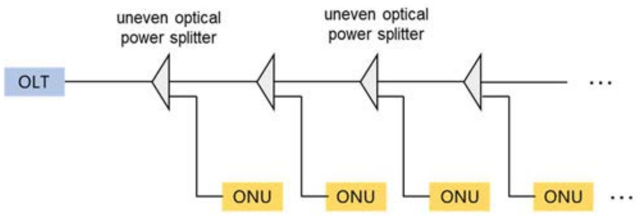


Figure 36: Industrial PON with chain topology

The tree and chain topologies can both be enhanced with dual-link protection switching scheme, to provide high network reliabilities required by the industrial applications.

One typical dual-link protection scheme is the hand-in-hand dual-OLT with dual-link protection. A typical architecture of tree and chain topologies are shown in Figure 37, and detailed analysis of different network protection switch schemes can be found in clause 7.2.2 of the present document.

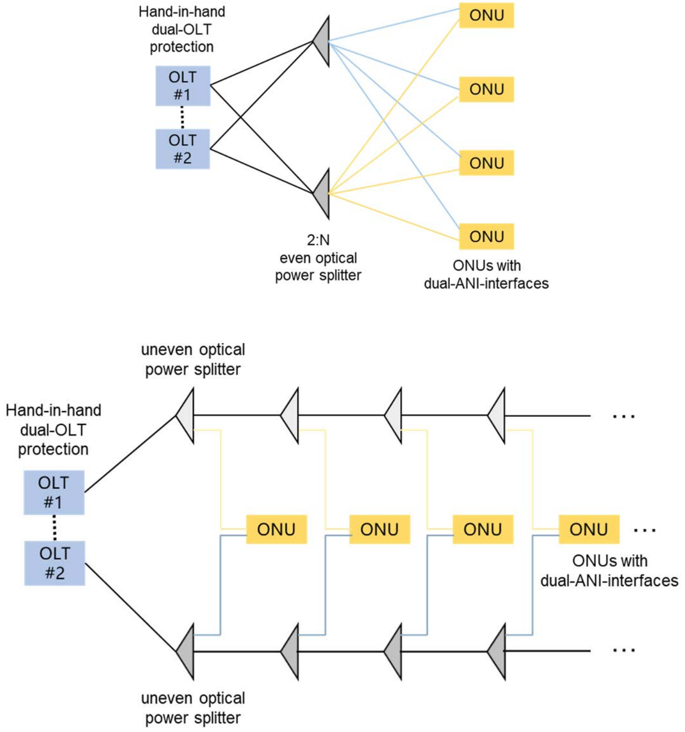

Hand-in-hand dual-OLT protection
OLT #1
OLT #2
ONU
ONU
ONU
ONU
2:N even optical power splitter
ONUs with dual-ANI-interfaces
uneven optical power splitter
Hand-in-hand dual-OLT protection
OLT #1
OLT #2
...
ONU
ONU
ONU
ONU
...
ONUs with dual-ANI-interfaces
...
uneven optical power splitter

Figure 37: Tree (top) and chain (bottom) topologies with enhanced protection schemes

7.2.2 Network resilience

7.2.2.1 Type C protection

Compared with the home scenarios, the industrial scenarios have more stringent requirements on network reliability, which require full redundancy protection for service traffic forwarding paths to prevent network faults caused by ODN degradation or queue congestion. In traditional industrial environments, ring topology networks are the main solution to provide service protection. Therefore, industrial PON needs to support ring topologies for seamless protection. In Recommendation ITU-T G.984.1 [i.5] Type-C is defined to provide network resilience capability based on dual fibre ODN, this can be configured as a ring topology as shown in Figure 38.

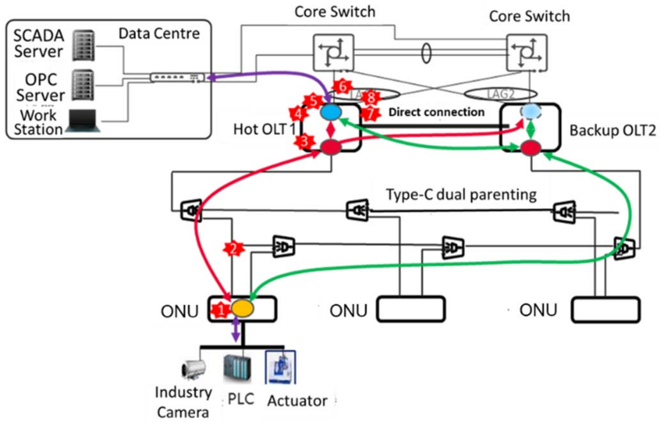


Figure 38: Type C protection for Industrial PON

An Industry PON network needs to provide protection for the following failures:

1) ONU optical interface failure.

2) Degradation of ODN link between ONU and OLT, including PON line fault alarms: LOSi (Loss Of Signal for ONUi), upstream SDi (Signal Degraded of ONUi) and SFi (Signal Fail of ONUi) alarms, downstream SDi and SFi alarms, and TF (Transmitter Failure) alarms.

3) Temporary packet loss in the traffic forwarding path (e.g. queue overflow, packet frame error).

4) OLT line card hardware failure.

5) OLT control board failure.

6) OLT uplink failure.

7) OLT uplink LAG (Link Aggregation) failure.

8) OLT power outage.

Type C protection can achieve overall network availability of up to 99,99 %. The switchover success rate of type C dual-homing protection is 99,99 %. The ONU does not go offline during the switchover, and the service interruption duration is about 100 ms depending on the service type.

7.2.2.2 Rogue ONU detection and isolation

A rogue ONU refers to an ONU whose optical transmitter is faulty. In this case, the ONU upstream signal does not comply with the pre-allocated timeslot in the PON system, thereby interfering with other ONUs in the same network, and causing an upstream data transmission failure for the entire PON system.

To reduce the impact of rogue ONUs on the industrial PON network, the ONU protection capability needs to be improved in the industrial environments and use redundant design to ensure service continuity when a fault occurs. In addition, big data is used to provide fault prediction capabilities.

1) Enhancing the ONU self-regulation function:

The ONU detects the launch power of the optical module light source in real time and compares it with the light source enable signal of the MAC electronic device. If a mismatch occurs, the ONU automatically shuts down the optical module light source. Therefore, fault tolerance is enhanced.

2) Supporting IP68 waterproof level of the ONU key components:

In some severe situation, for example, when the ONU is water damaged or eroded by water vapour, a hardware fault may lead to a rogue ONU. IP68 waterproofing is applied to key components and modules to effectively reduce the probability of rogue ONU fault being triggered.

3) Multipath binding:

The combination of type C protection and dual-wavelength pair per fibre provides upstream traffic up to four OLT ports. When an ONU port goes rogued and remaining ports are functioning normally, the services on all the ONUs are switched to an alternative OLT port with either another wavelength pair or fibre, ensuring higher availability of the services.

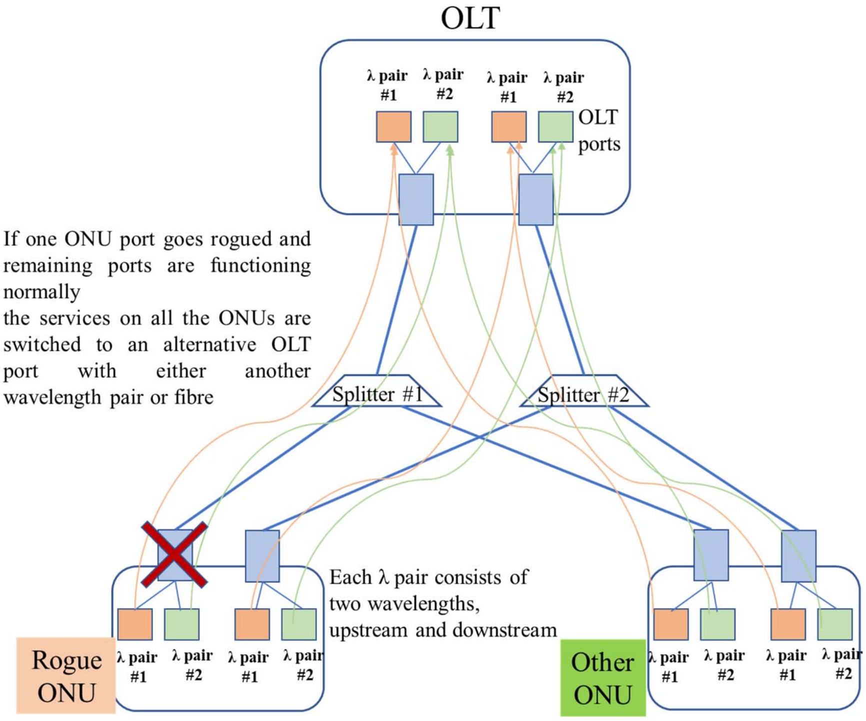

OLT
λ pair #1
λ pair #2
λ pair #1
λ pair #2
OLT ports
If one ONU port goes rogued and remaining ports are functioning normally
the services on all the ONUs are switched to an alternative OLT port with either another wavelength pair or fibre
Splitter #1
Splitter #2
Each λ pair consists of two wavelengths, upstream and downstream
Rogue ONU
λ pair #1
λ pair #2
λ pair #1
λ pair #2
Other ONU
λ pair #1
λ pair #2
λ pair #1
λ pair #2

Figure 39: Multipath binding with Type C protection and dual-wavelength pair per fibre

4) Efficient OLT detection and isolation:

The rogue ONU detection function is optimized based on various rogue ONU fault models. The rogue ONU detection function supports continuous-transmission detection and random-transmission detection that enables fast fault detection and troubleshooting.

5) Prediction and detection based on AI and big data analysis:

The OLT can predict and detect rogue ONUs based on AI and big data analysis. The OLT collects key information about the ONU's optical modules, line bit error data, and status change events, and analysis the terminal behaviour patterns and data correlations using big data or machine learning methods.

7.3 PON management system for industrial scenarios

7.3.1 Comparison to traditional PON management systems

Industrial customers have many specific function requirements on the network, which are very different from public access network users, and they also impose strict limitations on the investment and human resource cost aspects of the network deployment. Industrial PON can fulfil the above requirements and can be an attractive bearing network solution for the wired connectivity within the factory.

Current existing PON management systems are designed for very large number of users in the operator's public access networks, these all-in-one complex management systems impose very high hardware resource requirements. A large proportion of system modules and functions are dedicated for professional public access network management and configuration, which may not be needed in the industrial scenario. On the other hand, factories need many industrial specific functions which may not be fulfil by the existing PON management system. In addition it may be very hard and/or expensive for the factories to find professional network administrators capable of handling this complex management systems.

The main issues and concerns for directly deploying the current existing PON management systems in the industrial scenarios are listed below:

1) Main functions of the current existing PON management systems are dedicated designs for operator's public access networks.

2) These systems have comprehensive functions for the PON network operation and management, however, a large part of which may not be suitable for the industrial scenarios. Hence the industrial customers have to pay for the functions and modules they do not need.

3) These all-in-one systems put very high hardware resource requirements on industrial customers, which have to pay for the hardware resources.

4) On the other aspect, there are many industrial-related functions needed by industrial customers, which are still missing in these systems, such as functions and APIs for neighbour systems in factories, and specially optimized user interfaces for the users with less networking knowledge.

5) Industrial customers need to hire professional network administrators in order to operate these systems, which increase the human resource cost.

7.3.2 Function recommendations

Several surveys have been carried out focusing on industrial customers, on the functional recommendations of the industrial PON management systems. Below are the industrial customer's feedbacks on this issue:

1) The industrial PON management systems need to develop industrial specific modules and functions, in order to fulfil the needs of the industrial customers. Main functions include connecting with the neighbouring systems in the factories, and optimize the user interfaces, analysing and giving an overview of the network status, needs to be considered.

2) The modules within the system need to be loosely coupled, the versions of the management system needs to be tailored for different end users, and industrial customers need not pay for the functions and corresponding hardware resources that are not needed.

3) The operation of this management system needs to be easy, so that no dedicated professional networks administrators are needed, hence no additional cost on the human resources side.

4) There needs to be network status monitoring, analysis and fault diagnosis functions based on artificial intelligence technologies, which could aid the user to operate and manage the industrial PON system.

Based on the industrial customer feedbacks and recommendations, the industrial PON management systems needs to support the following capabilities.

1) A third party, independent management system that is de-coupled from PON devices of different vendors.

2) The management system could be customized and tailored, to provide the basic and essential network OAM functions and industrial specific functions required by the industrial customers.

3) The management system needs to provide an open APIs to other related systems within the factories, and capable of running functional modules for industrial protocol interpretation and conversion.

7.3.3 Typical Industrial PON management system architecture

The typical system architecture of industrial PON management system can be found in Figure 11 of clause 6.3.2.

7.3.4 Key function and modules

The key functions and modules of a typical industrial PON management system are shown in Figure 39.

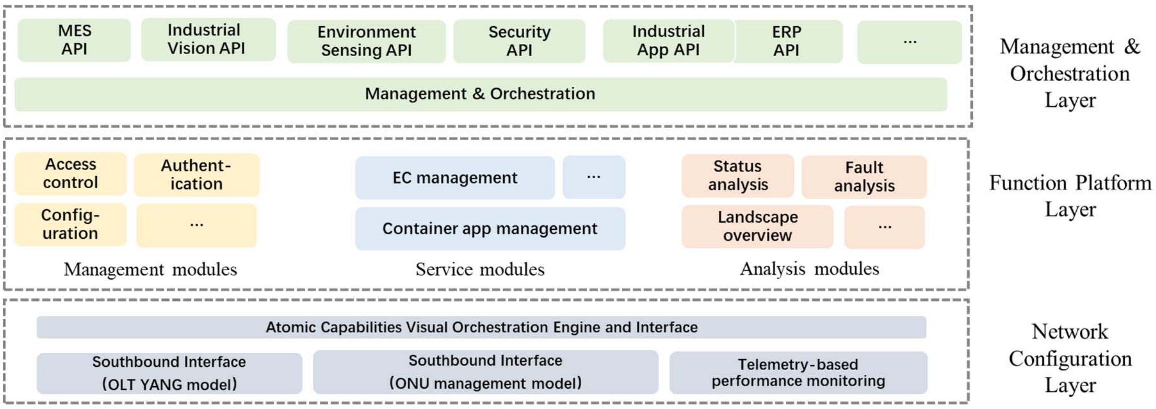


Figure 40: Key management system function overview

According to the typical system architecture, the industrial PON management system can be further divided into three layers:

1) Management & Orchestration Layer:

- This layer provides interfaces and communications to other neighbouring systems within the factory intranet, and performs the orchestration of different interfaces and related network configuration tasks.

2) Function Platform Layer:

- This layer provides various functions for realizing all the network OAM functions for the industrial users. And this layer can be further divided into three types of modules listed below:

  a) Management modules, to provide fundamental network OAM functions, such as ONU authentications, configuration distribution, warning message collection and fault reporting, etc.

  b) Service modules, to provide functions other than fundamental network OAM functions, such as configuration and monitoring of the edge computing platform on the OLT side, and container runtime environment in the PON systems.

  c) Analysis modules, mainly focus on analysis and statistical overview functions, including artificial intelligent technologies for analysis of the network status, fault locating, key network performance statistics and graphic overview generation, etc.

3) Network Configuration Layer:

- This layer can be divided into two types of modules listed below:

  a) Southbound interface modules, these modules provide southbound interfaces towards underlying PON devices. The standard and universal NETCONF/YANG schemes are used instead of proprietary ones from diverse vendors.

  b) Telemetry modules, realizing high precision and real-time performance monitoring of underlying PON devices based on telemetry schemes.

7.4 Industrial environment adaptation

7.4.1 Overview

Conventional PON systems deployed in the public access network, would not be require additional environmental adaptation capabilities, as these systems are located in very friendly ambient conditions (OLTs are deployed in the central offices and ONUs are placed in the indoor environments).

However, in the industrial scenarios, while the OLTs are still deployed in air-conditioned factory data centres, the ONUs may face very harsh working environmental conditions [i.9]. Typical industrial working scenarios for ONUs are listed below:

- In metallurgy industry scenario, ONUs are deployed in the workshops with very high ambient temperature.
- In outdoor video surveillance scenario, ONUs need to be capable of working over very wide temperature ranges.
- In outdoor video surveillance scenario, ONUs need to support certain water-proof level requirements.
- In some mining scenario, ONUs need to support certain dust-proof level requirements.
- In some regions, ONUs need to support operating under high humidity environment.
- In welding scenario, ONUs need to support certain EMC requirements.

Key recommendations on the environmental aspects for industrial PON ONUs are defined below. These recommendations are addressed independently, as the combination of these recommendations would further fragment the ONU vendor's product portfolio [i.14].

Industrial customers, need to further refine the ONU product list based on their specific needs on these environmental aspects.

7.4.2 Temperature

Industrial PON OLTs are deployed in air-conditioned factory datacentres, the operating conditions are similar to conventional public access networks, and thus there are no additional environmental recommendations for OLTs.

For the ONUs in the industrial scenarios, the working temperature range recommendations will differ depending on the detailed scenarios. For the welding scenario, upper limit as high as 80 °C may be required, while the lower limit may not exceed 0°C if the factory is in a tropical region. The lower limit as low as -40 °C may be needed if ONUs operate in the outdoor conditions in the winter in a high latitude region.

There is no universal temperature range for all the ONUs under each working condition. If such ONUs are produced with a universal working temperature range, the electronic devices and other ONU components would be more costly. These ONUs would have very poor price-quality ratio and may not be acceptable to Industrial customers.

A better solution is to define a set of temperature ranges each with different upper and lower limits, and different industrial customers could choose a certain temperature range combination for their environment. Therefore, a compromise between performance and cost can be achieved.

Table 7 shows the recommendations for different upper and lower limits in typical working and store temperature range.

Table 7: Recommendations for different upper and lower limits in a typical working and store temperature range

Type	Working temperature/°C		Store temperature/°C	
	Lower limit	Upper limit	Lower limit	Upper limit
I	-10	+60	To Be Determined	To Be Determined
II	-20	+70	To Be Determined	To Be Determined
III	-25	+75	-55	+85
IV	-40	+85	-55	+95

The recommended types in the above table are defined in [i.10].

Typical temperature range test and verification references can be found in [i.11],[i.12].

7.4.3 Water/dust resistance

Different industrial working scenarios also imposes different water and dust resistance capabilities for industrial PON ONUs.

IEC 60529 [i.10] defines several degrees of protection for enclosures, as shown in Table 8.

Table 8: Degrees of protection provided by enclosures (IP Code)

Dust proof level	Water proof level	Reference
IP4X IP5X IP6X	IPX0 IPX1 IPX2 IPX3 IPX4 IPX5 IPX6 IPX7	IEC 60529 [i.10] Degrees of protection provided by enclosures (IP Code)

7.4.4 Humidity

Industrial PON ONUs need to function normally in a high humidity environment.

Table 9 shows the typical recommendation for ONUs humidity working range.

Table 9: A typical recommendation for ONUs humidity working range

Lower limit/%	Upper limit/%
4	95

Typical humidity range test and verification references can be found in [i.9],[i.10].

7.4.5 EMC (Electromagnetic Compatibility)

EMC (Electromagnetic Compatibility) can be further divided into two aspects:

1) Electro-magnetic interference, which is the interference that the device induces into the environment under normal operating.

2) Electro-Magnetic Susceptibility (EMS), which is the resistance of the device to the electro-magnetic interference cause by the environment.

Typical EMC test and verification references can be found in [i.13].

8 Conclusion and next steps

PON technology has been widely deployed in public access network, it has the advantages of large bandwidth, low deploying cost, passive optical distribution network which is resilient to electromagnetic interferences, and smart operation and maintenance capabilities. PON has become the dominant access network solution for operators all around the world.

The PON technology can supports multiple diverse applications, and therefore is suitable also for industrial-grade applications with a few extensions. The extensions compared to residential deployments may include the support of different environmental conditions, industrial protocol adaptation, supporting different topologies, and higher quality of service performance. Industrial PON needs to provide higher performance, higher reliability, and intelligent management to satisfy the service requirements for various industrial customers.

The following are potential next steps and things to do for a successful industrial wide-scale deployment of this technology:

- A greater integration of industrial PON with existing multiple industrial manufacturing systems and information systems is needed.

- Reduction in the variety of ONUs to be built for the different environmental and business conditions.

- Integration of faster and more flexible edge computing functions for flexible adjustment to digitalization needs in manufacturing.
- Standardize the Industrial PON system architecture and interfaces.
- Standardize the ODN in terms of topology and splitting needs.
- Standardize the management architecture and interfaces.
- Standardize the interface and interaction with networks outside the factory.

History

Document history		
V1.1.1	January 2023	Publication