ETSI TR 128 907 V18.0.1 (2024-05)

TECHNICAL REPORT

5G;
Study on enhancement of management of non-public networks
(3GPP TR 28.907 version 18.0.1 Release 18)

Reference

DTR/TSGS-0528907vi01

Keywords

5G

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:
https://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

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.

Legal Notice

This Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

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.

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

Introduction

3GPP introduces basic management and orchestration aspects of non-public networks in TS 28.557 [2].

The present document studies enhanced management aspects of non-public networks.

1 Scope

TS 28.557 [2] introduces management support for non-public networks based on stage 1 service requirements in TS 22.261 [3]. The present document is studies further enhancements to management of non-public networks including the following aspects:

- Study enhanced management of SNPN and PNI-NPN. For example, study new requirements and potential solutions of management capability exposure for SNPN and PNI-NPN, and how the mobile network operator and vertical customer cooperate to realize management and orchestration of network in MNO-Vertical Managed Mode in TS 28.557 [2].
- Study management of vertical as an authorized NPN service customer, e.g. the management of authorized capability of utilizing management services and management data.
- Study requirements and potential solutions to support end to end network management (including RAN domain and CN domain) in NPN scenarios.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 28.557: "Management and orchestration; Management of Non-Public Networks (NPN); Stage 1 and stage 2".

[3] 3GPP TS 22.261: "Service requirements for the 5G system".

[4] 3GPP TS 22.867: "Study on 5G Smart Energy and Infrastructure".

[5] 5G-ACIA: Exposure of 5G Capabilities for Connected Industries and Automation Applications, https://5g-acia.org/whitepapers/exposure-of-5g-capabilities-for-connected-industries-and-automation-applications-2/

[6] 3GPP TS 22.104: "Service requirements for cyber-physical control applications in vertical domains".

[7] 3GPP TS 28.532: "Management and orchestration; Generic management services".

[8] 3GPP TS 23.501: "System architecture for the 5G System (5GS)".

[9] 3GPP TS 32.422: "Telecommunication management; Subscriber and equipment trace: Trace control and configuration management "

[10] 3GPP TS 28.552: "Management and orchestration; 5G performance measurements".

[11] 3GPP TS 28.541: "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3".

[12] 3GPP TR 28.824: "Management and orchestration; Study on network slice management capability exposure".

[13] 3GPP TS 28.104: "Management and orchestration; Management Data Analytics (MDA)".

[14] 3GPP TS 32.423: "Telecommunication management; Subscriber and equipment trace; Trace data definition and management".

[15] 3GPP TS 28.536: "Management and orchestration; Management services for communication service assurance; Stage 2 and stage 3".

[16] 3GPP TS 28.554: "5G end to end Key Performance Indicators (KPI)".

[17] 3GPP TR 28.817: "Study on access control for management service".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Non-Public Network: See definition in TS 22.261 [3].

Public network integrated NPN: See definition in TS 23.501 [8].

Stand-alone Non-Public Network: See definition in TS 23.501 [8].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

NPN	Non-Public Network
NPN-OP	NPN Operator
NPN-SC	NPN Service Customer
NPN-SP	NPN Service Provider
OT	Operation Technology
PLC	Programmable Logic Controller
PNI-NPN	Public Network Integrated NPN
SLS	Service Level Specification
SNPN	Stand-alone NPN

4 Overview

4.1 General

The management of Non-Public Networks (NPNs) is introduced in TS 28.557 [2] which focuses on the basic management and orchestration aspects of NPN. The present document is based on the fundamental concepts, management modes, roles related to NPN management and basic solutions mainly including provisioning of SNPN and PNI-NPN as specified in TS 28.557 [2].

5 Key Issues and potential solutions

5.1 Key Issue #1: E2E fault management

5.1.1 Description

In TS 28.557 [2], the deployment scenarios and solutions for management of Standalone NPN (SNPN) and Public Network Integrated NPN (PNI-NPN) have been specified. However, fault supervision management which is very important for NPN operators is not specified in detail. Furthermore, in some vertical scenarios, 5G industry terminal, e.g. camera, Programmable Logic Controller (PLC) and Smart Distribution Transformer Terminal and so on, are widely deployed. These large quantity 5G industry terminals which may be provided by multiple vendors are managed by multiple standalone terminal management systems and this increases the complexity and difficulty of NPN management, especially for E2E fault location. For example, if an NPN goes down, it is difficult to locate rapidly where the fault occurred or to determine whether the fault is caused by the industry terminal.

5G-ACIA has described the functional requirements for exposing the capabilities of non-public 5G systems to industrial factory applications in [5]. 3GPP should also provide potential solutions to support the use cases and requirements from 5G-ACIA. The requirements given in clause 4.3 of 5G-ACIA white paper in [5] are aspects of network management, as following:

> *"[R-4.3.1-07] The 5G exposure reference points must allow monitoring of errors and other alarms from physical/logical network components and connections.*
>
> *[R-4.3.1-08] The 5G exposure reference points must provide the monitoring information in such a way that it can be effectively used for error detection, localization, root-cause analysis, and error resolution."*

Therefore, for vertical industry scenarios, 3GPP management system needs to provide fault management capabilities scoping NPN and UEs representing 5G industry terminals. These capabilities need to be integrated with the ones scoping OT domain (non-3GPP domain), to allow for E2E fault location.

5.1.2 Potential solutions

5.1.2.1 Potential solution #1: fault management of NPN and 5G industry terminals

5.1.2.1.1 Introduction

This clause provides a potential solution for fault management capabilities scoping NPN and 5G industry terminals.

5.1.2.1.2 Description

In order to provide fault management capabilities scoping NPN and UEs representing 5G industry terminals, an NPN management system should monitor the fault of NPN and large quantity of 5G industry terminals which may be deployed in an enterprise:

- For the fault management of NPN, the network alarm can be discovered by analysing performance data or network alarm event reporting. In this case, the generic fault supervision management service and performance assurance management service in clause 11 of TS 28.532 [7] can be re-used to collect the network performance data and alarm data. For network failure prediction, the MDA capability described in clause 7.2.3.1 of TS 28.104 [13] can be reused.
- For the fault management of 5G industry terminals deployed in an enterprise, the NPN management system should support to performance monitoring and fault diagnosis for 5G industry terminals. NPN management system can collect the performance data and then execute data analysis for alarm detection, localization and/or resolution. The performance data collected from industry terminal may include UL/DL throughput volume, UL/DL throughput time used for calculation of UL/DL throughput, UL/DL packet delay per QoS level, UL/DL packet loss rate per QoS level, etc., defined in clause 4.34.1 of TS 32.423 [14]. The trace control and configuration of MDT in clauses 4.1, 4.2 and 6 of TS 32.422 [9] can be reused for trace/UE measurements activation/deactivation and MDT report to collect MDT data from 5G industry terminals.

5.1.3 Conclusion

The potential solution #1 introduces the management services and performance data which are reused to achieve fault management of NPN and 5G industry terminals.

The management services include:

- Generic fault supervision management service defined in clause 11.2 of TS 28.532 [7].
- Performance assurance management service defined in clause 11.3 of TS 28.532 [7].
- MDA assisted fault management service (e.g. failure prediction) defined in clause 7.2.3 of TS 28.104 [13].
- Trace control and configuration management service defined in TS 32.422 [9].

The performance data collected at 5G industry terminals level includes:

- MDT data (e.g. UL/DL throughput time used for calculation of UL/DL throughput, UL/DL throughput volume, UL/DL packet delay per QoS level, UL/DL packet loss rate per QoS level, etc.) defined in clause 4.34.1 of TS 32.423 [14].

Consequently, it is proposed to introduce the potential solution #1 in further normative work.

5.2 Key Issue #2: Management of NPN service customer

5.2.1 Description

As description in TS 28.557 [2], an NPN service customer is used to represent the role of communication service customer in NPN environment. NPN service customer can request and consume the management capabilities exposed by the mobile network operator. The mobile network operator would restrict the types (e.g. provisioning, fault supervision, performance assurance) of management capabilities and corresponding managed network resource exposed to an NPN service customer. The management of NPN service customers is not considered in TS 28.557 [2], including management of authorized capability of utilizing management services and management data. On the other hand, in some vertical industries, NPN service customer may be authorized to manage the terminal members of their own private network, e.g. monitoring smart distribution transformer terminal in smart grid.

3GPP management system may need to support the management of NPN service customer including:

- -Maintaining of the related information for NPN service customer, including identity of NPN service customer, available management capabilities and other attributes (e.g. service area).
- Member management of NPN service customer, e.g. state monitoring of terminal members, group management of terminal members.

5.2.2 Potential solutions

5.2.2.1 Potential solution #1: Management of the related information for NPN service customer

5.2.2.1.1 Introduction

This clause briefly describes the potential solution for management of the related information for NPN service customer.

5.2.2.1.2 Description

An NPN is provided to a vertical (playing the role of NPN-SC) for private use. Before an NPN is created, an MNO (playing the role of NPN-SP/NPN-OP) needs to authenticate the vertical. If the authentication is passed, the MNO management system should manage the related information for NPN service customer, for example, allocating a new identity of the vertical which can be used in MNO management system and creating the context of the vertical to keep the new identity, authorized available management capabilities, required coverage area and so on.

The procedure of management of the related information for NPN service customer is following. The pre-condition of the procedure is the business agreements between MNO and NPN-SC is reached.

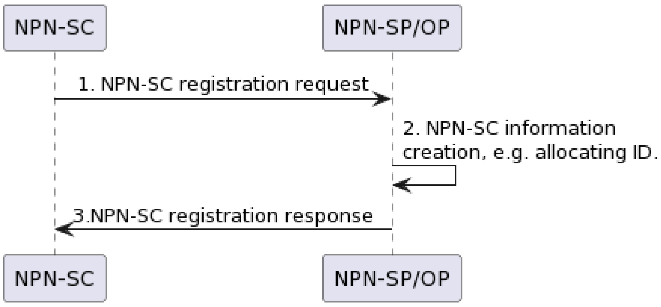
NPN-SC
NPN-SP/OP
1. NPN-SC registration request
2. NPN-SC information creation, e.g. allocating ID.
3.NPN-SC registration response
NPN-SC
NPN-SP/OP

Figure 5.2.2.1.2-1: Procedure of management of the related information for NPN service customer

1) NPN-SC provides the vertical information (e.g. human readable name of vertical, subscribed management capabilities exposed to vertical, etc.) to register a vertical to NPN-SP/NPN-OP through an NPN-SC registration request message. This message may be interacted with BSS layer. But the BSS layer should forward the subscription data to OSS layer to authorize the exposure of management capabilities and corresponding managed resources to NPN-SC.

2) NPN-SP/NPN-OP receives the vertical information from NPN-SC and executes the authentication and authorization for a vertical. The NPN-SP/NPN-OP allocates a new identity which is associated with the vertical identity and creates the context information of the vertical in local. The context information can be managed in form of NRM IOCs. The NPN-SP/NPN-OP uses the allocated new identity in MNO management system to identify the corresponding vertical.

   The details of the context information, as example, are:

   - consumerID: It is used to identify the MnS consumer (e.g. NPN-SC).

   - authorizedMnS: It gives a list of management services that are allowed to be exposed to the NPN-SC. The MnS components Type A, Type B and/or Type C should be specified in this attribute. The attribute `authorizedMnS` defined in Table 7.1.4-1 of TR 28.817 [17], which gives list of management services and its capabilities the consumer is authorized to access, can be used to for holding this information.

   - validDuration: It specifies a time period during which the NPN-SC can consume the exposed management capabilities. The NPN-SC is banned to consume exposed management capabilities when it is out of the valid duration. The attribute Validity defined in Table 7.1.4-1 of TR 28.817 [17] can be used to for holding this information.

3) The NPN-SP/NPN-OP sends NPN-SC registration response message to the NPN-SC including the authentication result (e.g. success or failure), the new identity, authorized available management capabilities information and other attributes which are part of the context information of the vertical.

5.2.3 Conclusion

The potential solution #1 introduces the procedure of creating NPN-SC context information, which can be applied by NPN-SP/NPN-OP to restrict the management capabilities and corresponding managed network resources exposed to NPN-SC. The details of the context information can be managed in form of NRM IOCs and it is proposed to introduce the potential solution #1 in further normative work for Rel-18 to update the NRM IOCs in TS 28.541 [11].

5.3 Key Issue #3: Resource isolation demand for Smart Grid Utilities

5.3.1 Description

Smart Grid is a representative utility with NPN. A power grid consists of four building blocks: power generation, transmission, distribution and consumption. These different phases require different services, and these services have distinct communication requirements.

As description in clause 5.9 of TS 22.867 [4]:

> According to the regulation of China Grid industry, the power grid business is mainly divided into two working categories: production control and information management. The production control can be further divided into safety zone I and safety zone II. The information management also can be further divided into safety zone III and safety zone IV.

Different kinds of safety isolation requirements are applied to different safety zones:

a) The energy applications belong to production control category i.e. safety zones I and II need to be physically isolated from other applications which do not belong to production control working category.

b) The energy applications belong to information management working category i.e. safety zone III and IV can be logically isolation from other applications including non-energy applications.

c) The energy applications belong to a same working category can be logically isolated each other.

d) The energy applications belong to a same safety zone can be logically isolated each other.

NPN may be deployed to support the different use cases and service requirements for multiple Smart Grid applications. For example, multiple NPNs (e.g. multiple PNI-NPNs, each having on-prem NFs and a dedicated portion of PLMN NFs as a slice of the PLMN) may be deployed to meet the requirements of physical isolation communication service. The logical isolation communication service on the other hand may be supported by shared network element or shared network resource in one NPN for Smart Grid.

To provide management mechanism to assurance resource isolation for different isolation modes, 3GPP management system may need to configure different network parameters whose purpose is for energy applications with different isolation modes.

Therefore, 3GPP management system needs to have the capability to meet the distinct communication requirements with different resource isolation demands for some smart grid applications supported by NPNs.

5.3.2 Potential solutions

5.3.2.1 Introduction

This clause provides a potential solution to satisfy the resource isolation demand described in clause 5.3.1.

5.3.2.2 Description

A resource isolation-sharing policy, which contains the logical and physical isolation policies among different safety zones, can be sent to NPN-OP.

The logical resource isolation-sharing policy includes several groups of safety zones. Energy applications belonging to the safety zones within the same group use the shared logical resources (e.g. a network slice), while energy applications categorized into different safety zones across different groups use isolated logical resources. An example of the division of safety zones into groups is shown in Figure 5.3.2.2-1.

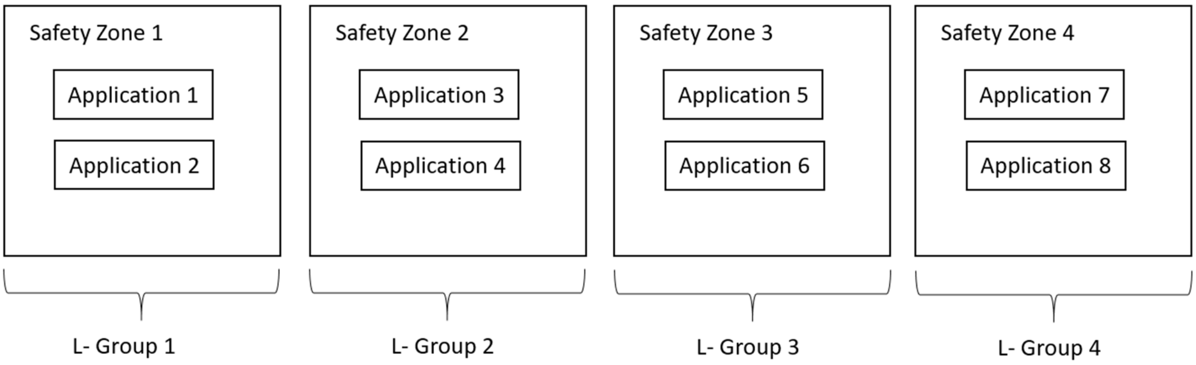

Figure 5.3.2.2-1: Example of logical isolation-sharing policy - groups cross multiple safety zones

In case that the applications belonging to the same safety zone require to be logically isolated with each other, the groups can reflect the resource isolation-sharing policy at a more granular level, such as specifying the applications. An example of the division of applications into groups is shown in Figure 5.3.2.2-2. Application 1-1 and Application 2-1 are further divided into different subgroups as they cannot share same logical network resources event though they are both categorized into safety zone 1.

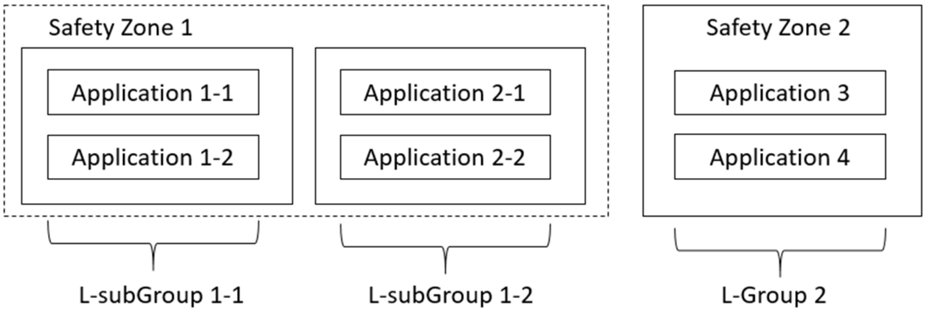

Figure 5.3.2.2-2: Example of logical isolation-sharing policy - subgroups within one safety zone

Similarly, the physical resource isolation-sharing policy includes several groups of safety zones. Energy applications belonging to the safety zones within the same group use the shared physical resources, while energy applications categorized into different safety zones across different groups use isolated physical resources. An example of the division of safety zones into groups is shown in Figure 5.3.2.2-3.

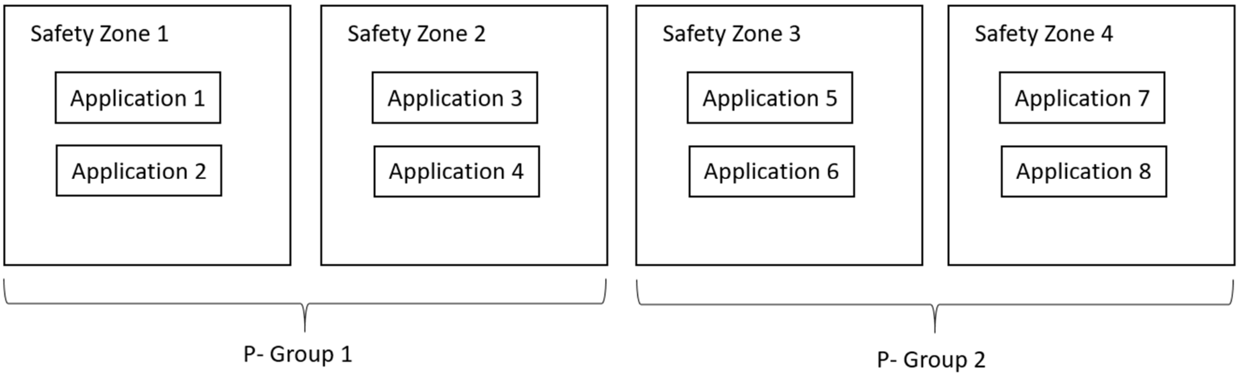

Figure 5.3.2.2-3: Example of physical isolation-sharing policy

All logical and physical isolation-sharing relations (i.e. shared or isolated) between every two safety zones could be figured out with the resource isolation policy, and the NPN-OP should take it into consideration when allocating network resources for each safety zone. When Smart Grid Utilities requests the network resources allocation for energy applications, the safety zone type and the related logical and/or physical resource isolation lists could be attached in the request to show the logical and/or physical resource isolation-sharing relations between one safety zone and other safety zones, so that the network resources allocation for energy applications belonging to certain safety zones satisfies the resource isolation demand. Detailed explanation of the safety zone type, logical and physical resource isolation lists are as following:

- The safety zone type is used to identify which safety zones the energy applications are categorized into.
- The subgroup identifier is used to identify the subgroups of energy applications within one safety zone. It is only applicable when applications belonging to a same safety zone requires to be logically isolated each other.
- The logical resource isolation list is derived from the logical isolation-sharing policy and contains safety zones that are required to be logical isolated with the current safety zone. Safety zones which are out of this list are ones that sharing the same logical network resources with the current safety zone. When the subgroup identifier is specified, the other subgroups of the current safety zone should also be included in the logical resource isolation lists.
- The physical resource isolation list is derived from the physical isolation-sharing policy and contains safety zones that are required to be physical isolated with the current safety zone. Safety zones which are out of this list are ones that sharing the same physical network resources with the current safety zone.

5.3.3 Conclusion

To satisfy the resource logical and/or physical isolation demand for Smart Grid Utilities, the potential solution #1 introduces a resource isolation-sharing policy which contains the grouping information based on division of safety zones. It is proposed to use the potential solution #1 as an input for the ongoing normative work item network slicing provisioning rules to discuss the normative solutions for Rel-18.

5.4 Key Issue #4: SLA monitoring and evaluation

5.4.1 Description

A Service-Level Agreement (SLA) consists of a technical part and a non-technical part (i.e., pricing and billing conditions, penalties, etc.). The technical part, referred to as SLS, capture service requirements which are input to 3GPP management system. For example, TS 22.104 [6] presents service requirements of cyber-physical control applications (e.g. motion control, process automation, etc.) in vertical domains, which require very high levels of communication service availability and/or very low end-to-end latencies. The end-to-end latency is also very important for the applications of smart Grid, e.g. differential protection in power distribution grid.

From network management perspective, the network management service provider allocates network resource to provide communication service based on related service requirements, monitoring the network performance to evaluate the SLA fulfilment. Therefore, the NPN management system may need to study how to assure whether the service and network requirements are achieved. Some related KPIs/KQIs like communication service availability, communication service reliability, end-to-end latency, UE speed, are clarified to continually monitoring the network performance to evaluate the assurance of the SLA. If the SLA is not fulfilled, the network optimization contributing to SLS assurance, e.g. reconfigure the resources should be adopted to resolve the performance degradation.

5.4.2 Potential solutions

5.4.2.1 Potential solution #1: high level process for NPN SLA management

5.4.2.1.1 Introduction

This clause briefly describes the potential solution for SLA monitoring and evaluation.

5.4.2.1.2 Description

The high-level process for NPN SLA management in figure 5.4.2.1.2-1.

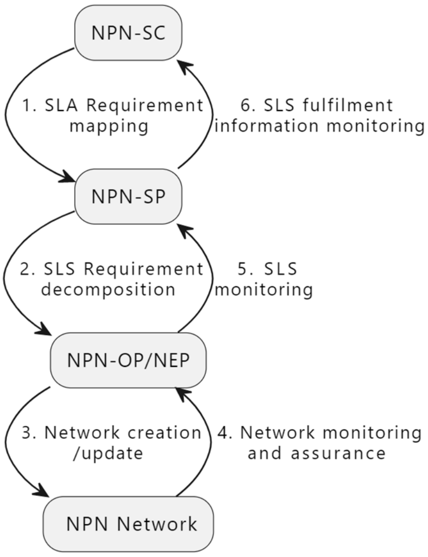
NPN-SC
1. SLA Requirement mapping
6. SLS fulfilment information monitoring
NPN-SP
2. SLS Requirement decomposition
5. SLS monitoring
NPN-OP/NEP
3. Network creation /update
4. Network monitoring and assurance
NPN Network

Figure 5.4.2.1.2-1: high level process for NPN SLA management

In figure 5.4.2.1.2-1, steps 1 to 3 describe the workflows of NPN creation or update which is specified as NPN provisioning procedures in TS 28.557 [2] in detail. The steps 4, 5 and 6 are the NPN SLS monitoring and SLA assurance loop.

The NPN management system (e.g. NPN-SP/NPN-OP/NEP) collects performance data (e.g. packet delay in TS 28.552 [10] and reliability in TS 28.541 [11]) to monitor the NPN status through performance assurance MnS. The typical categories of KPI include Accessibility, Integrity, Utilization, Retainability, Mobility, Energy Efficiency and Reliability as defined in TS 28.554 [16].

Based on the network KPIs, the NPN management system evaluates the network availability and reliability to assure the SLA fulfilment. If the SLA is not fulfilled, the NPN management system adopts some optimization methods to promote the network performance, such as SLA parameter coordination among RAN NEs, RAN resource and priority scheduling adjustment. For SLS fulfilment information monitoring, assurance closed control loop introduced in TS 28.536 [15] may be applied to achieve the SLS assurance control.

5.4.3 Conclusion

The potential solution #1 introduces the high level process for NPN SLA monitoring and evaluation. Four NPN roles (i.e. NPN-SC, NPN-SP, NPN-OP and NEP) are involved in the NPN SLA monitoring and evaluation. To achieve SLA monitoring and evaluation, NPN management system (e.g. NPN-SP/NPN-OP/NEP) performs network monitoring and evaluation for SLS fulfilment monitoring. For the details of SLA assurance, the closed control loop described in TS 28.536 [15] can be reused.

Consequently, it is proposed to introduce the potential solution #1 in further normative work for Rel-18.

5.5 Key Issue #5: Exposure of management capabilities and corresponding managed resources under MNO-Vertical Managed Mode

5.5.1 Description

TS 28.557 [2] specifies two management modes for PNI-NPN and three management modes for SNPN. Under MNO-Vertical Managed Mode for PNI-NPN and MNO-Vertical Managed Mode for SNPN, the vertical also plays the role of NPN operator shared with mobile network operator, to achieve management on the NPN served for the vertical.

Therefore, a bundle of management capabilities and corresponding managed resources should be exposed to the vertical from the mobile network operator according to the business agreement between the two parties under MNO-Vertical Managed Mode.

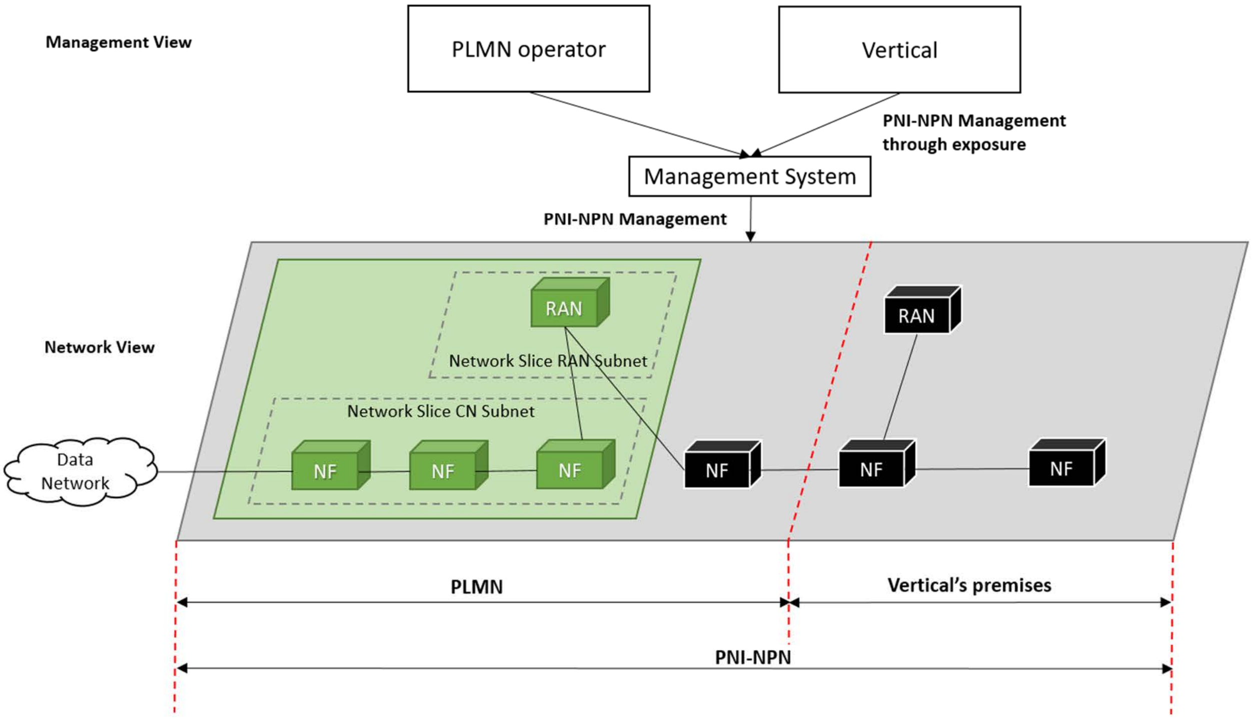

Figure 5.5.1-1: Vertical managing PNI-NPN through exposure

Figure 5.5.1-1, as an example, illustrates how the PLMN operator and the vertical manage the PNI-NPN under the MNO-Vertical Managed Mode. The PNI-NPN, which is deployed across one PLMN and the vertical's premises (e.g. factory), can be seen as an end-to-end network composed of two differentiated segments: one public, consisting of a (R)AN and network functions built upon public 5GC network resources; and one private, consisting of network functions deployed using non-public 5G network resources. The vertical can realize the management of PNI-NPN through management capabilities exposure.

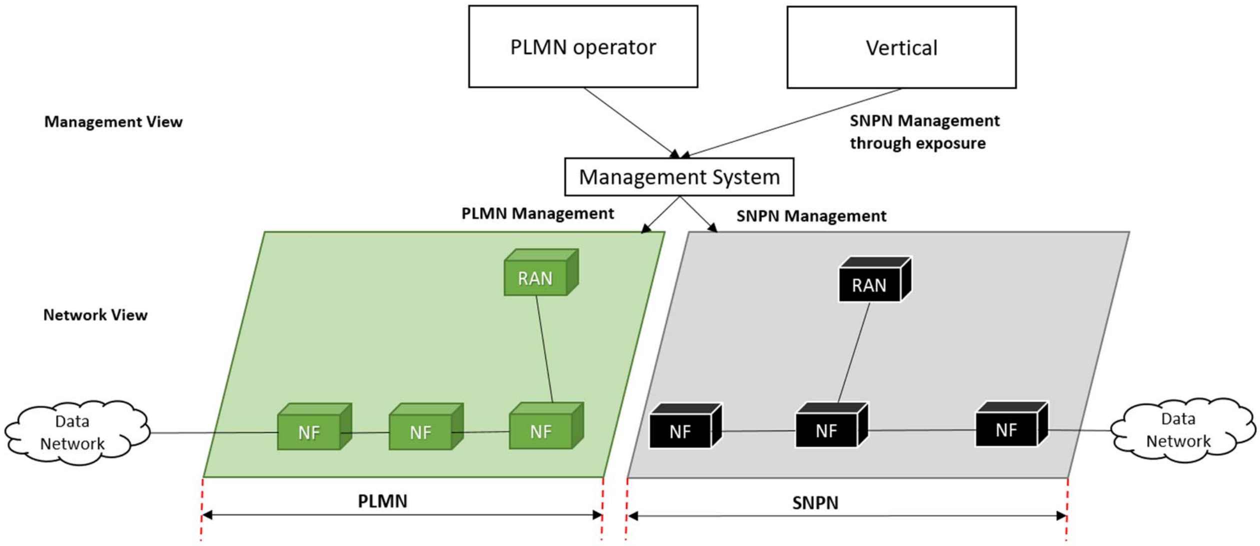

Figure 5.5.1-2: Vertical managing SNPN through exposure

Figure 5.5.1-2, as an example, illustrates how the PLMN operator and the vertical manage the SNPN under the MNO-Vertical Managed Mode. The SNPN is deployed as an independent, isolated network. All SNPN network elements are located inside the logical perimeter of the vertical's premises (e.g. factory) and the SNPN is separate from the PLMN. The PLMN operator and the vertical play the role of SNPN operator together, and the vertical can realize the management of SNPN through management capabilities exposure.

Exposing what kind of management capability and managed resources (e.g. local UPF, gNBs belong to vertical covering specific geographic areas, etc.) for vertical relies on specific cases, such as:

- As described in clause 5.1.1, the capability of monitoring network errors and alarms could be exposed to vertical to support its fault root-cause analysis, localization, etc., on NPN.
- According to the issue described in clause 5.3.1, the capability of configuring the NPN network resources (especially for those assets belong to the vertical e.g. local UPF or local gNBs covering specific geographic areas for a specific vertical) could further be exposed to vertical to satisfy the specific logical and/or physical resource isolation requirements for energy applications categorized into different safety zones.
- According to the issue described in clause 5.4.1, the capability of monitoring KPIs/KQIs, like communication service availability, end-to-end latency, etc., could further be exposed to vertical to detect performance degradation and support performance optimization on NPN.

5.5.2 Potential solutions

5.5.2.1 Potential solution #1: Exposure via OSS under MNO-Vertical Managed Mode

5.5.2.1.1 Description

Systems and layers related to this solution are introduced in clause 5.6.1 of [12] and also explained as follows:

- BSS: Business Support System
- OSS: Operations Support System, made up of the three following sub-systems:
    - SML: Service Management Layer
    - NML: Network Management Layer

- **EML: Element Management Layer**

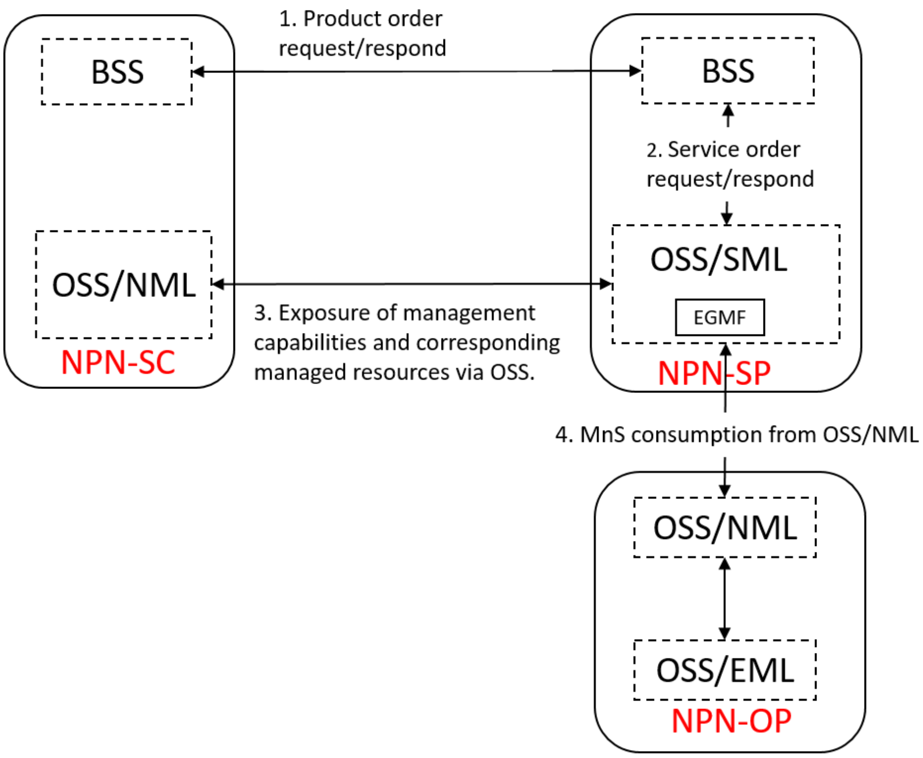
1. Product order request/respond
BSS
BSS
2. Service order request/respond
OSS/NML
OSS/SML
EGMF
3. Exposure of management capabilities and corresponding managed resources via OSS.
NPN-SC
NPN-SP
4. MnS consumption from OSS/NML
OSS/NML
OSS/EML
NPN-OP

Figure 5.5.2.1.1-1: Exposure via OSS

An illustration of the "product - service - network resource" layering in the context of NPN could be the following:

- NPN Service Provider offers an NPN Product as SNPN or PNI-NPN, for example:
  - There can be several ways to implement this Product, one of them being via network slicing.
- Two possible services to support this NPN product:
  - URLLC type network slicing over 5G NSA
  - URLLC type network slicing over 5G SA
- Network resource
  - For PNI-NPN network resource: The network resources include the PNI-NPN which is deployed across one PLMN and the vertical's premises (e.g. factory), can be seen as an end-to-end network composed of two differentiated segments: one public, consisting of a (R)AN and network functions built upon public 5GC network resources; and one private, consisting of network functions deployed using non-public 5G network resources.
  - For SNPN network resource: The network resources include the SNPN which is deployed as an independent, isolated network. All SNPN network elements are located inside the logical perimeter of the vertical's premises (e.g. factory) and the SNPN is separate from the PLMN.

Figure 5.5.2.1.1-1 illustrates the generic exposure process for NPN management via OSS under MNO-Vertical Managed Mode for PNI-NPN and MNO-Vertical Managed Mode for SNPN:

1. The product order request/respond between NPN-SC and NPN-SP via BSS. The product order may contain the requirements on the exposure of management capabilities and corresponding managed resources.
2. The service orders request/respond between NPN-SP BSS and NPN-SP OSS/SML. The service orders are decomposed from product order.

3. The exposed MnS consumption request/respond between NPN-SC and NPN-SP via OSS. The NPN-SC can consume the exposed management services directly from OSS/SML of NPN-SP to realize the management of NPN. A dedicated MnF (e.g. EGMF) may be responsible for the control of exposure governance.

4. According to the exposed MnS consumption request, the OSS/SML of NPN-SP may request the consumption of corresponding MnS provided by OSS/NML of NPN-OP.

Annex A: Plant UML source code

A.1 Procedure for management of the related information for NPN service customer

The following PlantUML source code is used to describe the procedure for management of the related information for NPN service customer, as depicted by Figure 5.2.2.1.2-1:

```
@startuml
"NPN-SC" -> "NPN-SP/OP": 1. NPN-SC registration request
"NPN-SP/OP" -> "NPN-SP/OP":2. NPN-SC information\ncreation, e.g. allocating ID.
skinparam responseMessageUpArrow true
"NPN-SP/OP" -> "NPN-SC":3.NPN-SC registration response
 skinparam sequenceMessageAlign center
@enduml
```

A.2 Procedure for high level process for NPN SLA management

The following PlantUML source code is used to describe the high level process for NPN SLA management, as depicted by Figure 5.4.2.1.2-1:

```
@startuml
"NPN-SC" --> [ 1. SLA Requirement\nmapping] "NPN-SP"
--> [ 2. SLS Requirement\ndecomposition] "NPN-OP/NEP"
--> [ 3. Network creation\n/update]" NPN Network"
--> [ 4. Network monitoring\nand assurance]"NPN-OP/NEP"
--> [ 5. SLS\nmonitoring]"NPN-SP"
--> [6. SLS fulfilment \ninformation monitoring]"NPN-SC"
@enduml
```

Annex B:
Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
04-2022	SA5#142e	S5-222266 S5-222267 S5-222268 S5-222667 S5-222668 S5-222272				Update to implement the agreed pCRs in SA5#142e: 1) S5-222266 pCR 28.907 Skeleton proposal from Rapporteur 2) S5-222267 pCR 28.907 Scope proposal from Rapporteur 3) S5-222268 pCR 28.907 Overview proposal 4) S5-222667 pCR 28.907 Key Issue on Resource isolation demand for Smart Grid Utilities 5) S5-222668 pCR 28.907 Key Issue on E2E fault management 6) S5-222272 pCR 28.907 Key Issue on Management of NPN service customer	0.1.0
05-2022	SA5#143e	S5-223609 S5-223610 S5-223608				Update to implement the agreed pCRs in SA5#143e: 1) S5-223609 pCR 28.907 Key Issue on SLA monitoring and evaluation 2) S5-223610 pCR 28.907 Potential solution for KI#1 3) S5-223608 pCR 28.907 Potential solution for KI#2	0.2.0
06-2022	SA5#144e	S5-224080 S5-224078 S5-224079				Update to implement the agreed pCRs in SA5#144e: 1) S5-224080 pCR 28.907 Rapporteur proposal 2) S5-224078 pCR 28.907 Update performance data collection procedure 3) S5-224079 pCR 28.907 Potential solution for SLA monitoring and evaluation	0.3.0
08-2022	SA5#145e	S5-225860 S5-225159 S5-225859 S5-225161 S5-225818				Update to implement the agreed pCRs in SA5#145e based on MCC EditHelp version: S5-225860 pCR 28.907 Rapporteur proposal S5-225159 pCR 28.907 Add introduction of TR S5-225859 pCR 28.907 Update clause 4.1 S5-225161 pCR 28.907 Add key issue for network capability exposure S5-225818 pCR 28.907 Potential solution for satisfying resource isolation demand for Smart Grid Utilities	0.4.0
2022-09	SA#97e	SP-220951				Presented for information	1.0.0
11-2022	SA5#146	S5-227000 S5-227001 S5-227002 S5-227003 S5-227004 S5-227005				Update to implement the agreed pCRs in SA5#146: 1) S5-227000 pCR 28.907 Potential solution for exposure of management capabilities and corresponding managed resources 2) S5-227001 pCR 28.907 Resolve Editor's note in clause 5.1.2.1.2 3) S5-227002 pCR 28.907 Resolve Editor's note in clause 5.4.1 4) S5-227003 pCR 28.907 Conclusion for E2E fault management 5) S5-227004 pCR 28.907 Conclusion for resource isolation demand for smart grid utilities 6) S5-227005 pCR 28.907 Resolve Editor's note in clause 5.2.2.1.2	1.1.0
03-2023	SA5#147	S5-232875 S5-232411 S5-232046 S5-232881				Update to implement the agreed pCRs in SA5#147 based on MCC EditHelp version: 1) S5-232875 pCR 28.907 Update conclusion for KI resource isolation demand for Smart Grid Utilities 2) S5-232411 pCR 28.907 Rapporteur proposal 3) S5-232046 pCR 28.907 Conclusion for KI management of NPN service customer 4) S5-232881 pCR 28.907 Conclusion for KI SLA monitoring and evaluation	1.2.0
2023-03	SA#99	SP-230186				Presented for approval	2.0.0
2023-03	SA#99					Upgrade to change control version	18.0.0
2023-03	SA#99					EditHelp review	18.0.1

History

Document history		
V18.0.1	May 2024	Publication