|  |  |
| --- | --- |
| 3GPP TR 28.829 V18.0.1 (2023-06) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on network and service operations for energy utilities  (Release 18) | |
|  | |
|  | 3GPP-logo_web |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

Introduction 6

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Symbols 9

3.3 Abbreviations 9

4 Overview 9

4.1 General 9

5 Concepts 10

5.1 Energy Service is Critical for Telecommunications Service Availability 10

6 Business use cases and potential requirements 10

6.1 Business use case: MNO exposes network performance monitoring 10

6.1.1 Description 10

6.1.2 Details 11

6.1.3 Potential Requirements 13

6.2 Business use case: Energy utility and telecommunication coordinated recovery of energy service 14

6.2.1 Description 14

6.2.2 Details 17

6.2.3 Potential Requirements 18

6.3 Business use case: Rapid intervention for outages without redundant energy feeder topology 19

6.3.1 Description 19

6.3.2 Details 20

6.3.3 Potential requirements 23

7 Key Issues and potential solutions 24

7.1 Key Issue #1: MNO exposes network performance monitoring 24

7.1.1 Description 24

7.1.2 Potential solutions 24

7.1.2.1 Potential Solution #1: MNO exposes network performance monitoring 24

7.1.2.1.1 Introduction 24

7.1.2.1.2 Description 25

7.1.2.2 Potential Solution #2: MNO exposes network performance monitoring 26

7.2 Void 26

7.3 Key Issue #3: Energy utility and telecommunication coordinated recovery of energy service 26

7.3.1 Description 26

7.3.1.1 General 26

7.3.1.2 Coordinated recovery of energy service with redundant topology 26

7.3.1.3 Coordinated recovery of energy service without redundant topology 27

7.3.2 Potential Solutions 27

7.3.2.1 Potential Solution # 1: Energy utility and telecommunication coordinated rapid recovery of energy service 27

7.3.2.1.1 Introduction 27

7.3.2.1.2 Description 28

7.3.2.2 Potential Solution # 2: Energy utility and telecommunication coordinated rapid recovery of energy service 30

7.4 Key Issue #4: Security aspects of exposure of energy service 30

7.4.1 Description 30

7.4.2 Potential solutions 30

7.4.2.1 Potential solution #1: CAPIF 30

7.4.2.2 Potential solution #2: MSAC 30

8 Conclusion and recommendation 30

8.1 Key Issue #1: MNO exposes network performance monitoring 30

8.2 Key Issue #3: Energy utility and telecommunication coordinated recovery of energy service 31

8.3 Key Issue #3: Security aspects of exposure of energy service 32

Annex A: Service model for energy utilities and communication service providers 33

Annex B: Network services and operations for energy utilities applicability statement 34

Annex C: Use cases not pursued 36

C.1 General 36

C.2 Business use case: DSO obtains network performance and outage information, current practice 36

C.2.1 Description 36

C.2.2 Details 39

C.2.3 Potential requirements 40

C.3 Business use case: DSO reporting to MNO to resolve problems and incidents, current practice 40

C.3.1 Description 40

C.3.2 Details 41

C.3.3 Potential requirements 42

C.4 Business use case Energy Outage Coordination current practice 43

C.4.1 Description 43

C.4.2 Details 43

C.4.3 Use case actors 44

C.4.4 Use case service flow 44

C.4.5 Potential requirements 44

C.5 Business use case: MNO exposes Network Alarm 44

C.5.1 Description 44

C.5.2 Details 45

C.5.3 Potential Requirements 46

C.6 Business use case: DSO Provides Performance Information indicating Relevant Changes to its Network 47

C.6.1 Description 47

C.6.2 Details 47

C.6.3 Potential Requirements 49

C.7 Business use case: DSO reports an incident to MNO 49

C.7.1 Description 49

C.7.2 Details 50

C.7.3 Potential Requirements 51

Annex D: Key issues not pursued 53

D.1 Key Issue # 2: DSO reports an incident to the MNO 53

D.1.1 Description 53

D.1.2 Potential Solutions 53

D.1.2.1 Potential Solution # 1: TMF API 621 (Trouble Ticket) 53

D.1.2.1.1 Introduction 53

D.1.2.2 Potential Solution # 2: MnS-based standardized interface 53

D.2.2.2.1 Introduction 53

Annex E: Change history 54

# 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

The purpose of the present document is to study on Network and Service Operations for Energy Utilities.

# 1 Scope

The present document considers service requirements introduced by the SEI work item related to telecom management [2] and [3]. This feasibility study identifies use cases and requirements for exposing capabilities of the 3GPP management system to external energy utility service providers. The study further considers how management capabilities or what information can be provided to MNOs by the external energy utility service providers. The study will consider both energy utility use cases and requirements. The study of FS\_NSCE [4] can be considered for the technical investigation.

# 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 22.104: "Service requirements for cyber-physical control applications in vertical domains".

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

[4] 3GPP TR 28.824: "Study on network slice management capability exposure".

[5] IT Process Wiki – The ITIL Wiki:. https://wiki.en.it-processmaps.com/index.php/ITIL\_Service\_Operation Content is available according to Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Germany License. Access 08.12.21.

[6] 3GPP TR 22.867: "Study on 5G smart energy and infrastructure"

[7] Connected Nations 2020, UK Report, Ofcom. https://www.ofcom.org.uk/\_\_data/assets/pdf\_file/0024/209373/connected-nations-2020.pdf Access 20.4.22.

[8] Telecom Services Security Incidents 2019 Annual Analysis Report, ENISA European Agency for Cybersecurity, July 23, 2020. https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2019.

NOTE: This publication is intended for information purposes only and is accessible free of charge. Reproduction is authorised provided the source is acknowledged. Access 20.4.22.

[9] DIRECTIVE (EU) 2019/ 944 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 5 June 2019 - on common rules for the internal market for electricity and amending Directive 2012/ 27/ EU (europa.eu)  
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0944&from=EN>

[10] IEC TC 57 <https://www.iec.ch/ords/f?p=103:7:511571509228708::::FSP_ORG_ID,FSP_LANG_ID:1273,25>

[11] 3GPP TS 32.130: "Telecommunication management; Network sharing; Concepts and requirements".

[12] 3GPP TS 28.554: "Management and orchestration; 5G end to end Key Performance Indicators (KPI)".

[13] 3GPP TS 28.552: "Management and orchestration; 5G performance measurements".

[14] 3GPP TS 22.104: " Service requirements for cyber-physical control applications in vertical domains ".

[15] 3GPP TS 32.404: " Performance Management (PM); Performance measurements; Definitions and template".

[16] 3GPP TS 28.530: "Management and orchestration; Concepts, use cases and requirements".

[17] CAMARA: Telco Global API Alliance <https://www.gsma.com/futurenetworks/ip\_services/understanding-5g/camara-telco-global-api-alliance/>, accessed 16.02.23.

[18] ETSI ES 202 336 (all parts): "Environmental Engineering (EE); Monitoring and Control Interface for Infrastructure Equipment (Power, Cooling and Building Environment Systems used in Telecommunication Networks)".

[19] IETF RFC 1628: "UPS Management Information Base", 1994.

# 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].

**Distribution System Operator:** a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity.

NOTE 1: see Article 2, definitions in DIRECTIVE (EU) 2019/ 944 [9].

**SCADA**: 'Supervisory Control and Data Acquisition'.

NOTE 2: The management system of power grid is standardized by IEC TC 57, see Dashboard, scope [10].

**Distribution Automation:** A family of technologies, systems and processes (including sensors, actuators, processors, communication networks, switches, etc.) that enable the remote, real-time monitoring, operation, and optimization of utility distribution systems on the field.

**Remote Terminal Unit:** a host in a customer network operated entirely out of the scope of 3GPP standardization.

**Uninterruptable Power Supply:** an independent source of energy that, for a limited time duration, can sustain operations normally despite an interruption of energy distribution services.

**Customer Premises Equipment:** a component of communications infrastructure that is installed in the facility owned and operated by a customer.

**Energy Supply** **ID:** This is the point where the energy supply terminates in the operator site and has a unique ID that is known by both the MNO and DSO.

**site operator:** A business entity who operates infrastructure on behalf of MNOs, e.g. in some networking scenarios, for base station(s) and/or cell site(s).

NOTE 3: This entity supports telecommunications operations and management, e.g. in network sharing scenarios. The site operator is a Master Operator (MOP) as defined in 32.130. [11]

## 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].

DSO Distribution System Operator

SCADA Supervisory Control And Data Acquisition

DA Distribution Automation

CPE Customer Premises Equipment

RTU Remote Terminal Unit

UPS Uninterruptable Power Supply

# 4 Overview

## 4.1 General

The delivery of energy has to occur with extreme levels of availability. Reliability is crucial in this domain, for regulatory, business and public health and safety requirements. To achieve this reliability, a range of 'smart energy services' are employed by the energy system. These services, largely standardized by IEEE and IEC, require communication. As greater degrees of efficiency, resiliency, responsiveness and other capabilities are sought in the generation and delivery of energy, more and more communications services are required by the energy sector.

There are many options for delivery of communication services today – power line communications, fibre optics, fixed networks, microwave transmission, satellite communications and mobile telecommunications. The appropriate means, or rather *mix* of communications services, depends on several factors including the location, the possibility of leveraging existing assets (e.g. power lines,) and the 'total cost of operations,' and the *properties* of the communication service.

To the extent that the 3GPP system can provide services that meet the needs of the energy sector, telecommunications will be an increasingly important part of the technical ecosystem by which energy is delivered.

The stage 1 feature 'Smart Energy Infrastructure' includes service requirements that will be considered further, in detail, in the present document. In particular, TR 22.867 [6] identified requirements for specific standardized capabilities that allow a utility operator to obtain information from an operator's network, and to share information with the operator. This information all serves to improve the realized availability of energy system services.

The energy utility service provider needs information regarding outages and performance degradation of the communication system, as it may be possible for the energy utility service provider to reactively or even proactively establish and use an alternative means of communication. Changes in the configuration of the network may also impact the energy utility service provider. Finally, the energy utility service provider can share information with the MNO in order to facilitate rapid diagnosis and recovery from performance problems and energy supply interruptions.

Another reason that energy utilities are an important sector for 3GPP is that telecommunications network operations themselves require energy. The relationship is bi-directional: MNOs require energy services, and energy utilities require communication services. This demands a particular risk management be undertaken by both systems, especially in the event of an energy outage. The present document considers how energy utility service providers and MNOs can exchange information in a standardized format related to an energy service interruption and how to resolve such energy service interruptions efficiently.

# 5 Concepts

## 5.1 Energy Service is Critical for Telecommunications Service Availability

It is important to note that energy outages are one of the principal factors that in telecommunication service availability failures.

Ofcom analysed service outages between September 2019 and August 2020 in the UK and found that power cuts were the #2 most common causes of telecommunications failure incidents during that period. [7]

ENISA analysed European data and found that in 2019, the second most common cause of telecommunications service failure were power cuts. " Power cuts are the second most common detailed cause: Overall, independent from the underlying root cause, power cuts are either a primary or a secondary cause in over a fifth of the major incidents" [8].

Governments in each country settle requirements for reporting of failure of power grid. In some cases, the consumer can claim economic compensations due to caused damage.

As a common principle in all countries worldwide, a state authority is responsible to report failures on a yearly basis in the power grid but deviations do exist.

The telecom network can be impacted by external factors, specifically by the power grid. If there is a failure in the grid, then the faulty part needs to be disconnected to avoid risk for fire or human injuries due to short circuit. Further, the telecom network requires electricity and has a limited capacity to operate without energy from the power grid.

The telecom network can be impacted due to internal power system failure at the site. This can be a short circuit or damaged batteries. This is part of telecom operator's incident management or fault management system and out of scope of this study.

The start up of electrical power grid can be cumbersome. As common a top-down approach is performed in centralized energy distribution system. However, in future a bottom-up approach may be the best alternative, since some of the micro grids may still work to the extent that they can operate autonomously. Detailed assessment of micro-grids is outside the scope of this study.

Each country sets their own requirements and regulations for the energy sector and telecom sector operating in that country. It is common for there to be the following regulation:

- Telecom act is controlling the telecom regulation. This is setting requirement for how the telecom service in the country is handling. This can include reliable operation.

- Energy act is controlling the energy regulation

Disaster act is giving guidance when major problem is impacting the countries. MNOs do have backup system installed at site since they are operating a mobile network 24/7. There can be external power failure and then the backup system can have internal problem or limited capacity.

# 6 Business use cases and potential requirements

## 6.1 Business use case: MNO exposes network performance monitoring

### 6.1.1 Description

**Motivation**

In clause C.2.1, it was explained that DSOs require extremely high availability for communication to provide distribution automation and SCADA services to prevent energy service outages. Unlike the use case C.5 MNO exposes Network Service Alarm, this use case focusses on proactive measures. The motivation for this is described in clause C.2.1.

The sooner and in sufficient detail that the DSO obtains information regarding communication service deterioration, the better. This deterioration may be considered a 'problem.' (The term 'problem' is used in the sense described in Annex A, a reduction in service metrics. This is distinguished from an 'incident' in which required service levels cannot be maintained.)

As described in clause C.2.1, a DSO can determine levels of service over time by means of their own infrastructure. The DSO has many routers in their network. These provide networking within substation networks and have wireless access interfaces to connect the substation network over a wide area. These routers perform periodic monitoring operations, e.g. sending ICMP echo (ping) messages to ascertain latency and reachability. In addition, the UE has access to radio and cellular information - signal strength, serviced Cell ID, radio technology. These measurements are captured on the UE and obtained 'over the top' by the DSO using their own management system over time. The acquired data are assessed to discern trends that, historically considered, indicate that an incident is likely. This monitoring occurs at a coarse granularity (e.g. one measurement per minute.) There are two shortcomings to this approach that this use case seeks to overcome:

1. The information is based on measurements of single nodes only, not the overall network. The DSO knows

(a) The location of each of their devices and the serving Cell ID.

(b) The DSO has several devices (in the same cell) and can by means of correlation of data received by devices identify possible problems that affect the entire cell.

(c) The nature of the deterioration of performance remains ambiguous - is it an issue in the DSO's own network (essentially a managed set of VLANs and substation networks), or is it a problem in the MNO's network?

2. The granularity of the measurement is coarse, the bandwidth requirements to control and collect the data significant compared to the service data traffic (when there is no need for more than routine monitoring and management of the energy system) and the measurements are distributed - requiring connectivity to all UEs. To the extent the performance deteriorates, so too does the access of the DSO to the UEs that provide measurements. So, as an incident approaches, just when more information granularity is needed, it becomes increasingly difficult to acquire data.

These two problems have one clear solution: centralized information obtained from the MNO instead of decentralized information acquisition. The exposed information from the MNO will correspond to the network performance absolutely, it need not be approximated. It will assist in determining the cause of performance problems - if the MNO does not report the problem but it is detected in the DSO network, this indicates that the problem is in the DSO network. If the MNO reports performance indicating a problem, then the DSO can focus on this rather than on investigating the root cause of the problem in their own network. The centralized measurements will be more efficient, can be of finer granularity, will be available even if the network performance seriously declines.

The acquired data is used, as described in clause C2, to determine when to initiate back up communication capabilities. These take some time (e.g. 2 minutes) to activate. Accurate, timely, sufficiently granular information can lead to better historical information, which correlates diverse behaviours of the network including service performance incidents. This can lead to improved understanding of service, such as periodic changes in service levels and on the other hand developments that have historically been associated with service level incidents.

In the latter, rare case, the DSO may elect to take proactive decisions. These proactive decisions will improve communication service availability. It is essential to maintain the best possible communication service availability to avoid even brief intervals of lack of availability of communication. If there is a specific need to monitor and manage the network during one of these intervals, it will not be possible to do so (i.e. by means of Distribution Automation or SCADA smart energy services), and this could lead to damage or an outage affecting energy service customers.

**Background**

See use case C.2.

### 6.1.2 Details

**Use Case Actors**

**DSO network operations centre engineer**: The DSO network operations centre engineer is responsible for deploying monitoring and control mechanisms in the network. The DSO network operations centre engineer determines how to control and configure the network for resiliency, e.g. when and how to switch between different accesses to maximize availability.

**DSO electrical system operations centre engineer**: This actor is responsible for maintaining availability, efficiency and safety of the energy system.

**Use case**

Service flow

1. The energy system is monitored and managed by the DSO electrical system operations centre engineer who relies upon a functioning network to communicate with electrical utility equipment in substation networks.

2. There are a set of substation networks with routers that include a UE for wide area communications. The DSO network operations centre engineer is responsible for this network. The DSO network operations centre engineer employs monitoring mechanisms to observe the performance of the telecommunications network over time, to capture historic data and continually watch for performance degradation indicating risk of an incident, as described in clause C.2.1 above. These monitoring mechanisms are exposed by the MNO, so that authorized third parties (including the DSO) are able to receive performance monitoring information.

NOTE: The alarms are provided at the network level, based on the overall statistical performance of the network. The alarms described here do not correspond to the performance of individual UEs or sessions.

3. The DSO network operations centre engineer, using the exposed monitoring mechanism interface, can request which metrics, under which conditions, will be provided. The interface provides a means by which the reports can be configured, including frequency and parameters to report.

Table 6.1.2-1: Report parameters

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Configuration | Expected Behaviour | Notes |
| latency | location (cell ID), frequency of reporting, granularity of reporting. | The report is provided by network exposure by the MNO. | The time of the measurement is crucial, so this information is included in the report delivered to the DSO. |
| throughput | location (cell ID), frequency of reporting, granularity of reporting. | The report is provided by network exposure by the MNO. | As above. |
| packet loss | location (cell ID), frequency of reporting, granularity of reporting. | The report is provided by network exposure by the MNO. | As above. |
| availability | location (cell ID) | The report is provided by the network exposed by the MNO. | As above. |

The information that are needed by the DSO will change over time, thus it is important that the DSO can configure the monitoring process, especially in terms of granularity.

4. The reports are delivered according to the above configuration.

Service flow result

When a problem develops, the DSO network operations centre engineer (or an automated management function) may trigger a fail-over to a backup network communications facility. This proactive and timely intervention can reduce or even eliminate the occurrence of incidents. Even if the activation of a back up communication facility occurs too late to entirely eliminate interval in which the DSO substation network components are unreachable or only reachable with inadequate quality of service, this interval will be significantly reduced.

### 6.1.3 Potential Requirements

PR 6.1.3-1. The 3GPP management system shall, according to mobile network operator policy, regulatory requirements and contractual obligations, expose standardized interfaces to authorized third parties that provide the ability to initiate and terminate requests for monitoring including the configuration of the monitoring (e.g. monitoring interval, measurement period granularity, location of interest, etc.)

Table 6.1.3-1: Information Elements and Management Functionality Mapping (see clause 7.1.2)

|  |  |  |
| --- | --- | --- |
| Purpose | Applied | Existing Management functionality or New Management Functionality |
| Determining monitoring configuration (monitoring interval, measurement period granularity) | Monitoring configuration is general and applied to any monitoring done to satisfy this requirement. | Existing: ThresholdMonitor IOC, monitorGranularityPeriod attribute of the ThresholdMonitor IOC |
| Determining location of interest (Lat/long, TAC, cell ID) | Monitoring location of interest will be used to scope the object instance to be monitored | Existing: targetThresholdlocation in ThresholdMonitor IOC |

PR 6.1.3-2. The 3GPP management system shall, according to MNO policy, regulatory requirements and contractual obligations, expose standardized interfaces to authorized third parties that provide a mechanism for the MNO to send reports containing required performance metrics measurements to the DSO. The measurements in these reports are provided in a form such that it will be possible to ascertain the number of measurements made as well as to calculate the standard deviation of those measurements, in order to aid in the interpretation of the reported measurement.

Table 6.1.3-2: Information Elements and Management Functionality Mapping (see clause 7.1.2)

|  |  |  |
| --- | --- | --- |
| Purpose | Applied | Existing Management functionality or New Management Functionality |
| Communicating Measurements | For any monitoring information provided by the MNO to the DSO. | Existing: Measurement [15] |

PR 6.1.3-3. The 3GPP management system shall support the following performance metrics to monitor information according to the associated configuration:

a) Latency between all served UEs and the corresponding base stations, at the granularity of a base station or network slice;

b) Throughput [an average for the base station's network traffic or network slice];

c) Packet loss [an average for the base station's network traffic or network slice];

d) Availability [an average for the cell's availability at a specific base station or at a (RAN) network level].

Table 6.1.3-2: Information Elements and Management Functionality Mapping (see clause 7.1.2)

|  |  |  |
| --- | --- | --- |
| Purpose | Applied | Existing Management functionality or New Management Functionality |
| Latency | Over Uu, for traffic between the UE and the base station (averaged); either for all traffic or for the network slice traffic. | Existing: As defined in clauses 5.1.1.1.1 and 5.1.1.1.3 in TS 28.552 |
| Throughput | As above | Existing: As defined in clauses 5.1.1.3.1 and 5.1.1.3.3 in TS 28.552 |
| Packet Loss | As above | Existing: As defined in clauses 4.2.1.5.1 in TS 38.314 for DL and in 5.1.3.1.1 in TS 28.552 for UL. |
| Availability | Availability (average) of cells. | New: To be defined (based on a cell's availability at the base station) |

PR 6.1.3-4. Authentication of the consumer (3rd party) by the producer (3GPP management system) shall be possible,

PR 6.1.3-5. Authentication of the producer (3GPP management system) by the consumer (3rd party) shall be possible.

PR 6.1.3-6. Authorization of the consumer (3rd party) by the producer (3GPP management system) shall be possible,

PR 6.1.3-7. Communication between the consumer (3rd party) and the producer (3GPP management system) shall be confidentially protected.

PR 6.1.3-8. Communication between the consumer (3rd party) and the producer (3GPP management system) shall be integrity protected.

## 6.2 Business use case: Energy utility and telecommunication coordinated recovery of energy service

### 6.2.1 Description

There is clearly a mutual interest in coordination between telecommunications and energy service operations to achieve rapid recovery of energy service. This is not only true for the MNO, who benefits from the availability of supplied power, but also of the DSO who needs mobile telecommunication service to restore and maintain the operation of its grid.

Energy service interruptions may occur in many parts of the energy system, ultimately effecting the end customer. This use case does not consider every service interruption scenario. It rather concentrates on one specific level of the system. The remainder of the task of efficient recovery is out of scope of this use case. Please consider the following model:

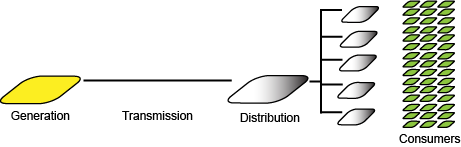


Figure 6.2.1-1: A simple model of the energy service delivery system

This use case concentrates on the distribution aspects, which is depicted above as a single level in a hierarchy, but in fact may have a series of sub-stations between high voltage transmission and the final distribution to energy consumers.

Interruptions occur in the distribution system, as at some level, the medium voltage network may require local reconfigurations or suffer unplanned loss of distribution service (e.g. due to distribution cable damage, etc.) The resulting energy service interruptions last a variable amount of time (from minutes to hours.)

The normal situation is that a utility may need to disconnect a certain Medium Voltage feeder. As the grid does not automatically re-connect this feeder to an active one, there will be a power outage in all points of supply connected to it while the power is being restored. The procedures and times to reconnect the affected feeder would be the same if for any reason this has been caused by a planned operation, an unexpected incident, or if it is a major grid problem.

In the recovery procedures, the DSO network operations centre needs to restore power in a certain order often for regulatory compliance: the order includes prioritizing the more important energy consumers (e.g., Hospitals, government sites).

This prioritization may also include major MNOs' sites, such as base stations and core network sites to restore communication services, which is in the interest of both MNO and DSO stakeholders. This prioritized recovery of MNO sites is enabled by this use case.

It is here where a standardized mechanism connecting DSOs and MNOs would be beneficial. This use case describes the information and operations that would be required on that interface.

Part of the information may have a more static nature.

This is the point of Energy Supply ID. The DSO is aware of each point of supply (to an energy consumer), by means of the Energy Supply ID. The MNO needs to let the DSO know the relevant Energy Supply IDs, so that the utility can know where they connect to its feeders. Another critical information element is the power back up installed by the MNO in each site (including 'back up' base stations), and its current expected duration. In addition, for each Energy Supply ID, base station, e.g. eNB, IDs (serving the cell IDs) served by the base station as shown in figure 6.2.1-2 below.

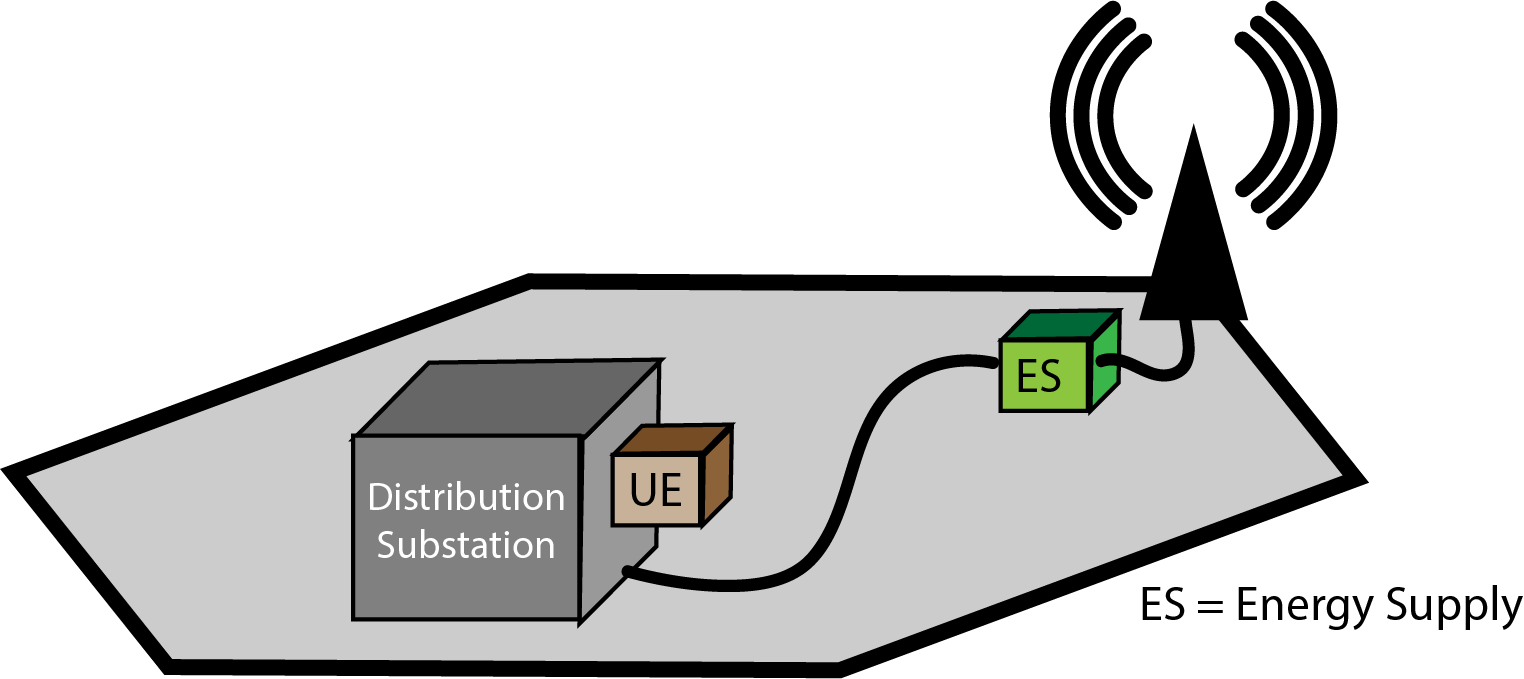


Figure 6.2.1-2: Local recovery scenario

NOTE 1: The representation of the ID above corresponds to the Energy Supply termination of the base station site.

The correspondence between the communication system serving the distribution substation by means of a UE (camped in the depicted cell), the Energy Supply ID of the base station and the ID of the base station enables the DSO to identify important operational aspects, such as:

(a) the impact of the distribution substation interrupting service: specifically the base station that the distribution substation relies on will have its power supply interrupted;

(b) upon recovery of the distribution substation, which substations may be high priority for resumption of service.

As implied in Figure 6.2.1-2, there is a dependency that the DSO has on the MNO in that the DSO relies upon data connectivity to smart energy equipment in the distribution system. Through the use of smart energy services, restoration of energy service is rapid and reliable. If the energy substation lacks data connectivity, it is sometimes necessary to send a technician to the site to restore service, which is time consuming.

Within the distribution substation is a router, a kind of customer premises equipment (CPE) that communicates as a router that supports a mobile interface, shown as the UE. Beyond the CPEs DSO Remote Terminal Units (RTUs) are connected. The DSO monitors and controls the RTUs as part of normal operations, especially in the event of a service outage.

Other information exposed by the new mechanism is dynamic.

The figure below depicts the situation at the time of a failure and what is needed in order to restore energy service.

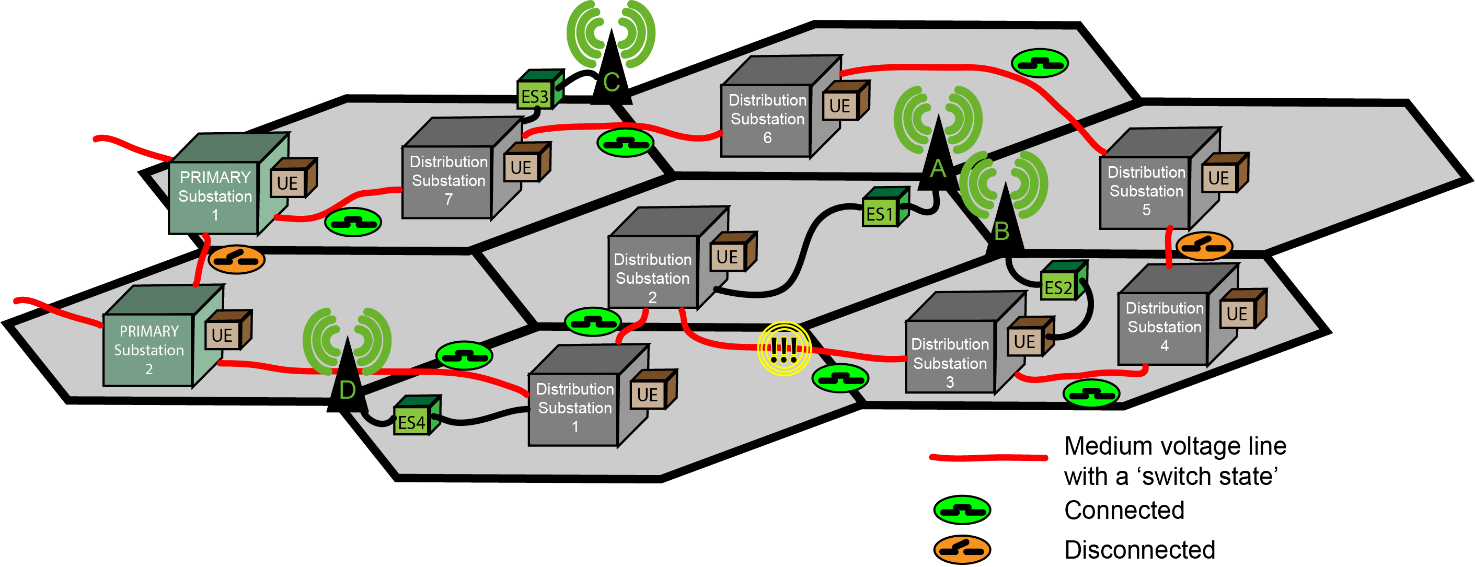


Figure 6.2.1-3: Local failure event

NOTE 2: In Figures 6.2.1-3 and 6.2.1-4, the green cubes labelled 'ES' represent energy supply points, associated with an Energy Supply ID.

The red lines above are medium voltage lines between energy distribution substations (DS). Note that initially Primary Substation (PS) 1 feeds DS7, DS6 and DS5, and PS2 feeds DS1, DS2, DS3 and DS4.

Between DS2 and DS3 there is a distribution failure. This has the result of causing DS3 and DS4 to no longer be able to maintain the energy distribution service to customers.

Note that the topology of energy distribution lines is redundant. In order to achieve distribution successfully through this redundant topology, energy service has to be **switched** **on and off** at corresponding distribution substations. This for example could be done between DS4 and DS5 to feed restore service to all substations. The switching is disruptive of energy service. For some time, energy supplied by the distribution substation to the energy customers is off-line. This would result in the following topology:

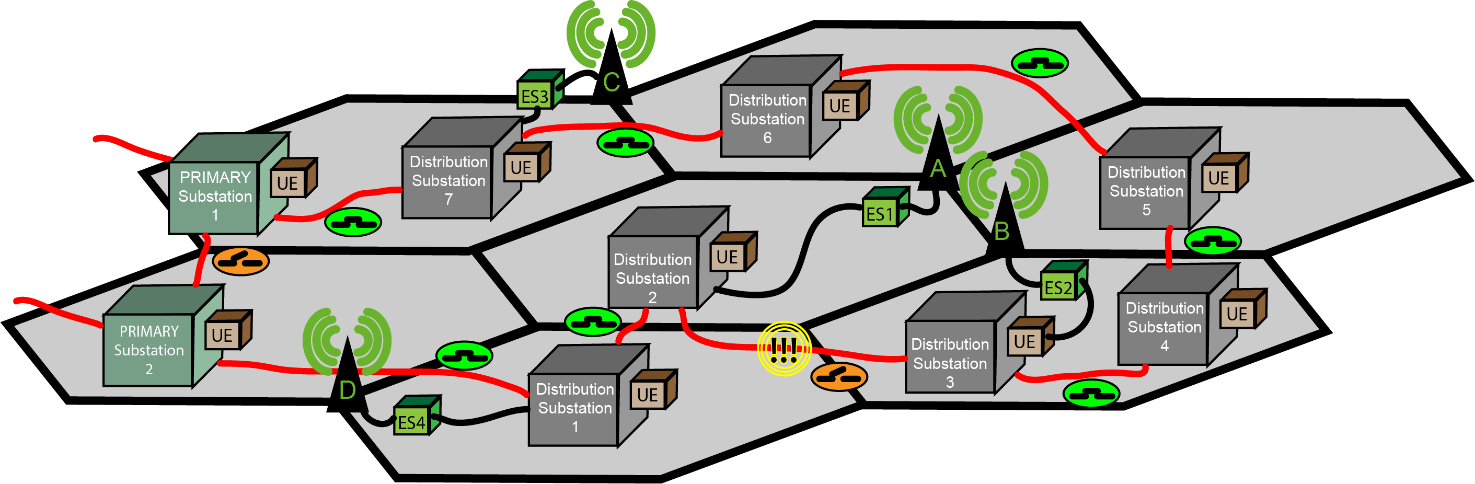


Figure 6.2.1-4: Local failure restored

The topology in Figure 6.2.1-4 is altered so that DS4 and DS5 are now connected, accepting the medium voltage line between DS2 and DS3 are disconnected. PS1 and PS2 remain disconnected; they represent another level of redundancy in the system.

If the process of switching on and off until a stable configuration is achieved has to be done **manually** the process can take considerable time (e.g. hours) as technicians has to be on-site to control the substation configuration. The technicians have to communicate, e.g. using mobile telecommunications. However, if the process takes a long time - the mobile telecommunication infrastructure, as shown by base station A and base station B, will likely have exhausted their Uninterruptable Power Supply (UPS), further complicating recovery procedures.

The alternative investigated in this use case involves taking into account the configuration (as described in Figure 6.2.1-2) and dynamic information obtained from the 3GPP network management system concerning the **current capacity (expected remaining duration of service) of the UPS in each of the MNO's infrastructure sites.**

Using smart energy services (principally Distribution Automation), it is possible to perform the 'switch on and off' procedures rapidly, within minutes, and reconfigure the network. There will still be transient electrical service outages to the customers that the distribution substations serves.

Taking into account (a) which mobile network infrastructure sites (i.e. base stations) are critical to service and which cells they serve, (b) the corresponding Energy Supply ID, (c) the distribution substation (UEs) that rely on these base stations, (d) the remaining UPS capacity available in the sites, it is possible for the DSO to plan the 'switch on / switch off process' to avoid any interruption of service. This is done by **selective ordering**of the switch on / switch off activity, to avoid exhausting any mobile network infrastructure UPS - especially where this base station (etc.) serves to enable communication services to a distribution substation.

Note that in figure 6.2.1-3, the cell in which each is located is served by a base station that can be affected by 'switching off.' It is also known to the DSO that e.g. DS2 is served by A and (secondarily) by base station B. Knowledge of this redundancy can also be of benefit to the planning of the DSO, to prevent in the worst case that both base stations UPS capacity is exhausted and there is no way to restore energy service to these sites.

In order to support the process described above, another example of dynamic real-time information is the 'real' current back up power available at the base station, at any moment in time; the intention is to see how much time the DSO has to restore the power before service interruption compromises the MNO's operation.

### 6.2.2 Details

**Use case actors**

**DSO network operations centre 'management system'**

The DSO network operations centre management system (DSO-MS) maintains operational information to inform DSO network operations.

**MNO network operations centre 'management system'**

The MNO network operations centre management system (MNO-MS) has and can expose operational information to DSOs concerning the network's configuration and status.

The MNO-MS is a 3GPP management system and the DSO-MS is not a 3GPP management system, however it supports mechanisms that are defined by 3GPP standards (e.g. it uses 'northbound interfaces' exposed by the 5G network management system.)

**Use case service flow**

Preconditions:

There is a feeder, whose operation requires smart energy services. The smart energy services are available through DSO equipment RTUs. These RTUs are connected with a router, a CPE in the DSO site, that supports a mobile telecommunications interface, a UE.

The DSO can obtain information from each UE in the DSO network. The DSO-MS is aware of the Base station ID of the serving base station for each UE.

On a regular basis, e.g. daily, the DSO-MS obtains 'static information' from the MNO-MS. The DSO-MS is aware which base stations each of the DSO's UE camp on. The DSO-MS is also aware of which base stations rely on which Distribution Substation.

**Service Flow: MNO-DSO coordination to achieve rapid energy service outage recovery**

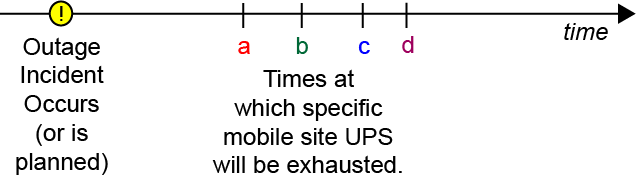


Figure 6.2.2-1: Timeline for Restoration of a Distribution Substation

1. The DSO-MS uses the standardized mechanism to identify an energy service outage at a particular Distribution Substation (or set of Distribution Substations).

This is shown in Figure 6.2.2-1 as the time of the outage incident.

2. The DSO-MS uses the standardized mechanism to request information from the MNO-MS, to identify the UPS capacity of the base stations in the vicinity of the outage, where the distribution substations will need to be switched on and off. This is shown in Figure 6.2.2-1 as a, b, c, d which correspond to base stations A, B, C and D.   
  
This request may be done repeatedly, over time, so that the DSO-MS can track the status of the MNO-MS. The MNO-MS may inform the DSO-MS of the current UPS status for a specific Energy Supply ID.

3. The DSO-MS can use the standardized mechanism to inform the MNO-MS of which sites (using the Energy Supply ID known by both the MNO and the DSO) will experience an outage. The DSO can inform the MNO in advance of a planned outage, e.g. when switching on and off will take place.

4. The DSO will actively switch on and off the medium voltage topology at the different distribution stations seeking to establish a stable and sufficient topology. The DSO will prioritize switching involving DS1 so that the UPS of base station A is not exhausted, because 'a' will expire first as shown in Figure 6.2.2-1.

5. A stable and sufficient medium voltage distribution topology is established without exhausting any of the UPS capacity of the base stations and other critical mobile infrastructure sites.

Post-conditions:

The DSO-MS has informed the MNO-MS before, during and after an energy service outage.

The DSO-MS has been able to obtain dynamic UPS information corresponding to mobile infrastructure sites throughout the recovery process.

Service Result:

Energy service is restored to the MNO sites and to the rest of the DSO's energy service customers efficiently, without requiring mobile manual intervention.

### 6.2.3 Potential Requirements

PR 6.2.3-1. The 3GPP management system should support, subject to operator policy, regulatory requirements and contractual obligations, the for the DSO to obtain the following information from the site operator.

For each 'site' for which energy service is critical to the site operator:

- Energy Supply ID

- UPS Capacity of the site (at the time at which this information is obtained);

- Base Station ID (if applicable. The site may not be a base station, e.g. it could be data centre or other facility.)

PR 6.2.3-2. The 3GPP management system should support, subject to operator policy, regulatory requirements and contractual obligations, the capability to enable the DSO to provide the site operator with information concerning the beginning of an energy service outage and the effected sites (e.g., Energy Supply IDs, Base Station IDs).

PR 6.2.3-3. The 3GPP management system should support, subject to operator policy, regulatory requirements and contractual obligations, the capability to enable the DSO to obtain information from the site operator concerning the UPS capacity corresponding to a specific site (e.g., Energy Supply IDs, Base Station IDs).

PR 6.2.3-4. The 3GPP management system should support, subject to operator policy, regulatory requirements and contractual obligations, the capability to enable the DSO to inform the site operator concerning the end of an energy service outage and the related sites (e.g., Energy Supply IDs, Base Station IDs).

PR 6.2.3-5. The 3GPP management system should support, subject to operator policy, regulatory requirements and contractual obligations, the capability to inform the DSO of any energy service outage to specific sites (e.g., Energy Supply IDs, Base Station IDs).

PR 6.2.3-6. Authentication of the consumer (3rd party) by the producer (3GPP management system) shall be possible,

PR 6.2.3-7. Authentication of the producer (3GPP management system) by the consumer (3rd party) shall be possible.

PR 6.2.3-8 Authorization of the consumer (3rd party) by the producer (3GPP management system) shall be possible,

PR 6.2.3-9. Communication between the consumer (3rd party) and the producer (3GPP management system) shall be confidentially protected.

PR 6.2.3-10. Communication between the consumer (3rd party) and the producer (3GPP management system) shall be integrity protected.

## 6.3 Business use case: Rapid intervention for outages without redundant energy feeder topology

### 6.3.1 Description

This use case is a variation on clause 6.2 above.

In 6.3, a redundant topology offers the opportunity to adjust the switching of medium voltage lines for energy distribution. When there is a failure of one of these lines, it is possible to adjust the topology to re-establish energy supply to all distribution substations.

This possibility exists only if there is a redundant topology. There are scenarios in which there is no redundant topology, either because a substation is remotely located or because the redundant topology is sufficiently damaged that a sufficient network cannot be re-established. This use case addresses these scenarios.

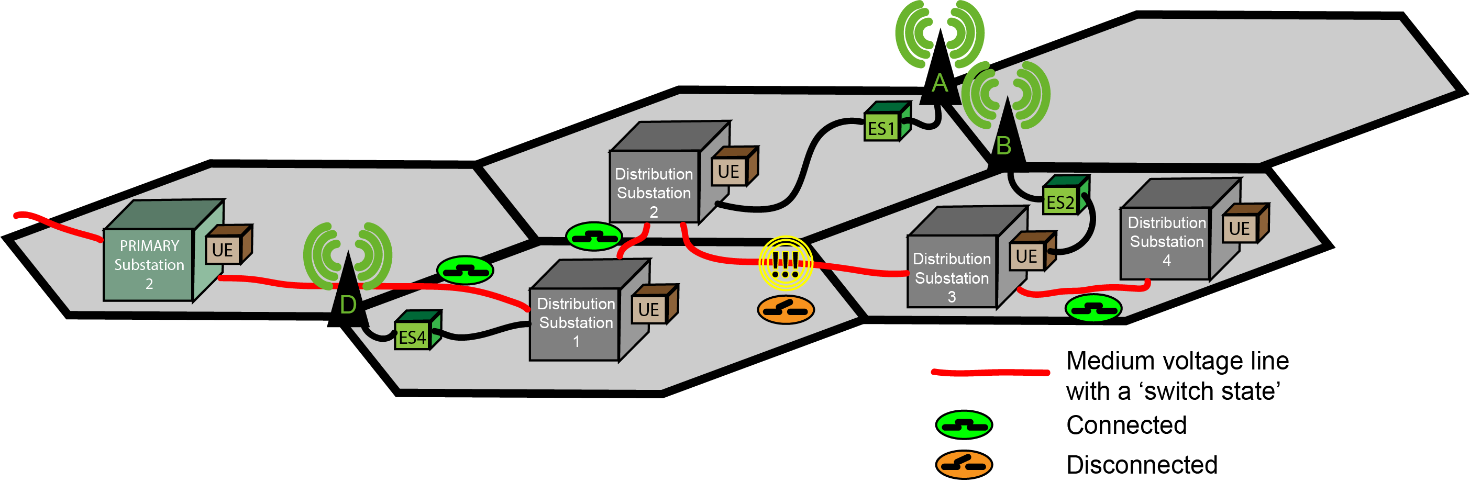


Figure 6.3.1-1: Local Failure Event of feeder of Distribution Substations without Redundant Topology

In figure 6.3.1-1, there is a failure in the distribution line between Distribution Substation 2 and Distribution substation 3. This will result in a failure to supply energy to ES2, and thereby base station B.

In this use case, it is necessary to re-establish the energy supply between substation 2 and substation 3 prior to resuming service in substation 3 and 4.

Once this has been re-established the topology is restored as shown in Figure 6.3.1-2.

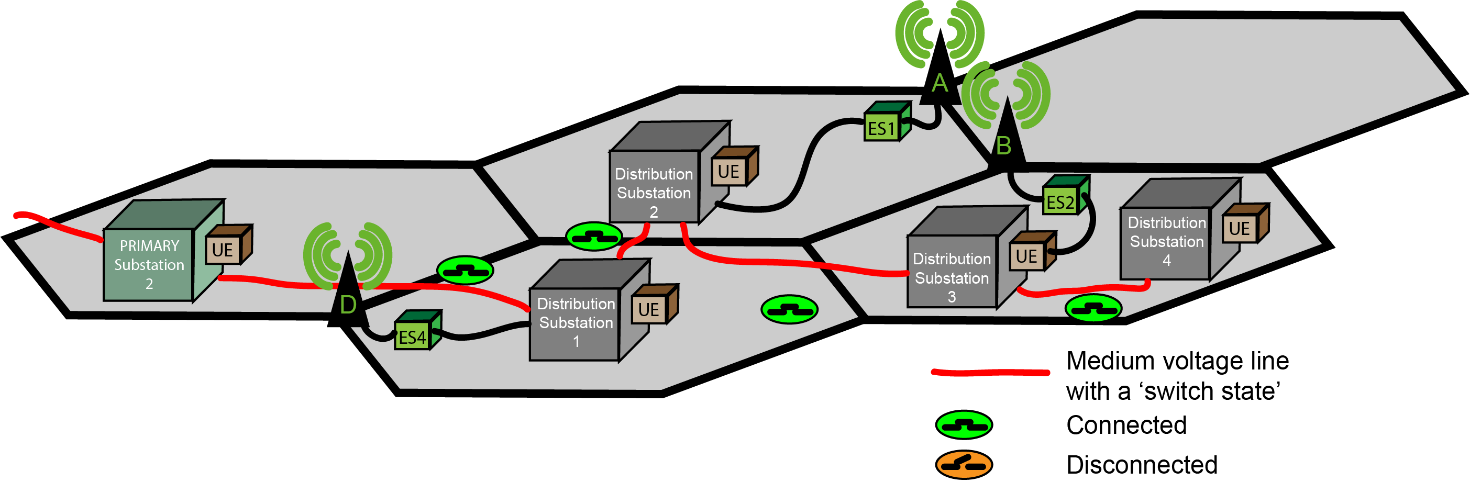


Figure 6.3.1-2: Restored Energy feeder to Distribution Substations

At the point when the distribution is again possible, it is necessary to resume service at distribution substation 3 and 4. However, as some time has elapsed, the UPS capacity of B will be exhausted. This will mean that any smart energy automated operations to distribution substation 3 and 4 will be impossible. Manual intervention to restart service will require substantially more time than automated response.

For this reason, this use case suggests a new operational capability to achieve rapid coordinated recovery. In this approach the DSO informs the site operators to reserve UPS capacity in certain sites, so that it will be possible to resume telecom operationssubsequent to the resumption of energy distribution service. If energy distribution service does not resume, after the UPS capacity becomes exhausted, telecom operations will become impossible.

### 6.3.2 Details

**Use case actors**

**DSO network operations centre 'management system'**

The DSO network operations centre management system (DSO-MS) maintains operational information used for DSO network operations. The DSO-MS supports interfaces defined in this use case. All other aspects of the DSO-MS are out of scope of 3GPP specification. The DSO-MS is a consumer of the 3GPP management system.

**Site Operator network operations centre 'management system'**

The site operator network operations centre management system (SiteOp-MS) has and can expose operational information to DSOs concerning the network's configuration and status. The SiteOp-MS as discussed in this use case can be considered a producer of management interfaces consumed by the DSO-MS. The SiteOp-MS is effectively a standardized subset of interfaces and semantics of the 3GPP management system. The SiteOp-MS is a 3GPP management system for 5G and the DSO-MS is not a 3GPP management system, however it supports mechanisms that are defined by 3GPP standards (e.g. it uses 'northbound interfaces' exposed by the 5G network management system.)

**Use case service flow**

Preconditions:

The purpose of the following description is to explain the scenario in which the energy utility operates a network by means of diverse accesses. It is important to mention that other access systems are used to access the energy utility site networks as well, but only access via the mobile telecommunication system is in of scope of this use case.

An energy utility maintains many energy distribution substations. Each is an energy utility infrastructure site that is responsible for distribution of energy to customer sites. This energy utility infrastructure site's operation requires smart energy services. The smart energy services are used to manage and control DSO equipment. This equipment is present on a local area network in the energy utility infrastructure site, which is accessed (e.g. as a VLAN) over any access. In this use case, the access that is used is 3GPP access. A UE is used effectively to carry DSO energy utility infrastructure site communication opaquely (that is, as encrypted traffic) to the Utility Service Provider Network. For background information on this scenario, see TR 22.867, clause 5.7 [6].

The DSO can obtain information from each UE that is used to provide access to the DSO networks. The DSO is, by means of this information obtained from UEs in the DSO network, aware of the Base station ID of the serving base station for each UE.

On a regular basis, e.g. daily, the DSO-MS reads information from the SiteOp-MS exposed 3GPP management system MnS Producer's exposed interfaces. The DSO-MS is aware which base stations each of the DSO's UE camp on. The DSO-MS is also aware of which base stations rely on which Distribution Substation.

Service Flow:

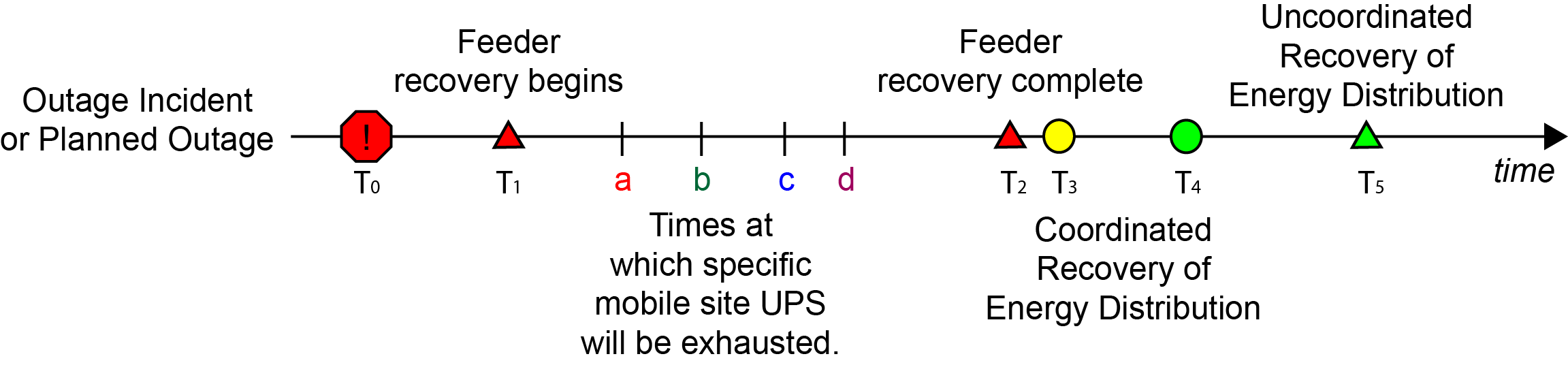


Figure 6.3.2-1: Timeline for Restoration of a Distribution Substation

1. At some time (T0) there is an outage incident either a planned or unplanned incident.

2. The DSO-MS uses the standardized mechanism to request information from the MNO-MS, to identify the UPS capacity, including remaining time of operation, of the base stations in the vicinity of the outage, where the distribution substations will need to be switched on and off.  
  
This request may be done repeatedly, over time, so that the DSO-MS can track the status of the MNO-MS. The MNO-MS may inform the DSO-MS of the current UPS status for a specific Energy Supply ID.

3. At some subsequent time (T1), the energy utility begins restoration of energy feeder lines or other affected infrastructure.

4. The period of time that will elapse before the restoration of energy service from some set of distribution substations will be longer than the UPS capacity of the mobile infrastructure sites. This use case assumes that the MNO knows or can estimate the remaining time of operation after T0 given the UPS capacity of different mobile infrastructure sites, as received in step 2, shown as a, b, c, d in Figure 6.3.2-1. That is, T2 occurs *after* the UPS capacity is exhausted in the sites affected by the energy outage. This use case assumes that the DSO knows or can estimate time at which energy distribution service can resume, shown as T2 in figure 6.3.2-1. This may not be the exact time at which resumption of energy service can resume, which is shown as T3. T2 is an estimate when the energy feeder will have recovered, while T3 represents the time at which energy feeder service resumes and restoration of distribution is possible.

5. The energy feeder for one or more energy distribution substations is now complete. At this point, it will be possible to restore energy distribution. However, operations are required at the distribution substation. This can be performed by smart energy services remotely if there is network coverage. The starting time, when the MNO provides service with remaining UPS capacity, is shown in Figure 6.3.2-1 as T3. The smart energy services to restore energy distribution services to all customers, including the MNO, is shown as T4.

There are two alternatives for how the restoration can occur. Manually, as described in 6a, or with remote intervention, as described in 6b.

6a. Without prior arrangement, there will be no UPS capacity remaining in the infrastructure that serves the distribution substations that have restored power. They will not be able to perform automated recovery, as explained in use case C.4. In this case, manual intervention is required to restore energy distribution. This will be complete after a substantial period of time (T5).

6b. Alternatively, prior arrangement can be made so UPS capacity will remain in the infrastructure at the time it is needed to restore energy distribution service. This prior arrangement is described in the steps below, and consists of operations between the DSO-MS and MNO-MS.

This is to enable the situation that, at time (T3), the MNO is able to use remaining UPS capacity to offer telecommunication service at the time at which the DSO will perform remote operations by means of data communications to restore service in the sites affected by the outage, and operates them until the outage concludes.

6.b.1. In this use case, the DSO-MS communicates to the MNO-MS:

- the affected sites (identified by the associated Energy Supply IDs) by the outage

- the time X after which recovery is possible

- the time Y (that is a certain interval of time after X) that the recovery is expected to complete (a small number of minutes)

The site operator, knowing this, has the opportunity to manage the use of the UPS in the affected sites so that they do not exhaust at time (a, b, c, d, etc.). Rather, capacity sufficient for operation of the base station between time X and Y is reserved. Figure 6.3.2-2 below shows a concrete example of this interaction.

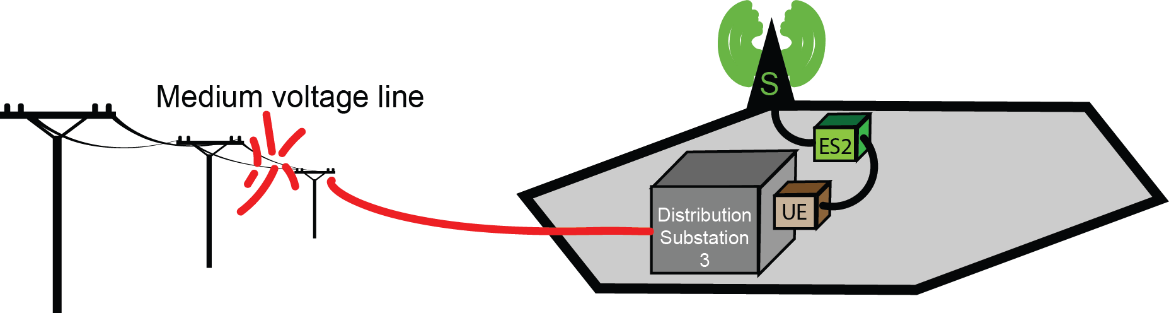


Figure 6.3.2-2: Example of Restoration Scenario of a Distribution Substation

Table 6.3.2-1: Example Sequence of Restoration of a Distribution Substation

|  |  |
| --- | --- |
| Time | Event |
| 00:34 | A storm rages and causes power lines to collapse in the mountain province. Energy distribution service by Distribution Substation 3 is no longer possible! |
| 00:36 | The DSO informs the MNO that there has been an energy distribution incident that will affect site S. The DSO expects to repair the medium voltage line by 02:45, and if telecommunications service permits it, remote control (using Distribution Automation and SCADA controls) of all sites served by Distribution Substation 3 can be restored - by 02:50.  In terms of the procedure step 5a, X=0:2:45, Y = 5 minutes. |
| 00:40 | The MNO conserves energy as appropriate to conserve 5 minutes of operating capacity of their UPS reserve. |
| 02:38 | The DSO informs the MNO that the feeder line is restored. Remote control restoration of service can begin now. This is T2 in Figure 6.3.2-1. |
| 02:43 | The MNO resumes operation at site S. The DSO is informed that the service has resumed. |
| 02:47 | The DSO completes distribution automation. Site S now has energy service. This is T4 in Figure 6.3.2-1. |

6.b.2. The DSO, after time (T3), employs smart energy services such as distribution automation or specific SCADA operations to restore service to customers rapidly, including the site operator.

6.b.3. The incident concludes (T4). Energy distribution service has been restored to the MNO site(s) as well as other energy service customers.

6.b.4 The DSO-MS notifies the MNO-MS that the restore operation is complete.

Service flow result

T4 occurs before manual uncoordinated recovery of service would be successful (T5 in Figure 6.3.2-1.) Thus, alternative 6.b is superior to 6.a for both the site operator and the DSO.

Service is restored to distribution substation 3 and 4 at T4, within minutes of the restoration of the medium voltage line between distribution substation 2 and 3 T3. This is substantially faster than service could be restored if a technician had to visit distribution substation 2 and 3 - represented on Figure 6.3.2-1 as T5. As a result, service is restored to the MNO sites affected more rapidly than in an uncoordinated incident.

### 6.3.3 Potential requirements

This use case also has potential requirements 6.3.3-1 through 6.3.3-10. These requirements, if supported, enable the site operator to voluntarily discontinue service, retain UPS capacity, and wait until an opportune time to restore service. This is subject to operator policy, contractual obligations and regulatory restrictions.

For all the requirements below, supported interaction is described between the DSO and the MNO (or site operator). The reason for this term 'site operator' is that in network sharing scenarios, the base station and/or cell site may be operated by a third party. In active network sharing scenarios the DSO can communicate with an site operator that operates the site, but can be distinct from the serving site operator. The interaction described is really between the DSO and the management services of the entity that operates the site essential for telecommunication service, identified by the energy supply ID.

PR 6.3.3-1. The 3GPP management system should expose management services, subject to operator policy, to enable the DSO to provide the MNO (or site operator) with information concerning the expected restoration time of its distribution services for site operator for effected sites.

PR 6.3.3-2. The 3GPP management system should support, subject to operator policy, the capability to enable the DSO to provide the MNO (or site operator) with information concerning the time when DSO restores its Energy "transmission" service. At this time the DSO needs the MNO's (or site operator's) communication services to be able to use its automated energy services for rapid remote recovery of energy distribution services.

PR 6.3.3-3. The 3GPP management system should support, subject to operator policy, the capability to enable the DSO to provide the MNO (or site operator) with information concerning the time duration for which DSO expects to require MNO's (or site operator's) communication services to achieve coordinated recovery for being able to use smart energy services to restore its energy distribution services. The time that the DSO provides to the MNO (or site operator) can be adjusted as new information becomes available. The time estimate specifies which base stations are needed for the remote recovery operations.

PR 6.3.3-4. The 3GPP management system should support, subject to operator policy, the capability to enable the DSO to provide the MNO (or site operator) with information concerning the locations where for example DSO substations need to restore distribution services on priority. Location information expressing where restoration will occur could be expressed in terms such as latitude-longitude pairs or Energy Supply Id.

PR 6.3.3-5. The 3GPP management system should support, subject to operator policy, the capability to enable the site operator to provide the DSO with information concerning the time at which MNO (or site operator) should actually be able to provide communication services to achieve coordinated recovery to DSO for a particular region.

PR 6.3.3-6. The 3GPP management system should support, subject to operator policy and other conditions, the capability to enable the DSO to provide the site operator with information concerning the time duration for which site operator would actually be able to provide communication services to achieve coordinated recovery of DSO's energy distribution services for a particular region.

PR 6.3.3-7. Authentication of the consumer (3rd party) by the producer (3GPP management system) shall be possible,

PR 6.3.3-8. Authentication of the producer (3GPP management system) by the consumer (3rd party) shall be possible.

PR 6.3.3-9. Authorization of the consumer (3rd party) by the producer (3GPP management system) shall be possible,

PR 6.3.3-10. Communication between the consumer (3rd party) and the producer (3GPP management system) shall be confidentially protected.

PR 6.3.3-11. Communication between the consumer (3rd party) and the producer (3GPP management system) shall be integrity protected.

PR 6.3.3-12. The 3GPP management system should support, subject to operator policy, the capability to enable the site operator to provide the DSO with information about locations where MNO (or site operator) will actually be able to provide dedicated communications services to achieve coordinated recovery of DSO's energy distribution services.

# 7 Key Issues and potential solutions

## 7.1 Key Issue #1: MNO exposes network performance monitoring

### 7.1.1 Description

This describes the issues to be studied in context of the use case of MNO exposes Network Performance Monitoring. This corresponds to the use case and associated requirements in 6.1. The requirements from C.5 are not addressed by this key issue: alarms and fault management are not considered by the solutions corresponding to this key issue.

This key issue is that DSO has to be an MNO trusted entity to access MnSes provided by the 3GPP Management System. The existing performance assurance mechanism can be used to report network performance to DSO. However, the following need to be studied

a. How the existing ThresholdMonitor can be used for configuring the network monitoring.

b. How the existing NtfSubscriptionControl can be used for sending reports as notifications against monitoring.

c. Whether the existing performance measurements [13] and KPIs [12] are enough to support the requirements (e.g. latency, throughput, packet loss, availability etc.)

### 7.1.2 Potential solutions

#### 7.1.2.1 Potential Solution #1: MNO exposes network performance monitoring

##### 7.1.2.1.1 Introduction

This solution addresses Key Issue 1 and the requirements in clause C.6.

The solution assumes that DSO is an MNO trusted entity and can access MnSes provided by the 3GPP Management System. In this solution, the existing provisioning MnS and related NRM fragments are used. DSO uses ThresholdMonitor to configure the related threshold for various network performance requirements e.g. latency, throughput, packet loss, cell/network availability etc. DSO also uses the NtfSubscriptionControl to subscribe for NotifyThresholdCrossing notifications. The management system monitors the network and delivers the notification when the measurement or KPI crosses the configured threshold limit.

Depending on the configuration of the monitorGranularityPeriod attribute of the ThresholdMonitor, the DSO can identify the frequency of the threshold to be checked, post which the notification will be sent.

The returned Measurements conform to the Measurement Template [15], which identifies each individual measured value distinctly. Thus, it is possible to ascertain from the report the number of samples per measurement as well as the distribution of the data (e.g. to compute the standard deviation.)

##### 7.1.2.1.2 Description



Figure 7.1.2.1.2-1: Monitoring Configuration Procedure

1. DSO sends createMOI request for perfMetricJob IOC to Performance Assurance Producer.

NOTE: The configured reporting mechanisms (file or stream) are established in this step.

2. createMOI response is sent by Performance Assurance Producer to DSO.

3. Performance Assurance producer creates the PM jobs on the specified object instances.

4. Performance Assurance Producer provides the required measurements and KPIs to DSO based on the configured reporting mechanisms (file or stream).

5. DSO sends createMOI request for ThresholdMonitor IOC to Performance Assurance Producer.

5a. The attribute performanceMetrics, contains the measurements defined for each of the network performance requirements as required by DSO e.g. latency, throughout, packet loss, availability etc.

5b. It also contains an attribute containing the location (Lat/long, TAC, cellid). This is used to scope the object instance to be monitored.

6. Performance Assurance Producer creates the MOI.

7. createMOI response is sent by Performance Assurance Producer to DSO.

8. DSO sends createMOI for NtfSubscriptionControl IOC to performance Assurance Producer.

8a. The attribute notificationRecipientAddress contains the address of the notification recipient i.e. DSO.

9. Performance Assurance Producer creates the MOI.

10. createMOI response is sent by Performance Assurance Producer to DSO.

11. Performance Assurance Producer checks for threshold crossing based on the current state of the related performance measurement.

12. Performance Assurance Producer sends notifyThresholdCrossing notification to DSO if the performanceMetrics value crosses the configured thresholdValue.

#### 7.1.2.2 Potential Solution #2: MNO exposes network performance monitoring

On one hand the DSO is interested in actual occurrences of threshold crossing events as described above. On the other hand, the DSO needs to be notified in advance about pending threshold crossings. The 3GPP management system may inform the DSO about the predicted end of a threshold-crossing condition. This information may be used to support the DSO regarding the coordination of recovery actions.

As a solution the 3GPP management system could notify about predicted threshold-crossing or alarming conditions, including the predicted start and end time of such conditions.

The corresponding sequence of steps is similar to the description of actual threshold crossings, except that the notifications inform about predictions of threshold crossing events.

## 7.2 Void

## 7.3 Key Issue #3: Energy utility and telecommunication coordinated recovery of energy service

### 7.3.1 Description

#### 7.3.1.1 General

This describes the issues to study in context of the use case of Energy utility and network operator coordinated recovery of energy service.

There is clearly a mutual interest in coordination between MNO and energy service operations to achieve rapid recovery of energy service. This is not only true for the MNO, who benefits from the availability of supplied power, but also of the DSO who needs mobile telecommunication service to restore and maintain the operation of its grid.

NOTE: Though DSOs use many forms of access (e.g. fixed access, dedicated fibber access, etc.), they increasingly rely on telecommunications services for communication access to many substations and other facilities. It therefore directly benefits the overall availability of communication service for the energy utility when the availability of the telecommunication service improves. The Energy utility provider (DSO) knows when and where outage has occurred and when telecommunication services are critically important for recovery. The MNO knows their uninterruptable power supply resources and the possibility of utilizing telecommunication services to enable utility's energy system rapid recovery via smart energy services.

Without a standardized mechanism to share all this information, the service recovery mechanism would be very inefficient and time consuming. Therefore, a standardized mechanism is needed to share all this information between DSO and MNO to enable efficient usage of smart energy services for service recovery.

#### 7.3.1.2 Coordinated recovery of energy service with redundant topology

The functions described here correspond to the requirements in the use case 6.2 "Business use case: Energy utility and telecommunication coordinated recovery of energy service".

a) How can the DSO obtain the information from the MNO that is listed in PR 6.2.3-1?

b) How can the DSO provide the MNO with information concerning the beginning of an energy service outage and the affected sites? [PR 6.2.3-2]

c) How can the DSO obtain the UPS capacity related info of a specific site from the MNO? [PR 6.2.3-3]

d) How can the DSO inform the MNO of energy service outages ending and the affected sites? [PR 6.2.3-4]

#### 7.3.1.3 Coordinated recovery of energy service without redundant topology

The functions described here correspond to the requirements in the use case 6.3 "Business use case: Rapid intervention for outages without redundant topology".

The key issue topics described in clause 7.3.1.2 has to be resolved for this key issue. In addition, the following key issues need to be addressed.

a) How does the DSO provide the MNO with information concerning the *expected time* at which the DSO will be able to restore its energy services? [PR 6.3.3-1]

b) How does the DSO provide the MNO with the *time* at which it has restored its energy transmission service? [PR 6.3.3-2]

c) How does the DSO provide the MNO with the *time duration* that the DSO expects to require to restore energy services, facilitated by telecommunication services? [PR 6.3.3-3]

d) How does the DSO inform the MNO of the locations affected by an energy service outage (latitude-longitude pairs, energy supply IDs) where the DSO would like to restore service on priority than some other locations? [PR 6.3.3-4]

e) How does the MNO inform the DSO of the *actual time* and *locations* (e.g. base station IDs) where the MNO is *able* to provide telecommunication services to enable the DSO to restore energy service? [PR 6.3.3-5]

f) How does the MNO inform the DSO of the *time duration* for which the MNO is able to provide telecommunication services to enable the DSO to restore energy service? [PR 6.3.3-6]

### 7.3.2 Potential Solutions

#### 7.3.2.1 Potential Solution # 1: Energy utility and telecommunication coordinated rapid recovery of energy service

##### 7.3.2.1.1 Introduction

The solution addresses key issues of Energy utility and telecommunication coordinated rapid recovery of energy service. It involves mutual exchange of information between an energy utility (DSO) and MNO using mechanisms exposed by 3GPP network management system. The mechanisms are for rapid recovery of utility's energy service outage and subsequent fallback by MNO from its UPS to utility's energy supply for MNO communications service/network operations. The solution also involves mechanisms to protect MNO sites from complete breakdown in case of UPS running out of its capacity due to prolonged DSO energy service outage. The DSO informs about its energy service outages like time of outage, locations, expected recovery time etc. to MNO. MNOs Rapid Intervention (MRI) is the approach by which DSO seeks dedicated communication service support from MNO using its UPS backup for network operations. DSO needs this to use its automated smart energy services for the rapid recovery of its energy distribution services.

The site operator has information on the state of its power backup e.g. UPS backup duration at different base station locations, base station IDs that are enduring DSO's power outage and are depending on UPS backup, base stations that provide communications services to DSOs substations for smart energy services implementation etc.

The UPS capacity can be obtained using the IETF standard UPS Management Information Base [19]. Another possibility to obtain the UPS capacity information is to use the ETSI standard ETSI ES 202 336 [18].

The DSO can obtain these UPS related information from the MNO and can avoid shutting down of energy service for base station IDs that their UEs camp on or for the critical MNO infrastructure that have insufficient UPS backup capacity to survive the planned outage. The DSO can potentially create the strategic energy service interruptions as long as there is sufficient UPS backup capacity remaining for the duration of the outage at the MNO site.

##### 7.3.2.1.2 Description

The procedure below includes the interactions required between the DSO MnS and MNO MnS in order to satisfy the operational requirements in key issue 7.3.1.2 and 7.3.1.3. The procedure is general in that it can be extended to other attributes easily, and it is based on existing mechanisms specified by SA5.

1. createMOI () Request

**DSO**

(MnS Consumer)

**MNO**

(MnS Producer)

3. createMOI Response

2. MOI will be created

5. createMOI(IntfSubscriptionCtrl) Request

4. IOC containing

UPS info instantiated

6. MOI will be created

7. CreateMOI Response

8. notifyMOIAttributeValueChanges

9. modifyMOIAttributes Request

10. modifyMOIAttributesResponse

11. getMOIAttributeRequest

12. getMOIAttributeResponse

**Initialization**

**MNO informs DSO of the changes**

**DSO updates the information**

**DSO retrieves the changes**

Figure 7.3.2.1.2-1: Coordinated Rapid Recovery and strategic outage plan Procedure

NOTE 1: Steps 1-7 in the procedure flow can be considered 'initial set up' to enable operations to address the functional requirements in clauses 6.2 and 6.3 and described in Key Issues 7.3.1.2 and 7.3.1.3.

1. In order to be able to provide energy service outage and recovery related information for MNO, DSO sends createMOI request for creating an IOC which contains information attributes for outage and rapid recovery by DSO such as:

a) Time stamp of DSO's energy distribution service outage

b) Locations (latitude-longitude pair and Energy Supply Id) where DSO's energy service outage occurs

c) Time by when DSO expects restoration of its distribution services for MNO.

d) Time when DSO has restored its energy transmission service and starts expecting rapid intervention by MNO.

e) Time duration for which DSO expects to require MNO's rapid intervention for being able to use smart energy services to restore its energy distribution services.

f) Information of locations where for example DSO substations need to restore distribution services on priority.

g) The time at which MNO will actually be able to provide rapid intervention to DSO.

h) The time duration for which MNO will actually be able to provide rapid intervention to DS

i) The information of locations where MNO will actually be able to provide rapid intervention to DSO.

j) The time stamp at which DSO's energy distribution services are finally restored.

k) The information of locations where (e.g. DSO substations) distribution energy service has been finally restored.

NOTE 2: Not all of the above will be configured at the time of IOC creation.

2. MnS producer in MNO creates the MOI that contains these information attribute records for multiple sites.

3. createMOI response is sent by MNO MnS producer to DSO.

4. MNO creates the MOI representing the UPS related information of MNO site. It is name-contained by IOC created in step 1. This is required by DSO from MNO to achieve coordinated intelligent outage planning by DSO during its energy outage recovery. UPS related information of MNO site has to be:

4.1 Information on whether the MNO site has UPS installed/available or not.

4.2 Information on the total UPS backup capacity installed in MNO site (suggested granularity: number of in minutes) i.e. the MNO site UPS backup has installed capacity of how many minutes.

4.3 Information on the status of the remaining UPS backup capacity (suggested granularity: number of minutes) available for MNO site at any given time.

4.4 The identity of DSO energy supply meter present in MNO site.

4.5 The identity of base station present in MNO site.

5. In order to be able to get automatically notified of any changes in the attributes information in the MOI, DSO sends createMOI request for NtfSubscriptionControl IOC to MNO.

NOTE 3: In step 5, if done, a subscription is created such that, subject to parameters in the NtfSubscriptionControl IOC, notifications are sent from the MNO to the DSO. This allows, for example, the MNO to notify the DSO of changes in the UPS backup capacity over time. This step is shown as step 8 below.

6. MNO MnS producer creates the MOI for NtfSubscriptionControl IOC.

7. createMOI response is sent by MNO MnS producer to DSO.

8. If there is a change in the attributes, the MNO sends a notifyMOIAttributeValueChanges notification to inform DSO about the changes.

NOTE 4: In steps 9 and 10 below, there is a change in an attribute of the MOI. This is done by DSO to update MNO on the changes, e.g. information about an expected outage for a specific site.

9. DSO can modify/update any information like outage start time stamp by sending a modifyMOIAttributes request to MNO. DSO can create/read/update/delete (CRUD operations) the information in the MOI by using provisioning MnS (defined in TS 28.532).

10. MNO MnS producer provides the modify response to the DSO.

NOTE 5: In steps 11 and 12 below, the DSO MnS requests and receives respectively the current value of one or more attribute(s).

DSO can also query the UPS related information as and when required by using the getMOIAttributes operation. For example the information could include identity of DSO energy supply meter, MNO base station, remaining UPS backup duration of a particular site, etc.11. DSO requests the required information from the MNO by using getMOIAttributes operation.

12. MNO provides the required information in the response to the DSO.

#### 7.3.2.2 Potential Solution # 2: Energy utility and telecommunication coordinated rapid recovery of energy service

The 3GPP management system and the DSO might inform each other about predicted alarming conditions, including the predicted start and end of the alarming condition. The DSO might inform the 3GPP management system about predicted start time and predicted end time of power outages, such that the MNO is able to plan its energy consumption properly. The 3GPP management system might inform the DSO about predicted start and end time of alarming conditions, such that the DSO is able to prepare corresponding counter measures. By this both DSO as well as MNO know in advance when the mobile network or the power supply will be unavailable and when they are predicted to be available again.

## 7.4 Key Issue #4: Security aspects of exposure of energy service

### 7.4.1 Description

The overall concept of exposing 3GPP management information and services from a 3GPP communications system assumes that the consumer of the information and services is approved to have access by the owner / operator of the communications system.

This includes:

- authentication of the consumer

- authentication of the producer

- authorization of the consumer

- confidentiality of the exposed information and communications

- integrity protection of the expose information and communications

### 7.4.2 Potential solutions

#### 7.4.2.1 Potential solution #1: CAPIF

CAPIF has been defined in 3GPP and provides necessary capabilities to meet these requirements.

#### 7.4.2.2 Potential solution #2: MSAC

SA5 work item Access control for management service (MSAC) has as an objective to extend service based management architecture to support authentication and authorization capabilities.

# 8 Conclusion and recommendation

## 8.1 Key Issue #1: MNO exposes network performance monitoring

The solution in clause 7.1.2.1 provides a mechanism by which the 3GPP management system, according to MNO policy, can expose standardized interfaces to DSO entity that provides the ability to initiate and terminate requests for monitoring and to receive reports containing the required performance data. This corresponds to the key issue objectives listed in clause 7.1.1.

The solution in clause 7.1.2.1 addresses only performance management use case (6.1). The requirements in clause C.5 on alarms are not addressed in this release. The purpose of the table below is to show that key issue 1 is fully addressed by the solution in clause 7.1.2.1.

Table 8.1-1: Key Issue to Solution Mapping

|  |  |  |
| --- | --- | --- |
| Key Issue | Solution | Remarks |
| 7.1.1.a. configuring network monitoring | 7.1.2.1.2, steps 5-7 |  |
| 7.1.1.b. obtain reports | 7.1.2.1.2, steps 8-12 |  |
| 7.1.1.c. does PM contain enough measurements and KPIs to support the requirements? | 7.1.2.1.2, step 5a | It is recommended that the required measurement and KPIs be defined as part of 28.552 [13] and 28.554 [12] respectively. |

The solution in clause 7.1.2.2 provides a mechanism by which the 3GPP management system, according to mobile network operator policy, can expose standardized interfaces to DSO entity that provides the ability to initiate and terminate requests for monitoring and to receive predictive reports containing the required performance data.

The solutions will entail:

1. An update to ThresholdMonitor for an additional location based attributes to be used to scope the objectInstance.

2. New Performance Measurements and KPI related to availability, cell in-service and out-service.

3. The specification of the procedure and explanation of its relevance to and use by energy utilities.

4. Allowing the DSO to make its own predictions of network impairment and also receive the 3GPP management system's predictions of network impairment. The DSO thus has the full complement of data to prepare countermeasures.

The solutions are feasible as they either re-use or build on existing mechanisms and follow the model driven approach. Hence, the recommendation is to normatively define the solutions. It is recommended to proceed solutions #1 and #2 above in normative specifications.

NOTE: The solutions enhance 3GPP management system capabilities so that DSO can use it for MNO's network monitoring purposes. However, the access to these capabilities will be subject to proper authorization and authentication. Further, all use of these mechanisms is subject to operator policy, contractual obligations and regulatory restrictions.

## 8.2 Key Issue #3: Energy utility and telecommunication coordinated recovery of energy service

Solutions #1 and #2. provides a solution to each of the elements in the key issues 7.3.1.2 and 7.3.1.3.

The data model containing all the above elements will be defined in the normative specification phase.

The solutions provide a mechanism for the energy utility (DSO) and telecommunication coordinated recovery of energy service. This involves mutual sharing of information between DSO and site operator, according to MNO policy, through standardized interfaces. The information has to be at least the following information elements:

- the time of the beginning of an energy service outage and the effected sites;

- the UPS capacity corresponding to a specific site, end of an energy service outage and the related sites

- DSO and site operator rapid intervention related information (transmission restore time, required intervention duration, feasible intervention duration).

For the solutions, supported interaction is described between the DSO and the site operator. In some network sharing scenarios, the base station and/or cell site may be operated by this third party. In this case, the specified interaction described is really between the DSO and the site operator would be between the DSO and the site operator of the site essential for telecommunication service, identified by the energy supply ID.

The solutions require the NRM enhancements related to step 1, step 4 in clause 7.3.2.1.2.

NOTE: The solutions enhance 3GPP management system capabilities so that DSO can use it for site operator's network monitoring purpose. However the access to these capabilities, when occurred, will be subject to proper authorization and authentication.

The specification of the procedure and explanation of its relevance to and use by energy utilities will be defined as part of the normative work.

The proposed solutions build on existing mechanisms and follows the model-driven approach. They provide means to satisfy the requirements given in clauses 6.2 and 6.3.

It is recommended to specify a means to support requirements in clauses 6.2 and 6.3 considering clauses 7.3.2.1.2 and 7.3.2.2 in normative specifications.

## 8.3 Key Issue #3: Security aspects of exposure of energy service

Solutions #1 and #2 are feasible. There are many existing CAPIF interfaces that have been exposed by 3GPP standards and these support bidirectional authentication, authorization, confidentiality and integrity protection. MSAC is developed in SA5 and supports access control.

It is recommended to adopt solutions #1 and #2 as a conclusion of the present document.

Annex A:   
Service model for energy utilities and communication service providers

The purpose of this annex is to discuss a model and terminology for IT service processes that will be useful when considering the use cases for this study.

IT processes concern the delivery of IT services within a given organization. The IT processes and operations of a third party are out of scope of 3GPP. The IT processes and operations of a MNO are also out of scope of the standard, and not exposed to a third party except in very specific cases, for specific reasons.

In the present document, the *interaction* between the energy utility and the communication service provider at the IT service level are considered. These interactions are essential to the successful service delivery of energy services. To the extent that these interactions can be standardized, they will become more efficient to operate and require less integration effort for both the energy utility service provider and the MNO.

There are three IT Service processes that will be considered briefly in this clause to provide context for the use cases that follow [5].

Table A.1: ITIL Processes

|  |  |  |
| --- | --- | --- |
| IT Process | ITIL Definition | Relevance to this study |
| Event Management | Process Objective: To make sure CIs and services are constantly monitored, and to filter and categorize Events in order to decide on appropriate actions.  An 'Event' is essentially an alert or alarm created by any IT service, CI or monitoring tool. It is further characterized, often as input to the Problem Management or Incident Management processes described below. | To address the objectives of the present document, alerts or alarms and related information will be considered, as communicated between the energy utility operator and the MNO. These may trigger further action by either the energy utility operator or MNO.  While the specifics of the use of categorization of events and the details of IT Processes is out of scope of this study (and 3GPP), the utility of creating and communicating standardized events to enable such processes is in scope. |
| Problem Management | Process Objective: To manage the lifecycle of all Problems. The primary objectives of Problem Management are to prevent Incidents from happening, and to minimize the impact of incidents that cannot be prevented. Proactive Problem Management analyses Incident Records, and uses data collected by other IT Service Management processes to identify trends or significant Problems. | Many of the use cases in the present document concern different problems. Either the energy utility operator or the MNO ascertains that a problem exists and is able to take further action to address this.  The specifics of the IT processes of the energy utility operator and the MNO are out of scope of the present document. However, there are some 'Problems' that may have relevance to both operators. |
| Incident Management | Process Objective: To manage the lifecycle of all Incidents. The primary objective of Incident Management is to return the IT service to users as quickly as possible. | Some of the use cases in the present document concern Incidents, specifically – communication service outages and energy service outages. Both of these have relevance to both energy utility operators and MNOs. For these specific Incidents some operational requirements may be identified to enable all actors to eliminated the unplanned interruption in service or reduction in quality of service. |

Annex B:   
Network services and operations for energy utilities applicability statement

The present document discusses how NSCE and layered services can complement the functionality in the conclusions of the present document.

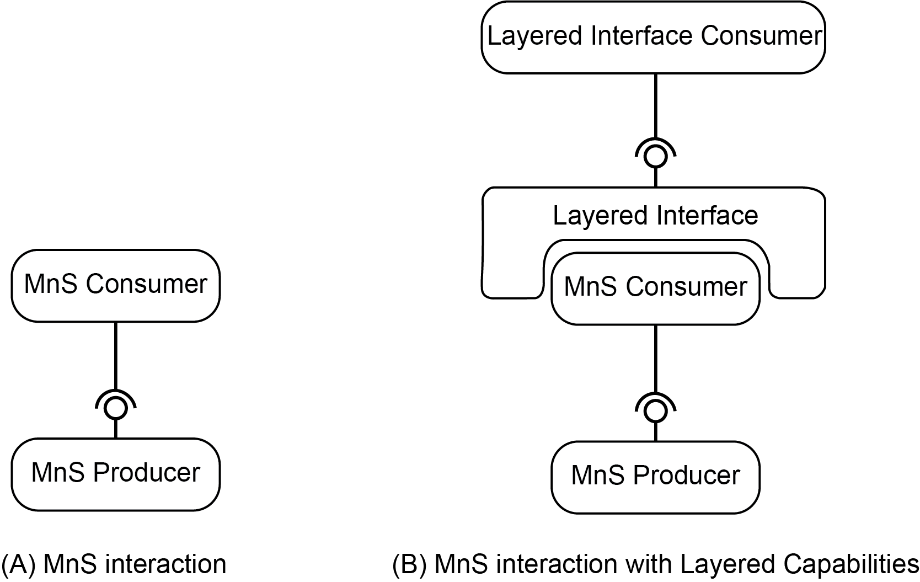


Figure B-1: Consumer Interaction with or without a Layered Interface

In Figure B-1, above, two distinct architectures are shown.

(A) includes a well-defined and understood management system relationship as defined in 3GPP.

NOTE 1: Given only model (A), an implementation and deployment of NSOEU will only be feasible given two assumptions:

- Energy utility backend IT systems from are able to consume as-is SA5 defined MnSs (i.e., they are able to interpret MnS component Type A, B and C,) and thus are able to become MnS consumers.

- As MnS consumers, the energy utility is authorized to gain access to MnS producer capabilities, according to a previous authentication and authorization procedure. Such procedures are not in scope of the present document.

It is noted that there are already systems that are deployed today by which energy utilities exchange information, mostly request and receive information, in a 'custom' (that is to say not a standards specified) manner. Extensive and successful experience in the past with custom exposed information through vendor extensions to RADIUS was the motivation to pursue SEI in 3GPP. This approach has two drawbacks:

- The functionality of the interface needs to be implemented for each energy utility-operator relationship.

- The security and policy governing this interface needs to be implemented for each energy utility-operator relationship.

The present document addresses these shortcomings of a proprietary approach. The conclusions of this study address the first shortcoming but not the second.

To address a policy and security framework for exposure of management services, the mechanisms in the conclusions of the present document can rely upon a layered interface. The layered service can do so in a general way, so that capabilities that are supported for all forms of management services, including those for energy utilities and far beyond.

Additional layered services are possible beyond those for authorization, security and access policy.

For example, the CAMARA initiative of GSMA [17] aims to define, develop, integrate and validate APIs that 3rd parties can invoke. Unlike standard telco-centric APIs (e.g. 3GPP APIs), which are mostly focused on ensuring interoperability within (multi-vendor) and between operators, CAMARA APIs will follow developer-friendly style, with semantics and consumption patterns that are tailored to the business and operational needs of 3rd parties (including especially third parties who are not in the telecommunications industry sector, specifically.) CAMARA can in future focus on defining which information will be exchanged between the MNO and third parties, including energy utilities. As stated in [17], CAMARA offers an " Abstraction from Network APIs to Service APIs is necessary: To hide telco complexity making APIs easy to consume for customers with no telco expertise (user-friendly APIs); To fulfil data privacy and regulatory requirements; To facilitate application to network integration."

In summary, without layered interface support, the solutions concluded in the present document will conform to the model depicted in Figure B-1 (A) above. The solution will require proprietary (closed) solutions to achieve the three objectives (hiding complexity, data privacy and regulatory requirements, application to network integration.) Standards supporting layered interfaces over the solutions defined in the present document, be they NSCE or CAMARA or both, would resolve these shortcomings.

NOTE 2: CAPIF exposure of management services addresses the data privacy objective discussed in the present annex.

Annex C:   
Use cases not pursued

# C.1 General

The use cases and the associated potential requirements in this annex have no associated solutions (clause 7) nor conclusions (clause 8). The potential requirements listed are not to be considered as conclusions of the present document.

# C.2 Business use case: DSO obtains network performance and outage information, current practice

## C.2.1 Description

**Motivation**

When there is an electrical outage, the electrical service operator strives to restore service as quickly as possible. There are several reasons for the need for rapid recovery from an interruption of electrical service:

- In some countries, regulations require rapid recovery and penalize an Energy Utility service provider for any time in which services does not operate. For example, at the least, in many countries customers do not have to pay for electrical service when it is not available.

- Interruptions in electrical service can be expensive, as businesses often require electricity for operations, manufacturing and to properly store valuable products. Thus, electrical outages can translate directly into business losses (of productivity or inventory.)

- Power outages for hospitals and care facilities can result in harm or even death to patients.

NOTE 1: Regulations identify 'critical' electricity customers which are obliged to install and maintain secure sources (e.g. local generators.) Public MNOs in some cases are not covered by these regulations. Further, public MNOs are generally not considered 'critical' electricity customers by regulation, so Energy Utility service providers cannot prioritize service to these customers.

- Electrical service outages affect many customers, so failure of service is not comparable in terms of business consequences to outages of mobile telecommunication service to a single customer.

For this reason, there are regulations that make energy service availability the highest priority. In order to achieve this, Smart Energy services such as protection, SCADA and Distribution Automation are used to monitor and adjust distribution equipment to avoid incidents that would reduce energy service availability.

As a point of comparison, a fibber optic access service is often offered with an availability of at least 99.999 %. Telecommunication systems may not achieve this level of service availability. Since telecommunications offers an *alternative* to fixed fibber optic access, additional means to achieve high degrees of availability are essential to the DSO.

**Background**

To achieve extreme telecommunication service availability, it is currently not feasible to rely on a single telecommunication network. Instead, DSOs networks employ communication access equipment that have multiple USIMs. If one telecommunication service provider is not available, the second can be used. However, this arrangement ('failover') is insufficient, as it requires in practice 2 minutes or more to bring up a secondary USIM and register with a back up network.

NOTE 2: An electrical service operator is a more general term than a DSO. For the purpose for the purpose of the use case, the term DSO is more appropriate, while the more general term is applicable to the motivation above.

To prevent an outage that will last an hour or more, Distribution Automation needs to be used to intervene in the first minutes, ideally in the first seconds, in which an outage occurs. The following examples show two outages and can be considered characteristic of the prospects of resolution in most situations.

In Figure C.2-1, an incident affecting an underground Medium Voltage (MV) line eliminated service to 4223 customers. The existence of DA in secondary substations along the line allowed the fault to be isolated quickly and then resolved. This dramatically reduced the service outage duration for a substantial number of customers. A few customers that were along a line without DA access required local operation that took more than one hour. (The time scale on the X axis is not to scale.)

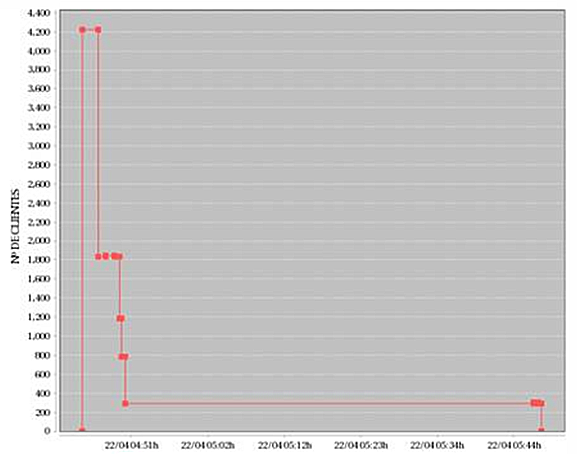


Figure C.2-1: Incident Example

Over 50 % of the customers could have their service restored in 3 minutes. Another 40 % of the customers had their service restored in under 10 minutes. The remaining roughly 10 % of the customers required manual intervention in order to have their service restored. The rapid service restoration saved EUR 1,000s in saved penalties as well as needing only one service truck to roll.

In Figure C.2-2, another example, another MV line was damaged, again showing a complication of a line that did not offer the possibility of DA intervention.

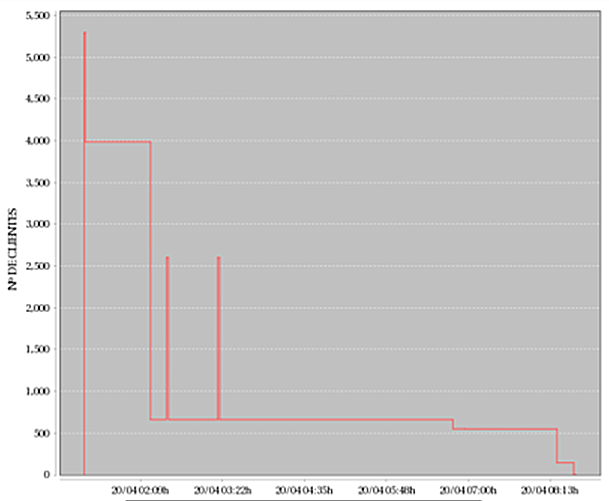


Figure C.2-2: Incident Example featuring a time consuming recovery for a minority of customers

This incident affected 5292 customers. The outage lasted 7 hours but it can be observed that most of the customers could have their service restored within the first minutes due to remote access to primary and secondary substations and intervention using DA. In this incident, EUR 10000s could be saved.

Considering the importance of rapid response during a power outage, it is important that the communication facility is available at the time of an outage. If communication failure only is ascertained during an incident, the outage duration can be extended significantly for most of the affected customers.

In order to improve availability, some DSOs use dual USIM UE deployments. In practice, it takes on the order of 2 minutes to bring up service on an alternate mobile network. These minutes, if they coincide with an outage, are expensive both in terms of penalties and in terms of problems faced by customers during the outage. This also uses up roughly half of the 'downtime budget' of 99.999 % availability (5 minutes per year unscheduled downtime maximum.)

Communication links are tested, e.g. every minute by means of ping messages end to end, to identify availability and latency. The effective availability of 3GPP telecommunications networks observed in practice can be more like 98.5 % (where availability means ability to achieve communication with the expectations of performance according to the service level agreement. While this is far below the levels energy utility operators expect from 5G and that are cited in stage 1 requirements, the fact is that observations of performance of past generations indicate that in order to achieve the target availability, information is needed. Please see TS 22.104 [14], Annex A.4.

NOTE 3: The actual availability of mobile network services is not exposed to energy utility service provider (customers), nor is the cause of the availability limit, e.g. limited capacity, radio quality issues, etc. This makes it difficult for energy utilities to perform risk assessment and network planning for communication services to carry their smart energy services.

Communication performance failure, based on extensive field experience, can be correlated with network performance events. Network performance can be compared to historic information indicating failures. In this case when communication with a 'primary' PLMN shows signs of declining performance, an 'alternate' communication channel can be employed, e.g. registration with another PLMN for a multi-USIM device. This action can be performed proactively, so that in the event that the 'primary' communication session does fail to deliver required performance, recovery can occur quickly (within seconds) to the 'alternative' communication session.

## C.2.2 Details

There is currently no mechanism to convey network or services status from the MNO to the DSO. While the DSO can access real information from their CPEs (radio module or connectivity state), no information comes from the MNO. Thus, in case service failure is happening in an area, the DSO can just infer this situation through a qualified guess.

DSOs have alternative telecommunication connectivity possibilities in any given site. This connectivity can be provided by private networks (different to the MNOs'), or can be provided via alternative MNOs (another CPE in the same site; several SIM cards in the same CPE; etc.). Many of the sites where DSOs need connectivity are mission critical; this means that the service has to be highly available. If the DSO is forced to use a standard MNO service, with no specific availability target, and no mechanism to know that service may be failing in an area, the DSO will not rely in MNO services and will develop alternative telecommunications infrastructure that will eventually make MNOs' services unnecessary.

The MNO has information on the state of its infrastructure. From the Core to the Radio Access Network, and through the different intelligent elements that make the 3GPP standards-based MNO network provide their services, the MNO can tell which network or service parts may be showing a degraded performance or potential unavailability. This information will enhance the MNO service visibility for specific user groups that may benefit from this, while making sure that some of them do not develop alternative solutions they can fully control.

Between the complete lack of information today, and the total control that MNO have of their network infrastructure, and that eventually may reach all the services provided to their customers, there is room to find added value service status information for specific user groups.

**Use case actors**

**DSO network operations centre engineer**: The DSO operations engineer is responsible for deploying monitoring and control mechanisms in the network. The DSO operations centre engineer determines how to control and configure the network for resiliency, e.g. when and how to switch between different accesses to maximize availability.

**DSO electrical system operations centre engineer**: This actor is responsible for maintaining availability, efficiency and safety of the energy system.

**Use case service flow**

0. The energy system is monitored and managed by the electrical system engineer. It relies upon the telecommunications network.

1. The DSO network operations centre engineer deploys monitoring and control mechanisms to determine when a telecommunications network is not available.

2. There is no standard way to obtain network availability or performance information, so the DSO network operations centre engineer has to rely upon 'over the top' monitoring processes. In order to ensure that these monitoring processes do not use a significant amount of the communications capacity, the monitoring relies on periodic probes, e.g. ICMP messages ('pings') every minute. This is a very 'coarse grain' monitoring process, since a failure or performance degradation may take a significant amount of time to detect.

3a. The DSO network operations centre engineer may manually trigger or set up a configuration that will automatically trigger a switch between one telecommunication network to a back-up communication access.

3b. The DSO network operations centre engineer is not successful to initiate and complete a telecommunications network switch because insufficient information was available to the network operations centre to predict the event so the network fails before fail-over can occur, i.e. for more than 2 minutes. This means that the fail-over occurs during a time in which no communication is possible. This results in a network failure visible to the energy system engineer who requires communication for smart energy services. If a fault or protection problem for example occurs in that time the failure can cause damage to the energy system, inefficiencies and even outages. Especially if control is needed (e.g. critical SCADA) during this time frame, a serious energy system outage could occur.

**Service flow result**

Since the information that the DSO network operations centre engineer relies upon is of coarse granularity, there is a high likelihood that performance degradation or failure will be detected after several seconds from the point when they occurred. This extends the period of time in which communication service will be inadequate or unavailable before a secondary communication access can be made available. This reduces the availability of the energy system because, should an energy outage or instability occur during the time in which there is no communication possible, or inadequate performing communicationthis will lead to an energy service outage as described above.

## C.2.3 Potential requirements

There are no potential requirements.

# C.3 Business use case: DSO reporting to MNO to resolve problems and incidents, current practice

## C.3.1 Description

Annex A of the present document describes two processes, Problem Management and Incident Management. In current practice, these processes require interaction between the DSO and MNO, but the interaction is specialized, entirely depending on the processes of each individual MNO.

Problems, generally an observed decline or lack of expected service in certain scenarios over a period of time, need to be addressed or they will likely lead to incidents (where service fails completely or degrades so that service levels do not meet agreed key performance indicator objectives). Problem management allows interaction between a service provider and service customer to address longer term issues - such as capacity planning, disaster recovery or, most relevant, analysis of problems to identify their root cause. If the observed communication problem in the energy utility service provider's network is decisively *not* the MNO's service and network, this will greatly help the energy utility service provider to diagnose and resolve the problem. If, on the other hand, it is the result of the MNO's service and network, this realization can lead to more rapid response.

Incidents, a service failure, are resolved by means of specific procedures defined by service providers. The goal of the customer and service provider is to resolve incidents as quickly as possible.

It is acknowledged that the specifics of the IT processes for Problem Management and Incident Management are out of scope of 3GPP standards. It is however possible that the diversity of interfaces used to report information and the format of those reports can be standardized in 3GPP.

Since an energy utility service provider has to work with many MNOs, especially if the energy utility service provider operates across national borders, the lack of standards in this area for providing information regarding a problem or incident brings complexity and can delay the resolution process.

Energy utilities have vast deployments of communicating devices in hundreds or thousands of static sites. The communication status of each of these devices is constantly monitored, especially their availability, but also latency and other performance metrics. This data, currently collected by energy utility service providers to identify problems and incidents in their own networks, could potentially be very useful to MNOs. This information is currently not shared by energy utilities with MNOs.

NOTE: An energy utility service operator is a more general term than a DSO. For the purpose for the purpose of the use case, the term DSO is more appropriate, as it concerns the operation of energy distribution services, while the more general term is applicable to the motivation above. This use case focusses on energy distribution not generation, transmission or consumption. Though each of these energy system components has relevant aspects for 'smart energy,' this use case focuses on distribution, where communication availability is absolutely critical for stability and recovery of service to customers.

## C.3.2 Details

**Use case I: Energy System Service Provider Network Problem Report**

Problem Management processes, by which the DSO works with the MNO to address such communication issues as observed erratic or declining performance occurs very infrequently today, with resolution and improvements for processes such as capacity planning and adjustments to service level agreements taking months or years. The opportunities to analyse problems that emerge from time to time in energy utility service provider networks essentially have to be analysed by the energy utility service providers independently, without cooperation with the MNOs to ascertain the root cause of failure. This network problem discovery, trend analysis and identification of root causes of problems is very labour intensive for energy utility service providers.

**Use case actors:**

**DSO network operations centre engineer:** The DSO operations centre engineer analyses collected information, creates and operates network monitoring tools including alarms, and seeks to identify areas of potential improvement in service delivery.

**MNO technical service / account manager:** The MNO operations centre service representative responds to queries from the energy utility service provider when needed. Such questions may arise when problems emerge, e.g. as network performance or availability appears to decline in the customer's network.

**Use case service flow:**

1) Using the DSO operational tools, the DSO network operations centre engineer gathers and analyses data, seeking to identify trends that appear threatening to the proper function of the energy utility service provider network.

2) When such trends are identified, the DSO network operations centre engineer uses tools to study the details of the potential problem.

3) The 'root cause' of the problem may need to be investigated before identifying a potential remedy is possible, or determining how high a priority the mitigation has. It is possible at that time that the DSO network operations centre engineer contacts the MNO technical service representative with particular questions. The communication between the two organizations is not based on any standard data model - it requires ad hoc consultation which is labour intensive for both the MNO technical service and DSO operations engineers.

**Service flow result:**

The DSO learns about performance problems in their network. With consultation, it is possible to ascertain whether the issues are also present in the mobile network. This consultation is complicated by the lack of standard ways to exchange management information regarding network problems. The MNO does not benefit from information ascertained by the DSO about network performance issues except through these consultations.

**Use case II: Energy System Service Provider Network Incident Report**

Incident management is triggered when there is a performance incident - either a service is delivered below the service level agreement parameters or there is a service outage. In order to qualify as an 'incident' some parameters may apply (how long it is sustained, how frequently it occurs, etc.) according to the service level agreement, the details of which are out of scope of 3GPP.

When an incident occurs, this triggers processes to end the service performance failure or service outage as quickly as possible. The DSO needs to diagnose the root cause of the incident and take the necessary steps to recover service. To the extent that the service failure is attributed to the mobile network, or the root cause is unknown and could be due to service problems in the mobile network, the DSO works together with the MNO to diagnose the incident and resolve it.

The term 'service desk' represents the service provider contact that is available when incidents occur. The service desk can take many forms and interactions and interfaces are not standardized in current practice.

While resolution is needed on the order of seconds or minutes, communication and collaboration between the DSO and MNO can take much longer, sometimes hours even days. A significant amount of time is needed to describe the incident in terms that enables the MNO to take action. The lack of standards in this area means that the DSO has to identify the reporting formats of each MNO separately, which is labour intensive especially for DSOs that operate across national borders and therefore have large numbers of subscriptions with each operator in each country they operate.

**Use case actors:**

**DSO network operations centre engineer:** The DSO operations centre engineer analyses collected information, creates and operates network monitoring tools including alarms, and seeks to identify areas of potential improvement in service delivery.

**MNO technical service desk engineer:** The MNO is represented by this actor, whose role is to capture the incident information, analyse the MNO's management system to find corresponding relevant information and to work with the customer who reports the incident and MNO operational staff to resolve the incident if it is indeed an issue in the mobile network.

**Use case service flow:**

1) The DSO network operational management system indicates a service outage in the DSO network. The DSO operations centre engineer analyses the alarm.

2) The root cause of the service outage is not clear. The DSO network operations centre engineer initiates a service desk procedure with the MNO providing service for the network that has a service outage.

3) The MNO technical service desk engineer gathers information from the DSO network operations centre engineer, partly through tools provided by the MNO service desk (e.g. web based reporting tools), partly through other forms of communication (phone, messages, etc.)

4) The MNO technical service desk engineer works with the MNO's operational staff and management tools to identify the corresponding network status.

4a) Sure enough, there is a service outage in the mobile network corresponding to the service desk 'ticket' initiated by the DSO.

5a) The MNO technical service desk engineer informs the DSO network operations centre engineer of the incident and the expected time until resolution.

6a) The DSO network operations centre engineer initiates recovery procedures using a back up access system, if possible, or otherwise works to mitigate the impact of the outage.

4b) Alternatively, the MNO network is functioning as expected - there is no service outage in the mobile network corresponding to the service desk 'ticket' initiated by the DSO.

5b) The MNO technical service desk engineer informs the DSO network operations centre engineer that the incident is not related to MNO network performance degradation or service failure.

6b) The DSO network operations engineer continues to work to identify the root cause of the failure, excluding the mobile network as the cause.

7b) Eventually the source of the failure is identified and remedied.

**Service flow result:**

The DSO and MNO work to identify the root cause of the service failure or performance failure incident. If the incident's cause is in the MNO network, MNO operational staff and tools resolve the problem. If the incident's cause is in the DSO network, the DSO's operational staff and tools resolve the problem. Since there is no standard means for communicating the nature of the incident, the 'reporting' process may be complex and varies from operator to operator. This may result in extended resolution times for incidents.

NOTE: The 'standard means for communicating the nature of the incident' from the DSO to the MNO is not part of current practice and is not explained further in this use case. The point of this use case is to identify the absence of any such interface to establish a motivation, or 'gap' that can be pursued in additional use cases in this study.

## C.3.3 Potential requirements

NOTE: Currently, there is no interface between DSO and MNOs. This means that both systems work based on their own premises. Through the use of non-standard, MNO-specific interactions, the DSO can report problems and incidents and work with the MNO to resolve these.

Since the interaction described above uses non-standard means, this clause does not imply any requirement on the 3GPP system.

There are however synergies and potential improvements for building an interface. More investigation and analysis are needed to find appropriate use cases, see TR 22.867 [11] which includes relevant possible requirements to address this.

# C.4 Business use case Energy Outage Coordination current practice

## C.4.1 Description

Energy outage incidents occur as a result of storms, accidents (e.g. a distribution line is broken due to construction work) and other unforeseen factors beyond the control of the energy utility operator. When an energy outage occurs, it will affect a specific region. Service contracts and regulations make a rapid recovery of energy essential.

If the power grid is faulty, then the energy utility operator localizes the fault to solve the problem and perform necessary recovery actions. Some power grid equipment may also require "manual" actions for equipment that are not capable of remote management and automatic recovery. Other equipment can be remotely managed by means of smart energy services that allow recovery operations without requiring manual intervention.

There are several Smart Energy services that can greatly reduce the recovery time: SCADA for remote control and monitoring of distribution systems and Distribution Automation specifically are quite important. Without these services it is generally necessary to send a technician to affected sites. While Smart Energy services cannot entirely eliminate the possibility of manual intervention (e.g. to restore damaged cables, etc.) in many cases, hours of service interruption can be reduced to minutes or even seconds.

Smart Energy services depend on telecommunications, increasingly. If there is an energy outage that affects telecommunications services in the same area where recovery is required, then there is a 'vicious circle': The energy system requires telecommunications to support smart energy services for a rapid recovery. The telecommunication system requires energy services in order to function at all.

This use case considers how this unfortunate system is addressed today.

NOTE: An energy utility operator is a more general term than a DSO. For the purpose of the use case, the term DSO is more appropriate, while the more general term is applicable to the motivation above.

## C.4.2 Details

The ambition of a DSO is to provide an always-on electricity service, with the agreed quality and the costs fixed by Regulators. DSOs understand the criticality of some electricity services they provide (e.g., hospitals), and try to prioritize the availability of these services. This applies not only to business-as-usual situations, but to disaster recovery circumstances. There are plans to provide emergency electricity service through ancillary devices, but also to restore the service in selected areas considering priorities.

MNO services are also considered in these plans. Although in some countries many institutions (blue light services) do not depend on MNO networks for disaster recovery other countries use MNO networks for first responder services, and MNO public service is highly relevant for regular citizens. Thus, energy utility operators find that helping MNOs to recover their normal electricity service is relevant for the society.

A second aspect of the above is to be considered with the MNO service for energy utility operators. DSOs do not rely on MNO service to help recover the grid from a blackout, as they know that there is no certainty that the MNO will work when needed in a blackout.

It is acknowledged that it would be of great value, if upon blackout recovery circumstances, some procedures and supporting management operations existed to allow DSO service recovery through the MNO network. Unfortunately, these procedures and standards specifically to support management operations coordination for recovery from energy outage events between DSO and MNO networks do not exist. See TR 22.867 [11] for more details.

NOTE: It is acknowledged that 3GPP does not specify procedural standards.

Communication between DSOs and MNOs for resolving incidents might be necessary. As there are so many actors (DSOs and MNOs) and each DSO has only information about a limited part in energy sector, resolving the incident could be very complex.

## C.4.3 Use case actors

**DSO response team member**: A representative of the DSO's incident response team who is responsible for communication with service providers, officials and key customers during power cuts.

**MNO service desk team member**: A representative of a MNO's incident response team who can be reached by 'enterprise customers.'

NOTE: In the present document, the role 'MNO' is to be considered as equivalent to 'CSP+NOP' as defined in TS 28.530 clause 4.8.

## C.4.4 Use case service flow

1. An energy system incident occurs in which a power cut results.

2. A DSO response team member may contact a MNO service desk team member. The DSO informs the MNO of the incident and the expected time until its resolution. It is usually not required by regulations and often not required by service contract that the DSO inform the MNO except as they would 'any energy service customer.'

3. The MNO may have the capability to continue to operate their network despite the power cut for a limited time, as they may support an uninterruptable power supply capability in the affected region. The DSO will not know this.

4. The DSO may have the ability to restore energy services rapidly using Smart Energy Services. However, the DSO does not have any means to identify this opportunity nor IT support to coordinate their recovery with the MNO so as to provide communication services for this operation. Without communication service, the DSO cannot use their Smart Energy Services to accelerate recovery and has to send a technician to affect manual operations to restore electrical services.

**Service flow result**

The power cut is resolved manually. Even if there is the possibility to intervene using Smart Energy Services, lack of telecommunications service during the power cut prevents this. There is no standard based coordination of energy system recovery between the MNO and DSO, so only ad hoc communication regarding energy system recovery is possible.

## C.4.5 Potential requirements

There are no potential requirements.

# C.5 Business use case: MNO exposes Network Alarm

## C.5.1 Description

**Motivation**

In clause C.2, it was explained that DSOs require extremely high availability for communication in order to provide distribution automation and SCADA services to prevent energy service outages.

The sooner the DSO obtains information regarding a communication incident the better. (The term 'incident' is used in the sense described in Annex A, a service outage - either where no communication is possible, or the service levels required cannot be maintained.)

As described in clause C.2, a DSO can determine an outage by means of their own infrastructure. The DSO has many routers in their network. These provide networking within substation networks and have wireless access interfaces to connect the substation network over a wide area. These routers perform periodic monitoring operations, e.g. sending ICMP echo (ping) messages to ascertain latency and reachability. If the access fails entirely, it is impossible for the DSO management operations system to collect this monitoring information. The failure is only detected after the periodic monitoring operations fail.

It has to be taken into account that DSO could have tens of thousands of services like these. So, automation has to be used to improve availability.

Despite response time (including the identification of the root cause) for these kind of incidents should be less than two hours, DSO has to dedicate more time (8 hour or more) because there is no information from the MNO and it is supposed that all incidents that are not solved by their own in 8 hour, need to be addressed individually. After these 8 hours, DSO generate incidents automatically with the whole information captured automatically. These incidents are managed manually. There are remote or onsite operation to solve the incidents. If DSO was able to receive information from MNO, this response time could be reduced dramatically to less than 1 hour, an availability of the network could be improved significantly

This use case considers the exposure of alarm messages from the MNO to the DSO to reduce this delay.

**Background**

See use case C.2.

## C.5.2 Details

**Use Case Actors**

**DSO network operations centre engineer**: The DSO network operations engineer is responsible for deploying monitoring and control mechanisms in the network. The DSO network operations centre engineer determines how to control and configure the network for resiliency, e.g. when and how to switch between different accesses to maximize availability.

**DSO electrical system operations centre engineer**: This actor is responsible for maintaining availability, efficiency and safety of the energy system.

**Use case service flow**

1. The energy system is monitored and managed by the DSO electrical system operations centre engineer. It relies upon a functioning network to communicate with electrical utility equipment in substation networks.

2. There are a set of substation networks with routers that include a UE for wide area communications. The DSO network operations centre engineer is responsible for this network. The DSO network operations centre engineer employs monitoring mechanisms to determine when the telecommunications network is not available. These monitoring mechanisms are exposed by the MNO, so that authorized third parties (including the DSO) are able to receive alarm messages.

NOTE 1: It has to be taken into account that the DSO does not need all alarms received in the MNO network. The DSO only needs to receive these alarms which could affect to the availability of their services.

NOTE 2: The alarms are provided at the network level, based on the overall statistical performance of the network. The alarms described here do not correspond to the performance of individual UEs or sessions.

3. The DSO network operations centre engineer, using the exposed monitoring mechanism interface, can request which alarms, under which conditions, will be provided. The interface provides a means by which the alarms can be configured, including thresholds and parameters to report. These alarms can indicate the start and end of incidents.

Table C.5.2-1: Alarm Information

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Configuration | Expected Behavior | Notes |
| latency | location (cell ID), incident threshold for 'start' in msec, incident threshold for 'stop' in msec. | If average latency for service crosses the thresholds, an alarm is sent. The alarm is provided by network exposure from the MNO. | The time of the alarm is crucial, so this information is included in the alarm delivered to the DSO. |
| throughput | location (cell ID), incident threshold for 'start' in Mbps, incident threshold for 'stop' in Mbps. | If average throughput for service crosses the thresholds, an alarm is sent. The alarm is provided by network exposure from the MNO.. | As above. |
| packet loss | location (cell ID), incident threshold for 'start' in packet loss ratio 'loss per million', incident threshold for 'stop' in packet loss ratio 'loss per million'. | If the average packet loss ratio for service crosses the thresholds, an alarm is sent. The alarm is provided by network exposure from the MNO.. | As above. |
| Cell outage | location (cell ID) | If service cannot be provided in a cell (of interest to the 3rd party) from the MNO. | As above |

4. An alarm is triggered because either

- The 3GPP management system determines that service has degraded with some KPIs (e.g. throughput, latency, etc.) above the threshold, or recovered so that they are below a threshold.

- The 3GPP management system determines that service is no longer available or has become available after having not been available.

**Service flow result**

When an incident occurs, an alarm is sent. Once the alarm is received, the DSO network operations centre engineer (or an automated management function) may trigger a fail-over to a backup network communications facility. This immediate alarm from the network facilitates a rapid response by the DSO, reducing or even eliminating the interval in which the DSO substation network components are unreachable or only reachable with inadequate quality of service.

## C.5.3 Potential Requirements

PR C.5.3-1. The 3GPP management system shall according to mobile network operator policy expose interfaces to third parties that provide the ability to:

a) enumerate alarms;

b) create alarms;

c) remove alarms;

d) configure alarms.

NOTE: The intention of this requirement is to enable DSOs to manage the set of alarms that the MNO will expose. That is, the DSO can create, configure, remove and enumerate the alarms that they request that the MNO expose to the DSO.

PR C.5.3-2. The 3GPP management system shall according to mobile network operator policy expose interfaces to third parties that provide a mechanism for the mobile network operator to send alarms to the third party.

PR C.5.3-3. The 3GPP management system shall support the following alarms and associated configuration:

a) Maximum throughput threshold crossed (where the trigger characteristic corresponds to measurement of [an average for the third party's network traffic]);

b) Maximum packet loss threshold crossed (where the trigger characteristic corresponds to measurement of [an average for the third party's network traffic]);

c) Cell outage (where the trigger characteristic corresponds to measurement of [where communication service is not possible at all on the third party]).

PR C.5.3-4. Authentication of the consumer (3rd party) by the producer (3GPP management system) shall be possible,

PR C.5.3-5. Authentication of the producer (3GPP management system) by the consumer (3rd party) shall be possible.

PR C.5.3-6. Authorization of the consumer (3rd party) by the producer (3GPP management system) shall be possible,

PR C.5.3-7. Communication between the consumer (3rd party) and the producer (3GPP management system) shall be confidentially protected.

PR C.5.3-8. Communication between the consumer (3rd party) and the producer (3GPP management system) shall be integrity protected.

# C.6 Business use case: DSO Provides Performance Information indicating Relevant Changes to its Network

## C.6.1 Description

**Motivation**

As described in clause C.3, DSO reporting to MNO to resolve problems and incidents, current practice, and Annex A, incident reporting is a vital component of service management. The reporting of such problems today occurs very infrequently, e.g. when service agreements are created or renewed. This exchange of information could be very beneficial to an MNO and lead to considerations such as adjustment of coverage (e.g. for optimization), capacity planning (e.g. to react to growth in utilization in some part of the network), disaster recovery planning, and more.

Providing information from the DSO to the MNO serves a broader set of motivations as well. As the DSO's organization and use of their own network changes, their measured performance will change. This information may be important in distinguishing whether differences in network usage arise from performance problems or instead whether the changes are intentional on the part of the DSO.

The DSO is in a unique position to provide information to an MNO regarding their service. The DSO not only has many deployed stationary UEs, but performs significant performance management for these and requires extremely high availability. The DSO therefore has a very detailed set of information gathered over time, across the MNO's network. Specifically, the DSO identifies where there are problems for their own purposes, for the purposes of proactive response to increase availability. (See clause C.3)

This 'problem' or 'utilization' information is in the interest of the DSO to share, as it could lead the MNO to consider service improvements or to identify issues that they may not have otherwise detected. Providing problem analysis information is an example of mutual advantage for both the customer and the service provider. In any case, if such information is needed by both sides, a standard interface for providing it will reduce the informal communication needed by both parties.

**Background**

See clause C.3.

## C.6.2 Details

Problem Management processes, by which the DSO works with the MNO to address such issues as observed erratic or declining performance, occur very infrequently today. Problem Management results in concrete proposals for improvements, essentially as input for processes such as capacity planning and adjustments to service level agreements. Problem management therefore results in changes that need to be considered over time, decisions that take months or years to conclude.

The opportunities to analyse problems that emerge from time to time in energy utility service provider communication networks can be analysed by the energy utility service providers in cooperation with the MNOs to ascertain the root cause of unexpectedly low or declining performance levels. This network problem discovery, trend analysis and identification of root causes of problems is, as a result of sharing information and conferring with MNOs, made easier for energy utility service providers.

**Use case actors:**

**DSO network operations centre engineer:** The DSO networkoperations centre engineer analyses collected information, creates and operates network monitoring tools including alarms, and seeks to identify areas of potential improvement in service delivery.

**MNO technical service / account manager:** The MNO technical service / account manager responds to queries from the energy utility service provider when needed. Such questions may arise when problems emerge, e.g. as network performance or availability appears to decline in the DSO's network.

**Use case service flow:**

1) Using the DSO operational tools, the DSO network operations centre engineer gathers and analyses data, seeking to identify trends that appear threatening to the proper function of the energy utility service provider network. An example of such a trend would be a gradual decline in performance parameters including observed increasing latency or jitter, or gradual decline in availability. Note that these parameters' decline even while remaining within the expectations of the service level agreement may merit investigation if the decline is prolonged and pronounced.

2a) When such trends are identified, the DSO network operations centre engineer uses tools to study the details of the potential problem.

2b) Another goal is to identify where there are not problems, despite data that appears to indicate problems. In some cases, when less or no traffic is sent or received over the mobile telecommunications network this may be a decision of the customer.

3) The DSO network operations centre engineer shares this information with the MNO by means of a standard interface, including the measured performance, physical location, Cell ID and other information.

NOTE: The physical location, Cell ID and other information is available to the MNO. It is given by the DSO in order to provide sufficient information that the observed performance information provided by the DSO can effectively be correlated and compared to management information collected by the MNO.

4a) The 'root cause' of the problem may need to be investigated by the DSO before identifying a potential remedy is possible, or determining how high a priority the mitigation has. This process can be accelerated and eased by collaboration and interaction between the DSO network operations centre engineer and the MNO technical service representative. The communication between the two organizations is based on any standard data model which eases communication and determining answers to essential questions for both the MNO technical service and DSO operations engineers.

4b) The apparent problem (reduced or zero network utilization) can be flagged to the MNO as 'intended'.

**Service flow result:**

The DSO learns about performance problems in their network. By sharing these problems in a standardized manner with the MNO, it is possible to more straightforwardly ascertain whether the issues are also present in the mobile network. The MNO benefits from information ascertained by the DSO about network performance issues.

The DSO is able to differentiate in the information it provides to the MNO between reduced performance in the network and intentional reduced utilization of the network. This will ease interpretation of the data by the MNO.

## C.6.3 Potential Requirements

PR C.6.3-1. Subject to operator policies, regulatory requirements and contractual obligations, the 3GPP management system may support a means for authorized third parties to provide network performance information to an MNO. The data model of the performance information provided by the DSO to the MNO has to include at least the following elements: {measurement granularity, location of measurement, latency, packet loss, throughput.}

a) Latency between the DSO's device and the DSO's server the device is communicating with [an average for the DSO's network traffic];

NOTE 1: Latency measurement end to end will include delay arising from a network outside the mobile telecommunication system.

b) Throughput [an average for the DSO's network traffic];

c) Packet loss [an average for the DSO's network traffic];

NOTE 2: Packet loss can be determined by means of observation of ICMP and TCP control information for traffic, sending probes, etc. This methodology is out of scope of 3GPP.

NOTE 3: The information elements to include in the incident report will be further clarified during the 'solution definition' stage of this study.

NOTE 4: The measurements provided by the DSO can be acquired by means that are outside the scope of 3GPP. Measurements may be acquired from management MIBs of routers that are operated by the DSO.

PR C.6.3-2. Authentication of the consumer (3rd party) by the producer (3GPP management system) shall be possible,

PR C.6.3-3. Authentication of the producer (3GPP management system) by the consumer (3rd party) shall be possible.

PR C.6.3-4. Authorization of the consumer (3rd party) by the producer (3GPP management system) shall be possible,

PR C.6.3-5. Communication between the consumer (3rd party) and the producer (3GPP management system) shall be confidentially protected.

PR C.6.3-6. Communication between the consumer (3rd party) and the producer (3GPP management system) shall be integrity protected.

# C.7 Business use case: DSO reports an incident to MNO

## C.7.1 Description

**Motivation**

As described in clause C.3, DSO reporting to MNO to resolve problems and incidents, current practice, and Annex A, incident reporting is a vital component of service management. Currently incident reporting is done through diverse mechanisms specific to each MNO, such as a voice call to a service desk or a web-based form. While such processes are out of scope of 3GPP and are vital to support of mobile subscribers in general, they are not well suited to a DSO. The DSO operates 100s of 1000s of UEs often with dual SIM configurations, in some cases in multiple countries. This results in a high degree of complexity for the DSO in terms of divergent procedures and manual effort required. A specific aspect of this challenge for DSOs is that the terminology, units and other aspects of incident reports differ between operators. Reporting incidents using 'business to consumer' oriented interfaces is not only cumbersome; it does not scale up to the number of concurrent incidents that can arise for a DSO.

Furthermore, the availability requirements of a mobile consumer are different from that of an energy utility service provider. It is essential that the DSO network operations network operations staff be able to ascertain the root cause of an incident as quickly as possible. If the root cause is an incident in the mobile telecommunications network, and this information is readily available, this will help to focus the recovery efforts on the DSO. If on the other hand, there is no known mobile telecommunications network failure, the DSO can focus their recovery efforts on their own network.

The intention of this use case is to identify how standardized interfaces can facilitate large scale, rapid and uniform incident reports from a DSO to an MNO. This use case does not consider how to automate or standardize the incident reporting *process* since process standardization is out of scope of 3GPP and it is recognized that different operators have unique and specific business processes. As incident reporting mechanisms will vary between operators, only a 'least common subset' of reporting information is identified in the requirement, and a 'least common subset' of responses to these reports.

**Background**

See clause C.3.

## C.7.2 Details

Incident management is triggered when there is a performance incident - either a service is delivered below the service level agreement parameters or there is a service outage. In order to qualify as an 'incident' some parameters may apply (how long it is sustained, how frequently it occurs, etc.) according to the service level agreement, the details of which are out of scope of 3GPP.

When an incident occurs, this triggers processes to end the service performance failure or service outage as quickly as possible. The DSO needs to diagnose the root cause of the incident and take the necessary steps to recover service. To the extent that the service failure is attributed to the mobile network, or the root cause is unknown and could be due to service problems in the mobile network, the DSO works together with the MNO to diagnose the incident and resolve it.

The term 'service desk' represents the service provider contact that is available when incidents occur. The service desk can take many forms and interactions and interfaces are not standardized in current practice.

While resolution is needed on the order of seconds or minutes, communication and collaboration between the DSO and MNO can take much longer, sometimes hours even days. A significant amount of time is needed to describe the incident in terms that enables the MNO to take action. The lack of standards in this area means that the DSO has to identify the reporting formats of each MNO separately, which is labour intensive especially for DSOs that operate across national borders and therefore have large numbers of subscriptions with each operator in each country they operate.

**Use case actors:**

**DSO network operations centre engineer:** The DSO network operations centre engineer analyses collected information, creates and operates network monitoring tools including alarms, and seeks to identify areas of potential improvement in service delivery.

**MNO technical service desk engineer:** The MNO is represented by this actor, whose role is to capture the incident information, analyse the MNO's management system to find corresponding relevant information and to work with the customer who reports the incident and MNO operational staff to resolve the incident if it is indeed an issue in the mobile network.

**Use case service flow:**

1) The DSO operational management system indicates a service outage in the DSO network. The DSO network operations centre engineer analyses the alarm.

2) The root cause of the service outage is not clear. The DSO operations centre engineer initiates a service desk procedure with the MNO providing service for the network that has a service outage. This service desk procedure includes submission of a **standard form for incident reporting** that can be provided by the DSO by means of an interface exposed by the MNO.

3) The MNO technical service desk engineer obtains information from the DSO network operations centre engineer, principally by means of the exposed interface. If needed, other means of communication are also provided by the MNO service desk (e.g. web based reporting tools), partly through other forms of communication (phone, messages, etc.)

4) The MNO technical service desk engineer works with the MNO's operational staff and management tools to identify the corresponding network status.

a) Sure enough, there is a service outage in the mobile network corresponding to the service desk 'ticket' initiated by the DSO.

a.1) The MNO technical service desk engineer informs the DSO network operations centre engineer of the incident and the expected time until resolution, by means of the **standard form for** **incident response**.

a.2) The DSO network operations centre engineer takes the appropriate action, e.g. initiates recovery procedures using a back up access system, if possible, or otherwise works to mitigate the impact of the outage.

b) Alternatively, the MNO network is functioning as expected - there is no service outage in the mobile network

b.1) The MNO technical service desk engineer informs the DSO network operations centre engineer by means of the **standard form for incident response** that the incident is not related to MNO network performance degradation or service failure.

b.2) The DSO network operations engineer continues to work to identify the root cause of the failure, excluding the mobile network as the cause.

b.3) Eventually the source of the failure is identified and remedied.

NOTE: A quick and standard exchange of information can provide valuable data to both sides minimising the request for further information during the troubleshooting of the incident.

## C.7.3 Potential Requirements

PR C.7.3-1. Subject to operator policies, regulatory requirements and contractual obligations, the 3GPP management system shall support a means to expose a standard interface for incident reporting by authorized consumer. The process of incident reporting itself is out of scope of this requirement as this is a business process. The information that this incident report contains is intended to be a 'common subset' supported by incident reporting procedures and tools today.

NOTE 1: An example of such information elements includes: {UE Identifier e.g. IMSI, performance characteristics that constitute a service level failure, time of start of incident, location of UE, cell ID serving the UE, ... }

NOTE 2: More than one incident report may be submitted, e.g. as more information is learned by the customer.

NOTE 3: The information elements to include in the incident report will be defined and evaluated during the 'solution description' phase. These information elements are expected to include {UE Identifier e.g. IMSI, performance characteristics that constitute a service level failure, time of start of incident, location of UE, cell ID serving the UE, . . . }

NOTE 4: This requirement does not imply that the incident reporting interface required will replace existing tools or processes. The 'common subset' of information defined for the incident reporting interface does not limit incident reporting by the customer to the operator to this subset - additional information will be collected by tools and/or interfaces as well.

PR C.7.3-2. Subject to operator policies, regulatory requirements and contractual obligations, the 3GPP management system shall support a means to expose a standard interface for incident response to authorized DSOs. The process of responding to incident reports itself is out of scope of this requirement as this is a business process. The information that this response contains is intended to be a 'common subset' supported by incident responses procedures and tools today.

NOTE 5: An example of such information elements includes: {incident does or does not correspond to known fault or performance degradation in the mobile network, expected time of restoration of service, . . .}

NOTE 6: More than one incident reporting response may be sent to the customer, e.g. as more information is learned by the MNO.

NOTE 7: The information elements to include in the incident report will be defined and evaluated during the 'solution description' phase. These information elements are expected to include {incident does or does not correspond to known fault or performance degradation in the mobile network, expected time of restoration of service, . . .}

NOTE 8: This requirement does not imply that the incident response interface required will replace existing tools or processes. The 'common subset' of information defined for the incident response interface does not limit incident response by the operator to the customer to this subset - additional information will be provided by tools and/or interfaces as well.

NOTE 9: All requirements above concerning the MNO apply to the site operator. In some network sharing scenarios the site operator could be an entity other than an MNO. In active network sharing scenarios the DSO can communicate with an MNO that operates the site, but can be distinct from the serving MNO.

PR C.7.3-3. Authentication of the consumer (3rd party) by the producer (3GPP management system) shall be possible,

PR C.7.3-4. Authentication of the producer (3GPP management system) by the consumer (3rd party) shall be possible.

PR C.7.3-5. Authorization of the consumer (3rd party) by the producer (3GPP management system) shall be possible,

PR C.7.3-6. Communication between the consumer (3rd party) and the producer (3GPP management system) shall be confidentially protected.

PR C.7.3-7. Communication between the consumer (3rd party) and the producer (3GPP management system) shall be integrity protected.

Annex D:   
Key issues not pursued

# D.1 Key Issue # 2: DSO reports an incident to the MNO

## D.1.1 Description

In response to the use case C.7 and the potential requirements identified in C.7.3, new and existing solutions for incident reporting will be considered.

## D.1.2 Potential Solutions

### D.1.2.1 Potential Solution # 1: TMF API 621 (Trouble Ticket)

#### D.1.2.1.1 Introduction

It was suggested to investigate whether and how a DSO could create a Trouble Ticket to report an incident to satisfy the requirements in clause C.7. This solution will not be further developed in this version of the present document.

### D.1.2.2 Potential Solution # 2: MnS-based standardized interface

#### D.2.2.2.1 Introduction

It was suggested to investigate the feasibility of a MnS-based standardized interface to satisfy the requirements in clause C.7. This solution will not be pursued in this version of the present document.

Annex E:   
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Change history | | | | | | | |
| Date | Meeting | TDoc | CR | Rev | Cat | Subject/Comment | New version |
| 04-2022 | SA5#142e | S5-222671 S5-222672  S5-222019  S5-222020 S5-222016 |  |  |  | Update to implement the agreed pCRs in SA5#142e:  1. S5-222671\_Rel-18 TR 28.829-Cover-Sheet  2. S5-222672\_TR 28.829-Structure  3. S5-222019 Rel-18 pCR TR 28.829-Scope-02  4. S5-222020 Rel-18 pCR TR 28.829-Overview-05  5. S5-222016 Rel-18 pCR TR 28.829-Annex-B-IT Services Model-03 | 0.1.0 |
| 05-2022 | SA5#143e | S5-223611  S5-223612  S5-223613 |  |  |  | Update to implement the agreed pCRs in SA5#143e:  1. S5-223611 pCR TR 28.829 Business use case - MNO provides performance info  2. S5-223612 pCR TR 28.829 Business use case - Utility provides performance and failure info  3. S5-223613 pCR TR 28.829 Business use case - Energy outage coordination | 0.2.0 |
| 07-2022 | SA5#144e | S5-223613  S5-224434  S5-224434 |  |  |  | Update 0.2.0 version to properly implement S5-223613 from SA5#143e: a change missed in (definitions were added but not implemented), style corrected in 6.1.1, 6.3.1 and 6.3.2. Reference corrected in 6.2.3.  Update to implement the agreed pCRs in SA5#144e  1. S5-224434  2. S5-224435 | 0.3.0 |
| 08-2022 | SA5#145e | S5-225865  S5-225866  S5-225867  S5-225868 |  |  |  | Rel-18 pCR 28.829 KI and solution for MNO exposes Network Performance  pCR TR 28.829 Business use case - DSO Provides Performance Reporting indicating Problems  pCR TR 28.829 Business use case - DSO Provides an Incident Report  pCR TR 28.829 Clean up | 0.4.0 |
| 11-2022 | SA5#146 | S5-226808  S5-226809 |  |  |  | Rel-18 pCR 28.829 Corrections  Rel-18 pCR 28.829 Use case on Energy System Recovery | 0.5.0 |
| 2023-03 | SA5#147 | S5-232850  S5-232851  S5-232852  S5-232657  S5-232854  S5-232856  S5-232857  S5-232671  S5-232858  S5-232673  S5-232859  S5-232675  S5-232855  S5-232678  S5-232896  S5-232898  S5-232894  S5-232895  S5-233065 |  |  |  | Rel-18 pCR 28.829 Completion of 7.1.2.1  Rel-18 pCR 28.829 Clean Up 6.1, 6.3  Rel-18 pCR 28.829 Update 6.4, 6.5, 6.6  Rel-18 pCR 28.829 Discontinuing work on objective #2  Rel-18 pCR 28.829 – Update 6.7  Rel-18 pCR 28.829 – Update 6.8  Rel-18 pCR 28.829 – Update 6.1  Rel-18 pCR 28.829 – Update 6.2  Rel-18 pCR 28.829 – Update 6.3  Rel-18 pCR 28.829 – Update 6.4  Rel-18 pCR 28.829 – Update 6.5  Rel-18 pCR 28.829 – Update 6.6  Rel-18 pCR 28.829 – Update 6.8  Rel-18 pCR 28.829 – Update 7  Rel-18 pCR 28.829 – Key Issue for Energy utility and telecommunication coordinated rapid recovery of energy service  Rel-18 pCR 28.829 – New use case for Rapid Intervention for Outages without Redundant Topology  Rel-18 pCR 28.829 – Conclusion and Recommendation for Key Issue 1 - MNO exposes Network Performance Monitoring to DSO  Rel-18 pCR 28.829 – Conclusion and Recommendation for Key Issue i (energy utility and telecommunication coordinated recovery of energy service)  28829 pCR Annex on NSOEU Applicability | 0.6.0 |
| 2023-03 | SA#99 | SP-230191 |  |  |  | Presented for information | 1.0.0 |
| 2023-04 | SA5#148e | S5-233621  S5-233622  S5-233623  S5-233367  S5-233368  S5-233369  S5-233370  S5-233371  S5-233372  S5-233373  S5-233374 |  |  |  | Rel-18 pCR 28.829 – Potential Solution for Energy utility and telecommunication coordinated rapid recovery of energy service  pCR TR 28.829 v1.0.0 cl 7.X key issue  Rel-18 pCR 28.829 – Potential Solution for Energy utility and telecommunication coordinated rapid recovery of energy service  pCR TR 28.829 v1.0.0 cl 6.8 description & details  pCR TR 28.829 v1.0.0 cl 6.9 description & details  pCR TR 28.829 v1.0.0 cl 6.4 requirements  pCR TR 28.829 v1.0.0 cl 6.5 requirements  pCR TR 28.829 v1.0.0 cl 6.6 requirements  pCR TR 28.829 v1.0.0 cl 6.7 requirements  pCR TR 28.829 v1.0.0 cl 6.8 requirements  pCR TR 28.829 v1.0.0 cl 6.9 requirements | 1.1.0 |
| 2023-05 | SA5#149 | S5-234538  S5-234539  S5-234540  S5-234541  S5-234542 |  |  |  | Rel-18 pCR 28.829 7.1.2.1 Solution #1 correction  Rel-18 pCR 28.829 6.3.3 Requirements clarification  pCR TR 28.829 v1.1.0 potential solutions  Rel-18 pCR 28.829 – Corrections  Rel-18 pCR 28.829 – Clean up |  |
| 2023-06 | SA#100 | SP-230644 |  |  |  | Presented for approval | 2.0.0 |
| 2023-06 | SA#100 |  |  |  |  | Upgraded to change control version | 18.0.0 |
| 2023-06 | SA#100 |  |  |  |  | EditHelp review | 18.0.1 |