International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series L

Supplement 25

(04/2016)

SERIES L: ENVIRONMENT AND ICTS, CLIMATE CHANGE, E-WASTE, ENERGY EFFICIENCY; CONSTRUCTION, INSTALLATION AND PROTECTION OF CABLES AND OTHER ELEMENTS OF OUTSIDE PLANT

ITU-T L.1502 – Best practices for infrastructure adaptation to climate change

ITU-T L-series Recommendations – Supplement 25

ITU-T L-SERIES RECOMMENDATIONS

ENVIRONMENT AND ICTS, CLIMATE CHANGE, E-WASTE, ENERGY EFFICIENCY; CONSTRUCTION, INSTALLATION AND PROTECTION OF CABLES AND OTHER ELEMENTS OF OUTSIDE PLANT

OPTICAL FIBRE CABLES	
Cable structure and characteristics	L.100–L.124
Cable evaluation	L.125–L.149
Guidance and installation technique	L.150–L.199
OPTICAL INFRASTRUCTURES	
Infrastructure including node element (except cables)	L.200–L.249
General aspects and network design	L.250–L.299
MAINTENANCE AND OPERATION	
Optical fibre cable maintenance	L.300–L.329
Infrastructure maintenance	L.330–L.349
Operation support and infrastructure management	L.350–L.379
Disaster management	L.380–L.399
PASSIVE OPTICAL DEVICES	L.400–L.429
MARINIZED TERRESTRIAL CABLES	L.430–L.449

For further details, please refer to the list of ITU-T Recommendations.

Supplement 25 to ITU-T L-series Recommendations

ITU-T L.1502 – Best practices for infrastructure adaptation to climate change

Summary

Supplement 25 to the ITU-T L-series of Recommendation provides general principles and illustrates best practices on how information and communication technology (ICT) infrastructure can be adapted to cope with the effects of climate change.

Examples cited provide countermeasures to climate vulnerabilities identified in the Checklist in Recommendation ITU-T L.1502. These are: temperature rise, humidity, wind loading, sea level rise, rainfall, floods, landslides, snow and ice fall, lightning strikes and species damage.

Continuity of electric power supply is an important consideration in the event of electric grid failure, or failure of any other primary source of power. Functions that before were all in the same local system will have some of their functions possibly located hundreds of kilometres away, in a data centre. Such data centres may belong to services other than telecommunications. This will pose new challenges to primary service availability and continuity in case of occurrence of extreme events such as loss of power.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T L Suppl. 25	2016-04-27	5	11.1002/1000/12893

Keywords

Climate change adaptation, infrastructure, protection systems, resilience, telecommunications network.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 25 to ITU-T L-series Recommendations

ITU-T L.1502 – Best practices for infrastructure adaptation to climate change

1 Scope

This Supplement provides general principles and examples of best practices which demonstrate information and communication technologies (ICTs) which can enable telecommunications infrastructure to adapt to the effects of climate change.

Examples cited provide countermeasures to climate vulnerabilities identified in the ITU-T L.1502 Checklist. These are: temperature rise, humidity, wind loading, sea level rise, rainfall, floods, landslides, snow and ice fall, lightning strikes and species damage.

Examples of resilient networks are included in this Supplement.

Continuity of electric power supply is an important consideration in the event of electric grid failure or failure of any other primary source of power.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T L.1502] Recommendation ITU-T L.1502 (2015), *Adapting information and communication technology infrastructure to the effects of climate change*.

3 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

FG-DR&NRR	Focus Group on Disaster Relief Systems, Network Resilience and Recovery
G	Generation (of mobile network type, e.g., third generation, 3G)
ING	Intelligent Network Gateway
IP	Internet Protocol
IUG	Intelligent User Gateway
NFV	Network Function Virtualization
PSTN	Public Switched Telephone Network
QoE	Quality of Experience
QoS	Quality of Service
SDH	Synchronous Digital Hierarchy
SDN	Software Defined Network
SLA	Service Level AgreementTV Synchronous Digital Hierarchy
UPS	Uninterruptible Power Supply
USAID	United States Agency for International Development

4 Resilience in telecommunications networks

Although not targeted at any specific climate-change vulnerability, networks can be made more resilient by providing duplication of paths to access telecommunications services. Such networks can withstand at least one failure before access to essential services is cut off. Resilience is commonly provided by network operators where the traffic of more than 100 users is aggregated onto a common path.

The ITU-T Focus Group on Disaster Relief Systems, Network Resilience and Recovery (FG-DR&NRR) was established by ITU-T Telecommunication Standardization Advisory Group (TSAG) in Geneva, 10-13 January 2012 and concluded with a number or technical reports in June 2014 [b-ITU-T FG]. An overview of resilience in telecommunications networks can be found in [b-Overview] and several other technical reports also discuss resilience in the context of disaster relief systems. The gap analysis [b-ITU-T FG-Gap] includes a review of ITU-T Recommendations on lightning strikes, protection switching, natural disasters, electricity provision and backup, as well as systems for disaster relief.

5 Examples of resilience in fixed and mobile telecommunications infrastructure

An example of resilient network design which represents best practices for both fixed telecommunications and cellular network types is shown in Figure 1.

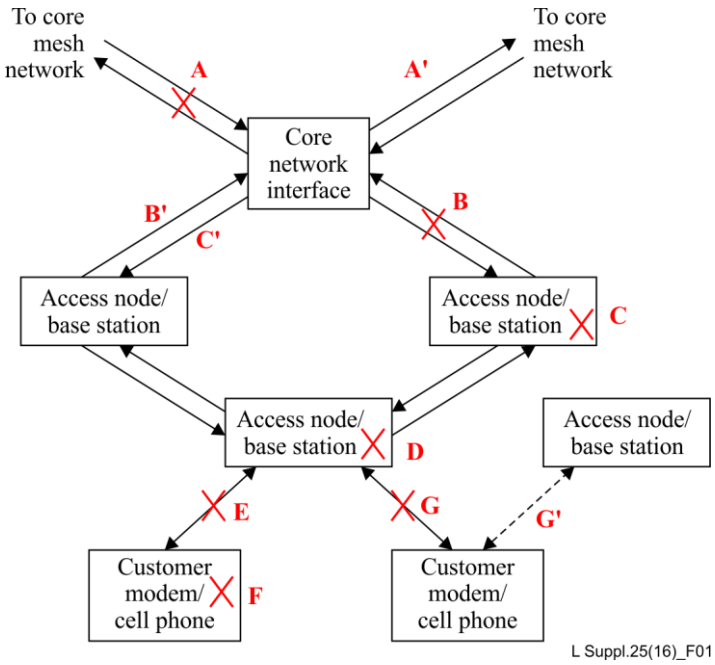

Figure 1 – Resilient network design

The core network is shown at the top of the figure and is connected to a fully meshed set of core network switches which include international gateways. The meshed core network is inherently resilient against single and some multiple failures. Examples of customer nodes are shown at the bottom of the figure. The access and backhaul network is at the centre. This forms a bi-directional ring which may be looped back at any node in the event of a path or node failure. Once looped-back, it becomes a single "folded ring". A number of failure/resilience modes are shown with the letters A-F.

- In case A, the network is protected against a single point of failure by path A'. When path A fails, path A' takes over the traffic.

- In case of a break at B, loop back is applied to the remaining three links so that traffic is routed via B'.
- In case of a failure at node C (e.g., power), loop back is applied to the remaining two links so that traffic is routed via C'.
- Cases D, E and F represent a single point of failure so no protection is available from the service provider at that level.
- In case G the customer has an alternative access network which allows continuity of service via another access node, such as a cellular base station or a satellite terminal via link G'.

As shown, the network has a number of features which mean that the network has some resilience to extreme climate events, disasters or technology failures. Nevertheless, due to cost, the level of redundancy is highest in data centres, core networks, and in the most important telecommunications centres. Resilience gradually decreases where density of equipment and users lessen. Generally, the highest redundancy is found in cities and main national trunk networks, while it is lowest where the level of aggregated traffic is low, such as in the access networks and in remote and less populated areas.

Figure 1 shows a typical provision for resilience in the core and backhaul networks, but none in the access network. Resilience in the fixed access network is possible if, for example, two optical fibres follow different paths into a building. The long-reach of fibre access networks allows them to be hosted on different central offices. Examples may be found in [b-ITU-T G.984.1].

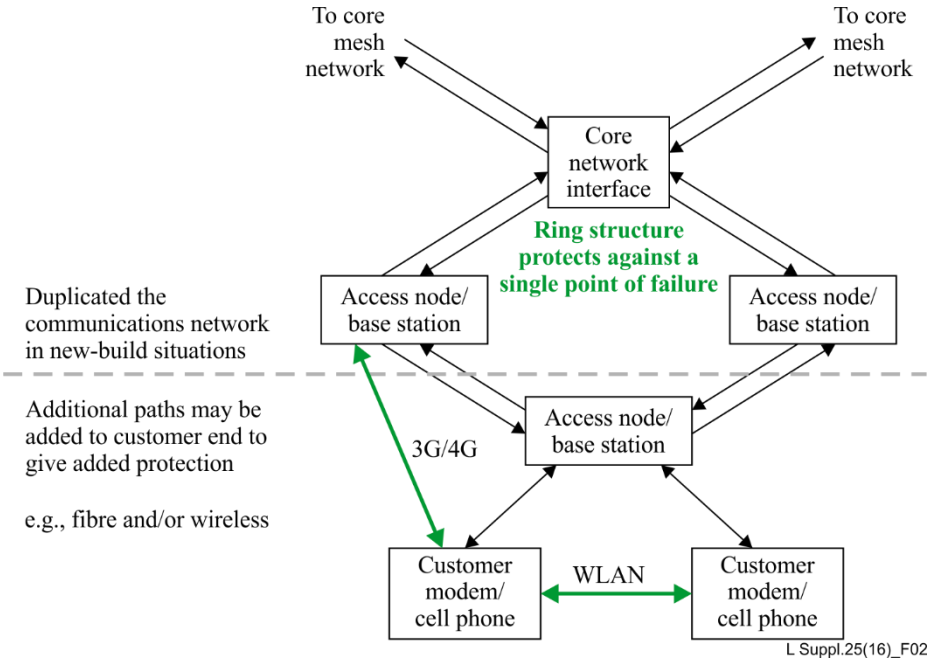

Figure 2 – Ensuring telecommunications service continuity (source [b-ITU-T G.984.1])

Figure 2 is an example of resilient access using both wired and wireless (cellular) services to maintain services in all buildings. Additionally, alternatively fixed network operators may facilitate access to their networks using the wireless LAN installation of another customer. An example is described in [b-BT Wi-Fi].

Broadband access via satellite also offers a means of providing dual access paths for resilience. Users in remote sites may have satellite as their only broadband access option. However, systems are being considered whereby an asymmetric digital subscriber line (ADSL) or a third generation/fourth

generation (3G/4G) wireless network may additionally be connected via satellite. This allows, for example, fast download of large files via satellite when the fixed access network is congested or unavailable because of a fault. An example is given in Appendix I.

Other resilience features include backup power via batteries and/or a generator at the access node or cellular base station. It is generally left to the customer to provide backup power for cell phones and computer equipment at the customer's premises. Legacy fixed line telephony, the public switched telephone network (PSTN), is powered by battery in the central office and is therefore protected against loss of electricity at the customers' end. Telecommunications operators power their nodes (in central offices or in outside plant sites) while customers are responsible for the energy fed to the end-equipment (e.g., modem, access gateway, set-top box), including any backup. Additional measures are brought into play to protect calls to emergency services. With the advent of voice services over the Internet the responsibility for powering broadband telecommunications is split between telecommunications operators and customers. To enable emergency services to be maintained, new Federal Communication Commission (FCC) rules are being introduced, "providers of modern home voice services (i.e., facilities-based, fixed, voice residential service that is not line-powered) will be required to ensure that a technical solution for eight hours of standby backup power is available for consumers to purchase at the point of sale" [b-FCC rule].

Traffic to broadcast radio and television (TV) transmitters is also protected when routed over core and protected backhaul networks.

A mobile network topology is shown in Figure 3, see [b-BridgeWave]. This uses synchronous digital hierarchy (SDH) rings for backhaul of voice and data services (2G, 3G and 4G) and Ethernet rings for 4G upgrades to a serving area.

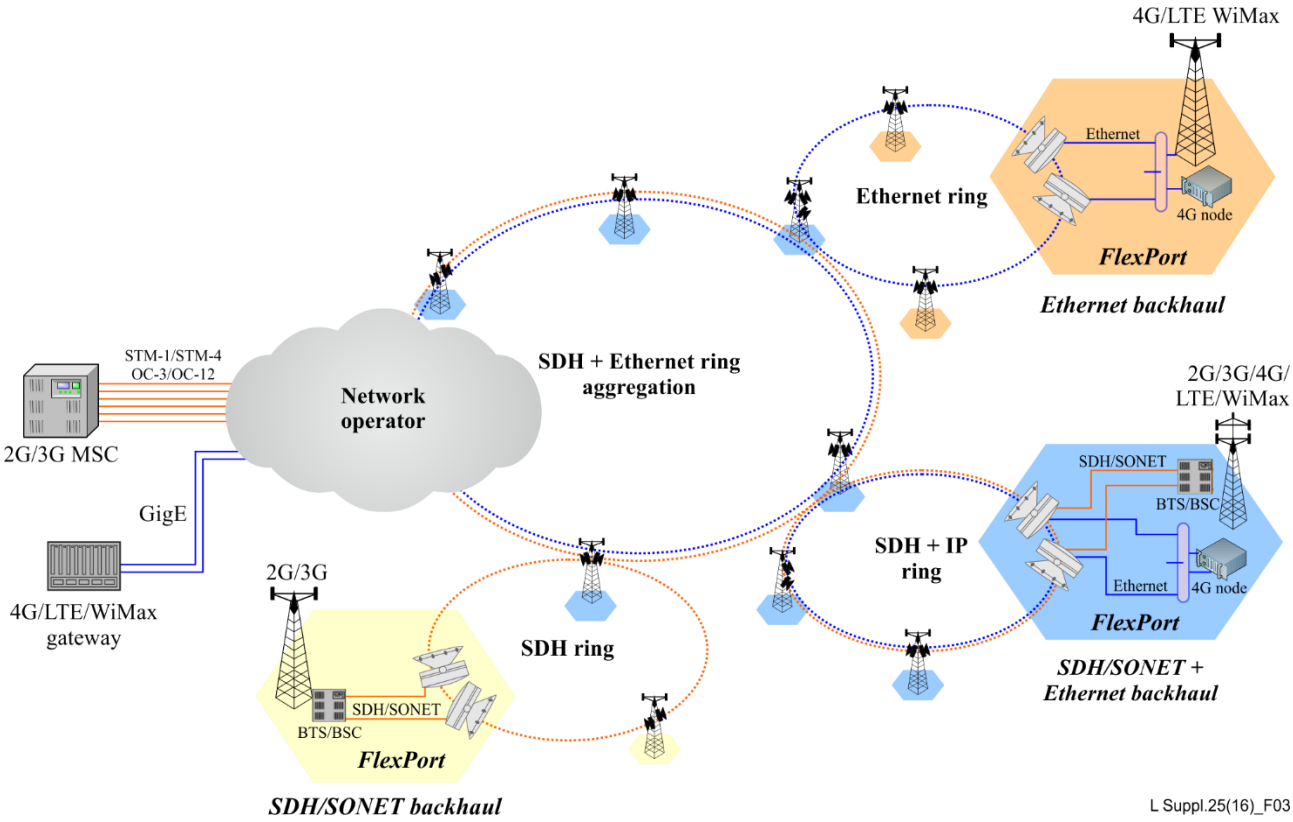

Figure 3 – Mobile network topology

In addition, the Internet protocol (IP) used for data transmission includes a facility for seeking an alternate path in the event of failure of the primary path through the network, but the self-recovery time can be up to three minutes.

6 Examples of climate change adaptation options and strategies

This section lists examples of measures that can be taken to improve the resilience of telecommunications infrastructure to extreme weather events arising from climate change. Public safety can be improved by implementing measures to improve continuity of communications services during extreme weather events.

- Make the backbone network redundant for most if not all service areas, and more resilient to all types of extreme weather events.
- Provide reliable backup power with sufficient fuel supply for extended grid power outages.
- Decouple the communication infrastructure from the electricity grid infrastructure to the maximum extent possible, and make both more robust, resilient and redundant.
- Minimize the effects of power outages on telecommunications services by providing backup power at telecommunications sites such as generators, solar-powered battery banks, and "cells on wheels" that can replace disabled towers. Extend the fuel storage capacity needed to run backup generators for longer outages.
- Protect against outages by trimming trees near power and communication lines, maintaining backup supplies of poles and wires to be able to quickly replace those that are damaged, and have emergency restoration crews ready to be deployed ahead of a storm's arrival.
- Place telecommunication cables underground where technically and economically feasible, ensuring that they are appropriately protected against water ingress. In the long term it is normally impossible to guarantee a pipe's sealing. Thus, cables themselves have to be constructed to resist prolonged immersion in water. This can be obtained through use of water resistant metallic sheets, gel fillings, or blowing higher air pressure into cables.
- Replace the segments of the wired network that are most susceptible to weather events (e.g., customer drop wires) with more resilient low-power wireless solutions.
- Relocate central offices that house telecommunication infrastructure, critical infrastructure in remote terminals, cell towers, etc., and power facilities out of future floodplains, including coastal areas which are increasingly threatened by sea level rise combined with coastal storm surges.
- Further develop backup cell phone charging options at the customer's end, such as car chargers, and create a standardized charging interface that allows any phone to be recharged by any charger.
- Assess, develop and expand alternative telecommunication technologies if they promise to increase redundancy and/or reliability. Examples include free-space optics (which transmits data with light rather than physical connections), power line communications (which transmits data over electric power lines), satellite phones, and ham radio.
- Reassess industry performance standards combined with appropriate, more uniform regulation across all types of telecommunication services. Uniformly enforce regulations, including mandatory instead of partially-voluntary outage reporting to the regulatory agencies.

- Develop high-speed broadband and wireless services in low-density rural areas to increase redundancy and diversity in vulnerable remote regions. Include multiple operators who may benefit from infrastructure sharing to minimise costs.
- Perform a comprehensive assessment of the entire telecommunications sector's current resiliency to existing climate perils, in all of their complexities. Extend this assessment to future climate projections and likely technology advances in the telecommunications sector. This includes the assessment of co-dependency between the telecommunications and power sectors' relative vulnerabilities. Provide options and incentives to decouple one from the other while improving the resiliency of each.

The cost of implementing each of the above measures should be assessed by individual organizations and countries and set against the economic cost of loss of service and of repairing the damage to infrastructure if the above measures are not implemented. The economic benefit of each measure can then be assessed, and funding secured (if necessary from bodies such as the World Bank and the United States Agency for International Development (USAID)) to implement any measures which are demonstrated to provide a clear economic benefit.

7 Repair of ICT infrastructure for service restoration

In the event of an environmental disaster affecting ICT infrastructure (causing service disruptions), a disaster recovery plan should be triggered in response to mitigate damages. At best, all operations should resume back to normal, but during a more severe incident only limited services will be available. Priority should be given to ensure critical operations are maintained and damage is minimized. In contrast to planned or autonomous adaptation measures, recovery requires assessment of current conditions and immediate decisions are needed on the required actions based on the recovery plan. A disaster recovery plan should include sections on managing ICT infrastructure recovery and on actions required in various scenarios including the effects of climate change. In a broad sense, the response plan should include the activities needed to repair, replace or remove.

Repair – In situations where there is minimum damage, repairing on site might be the best option. However, consideration must be given on the duration of repair, available parts, skilled resources and access to the location. For critical situations, temporary measures must be put in place to ensure continuous operation during repair. Recovered equipment might be brought back to base for repair to be re-deployed once tested. For example, fibre fractures causing failure to a primary transmission link need to be spliced back together and restored to service in due time.

Replace – Replacement might be required for severe damage either as a temporary or permanent solution depending on the service level agreement (SLA) required to be met. Direct replacement of similar equipment is only possible if the required parts and resources are available and conditions permit. Typically, a short term temporary solution is deployed to maintain service availability (partial or full) until a permanent replacement is available. For example, a mobile vehicle including a base station can be deployed to restore coverage for mobile base stations damaged by flood. Power may come from mobile generators.

Remove – In certain situations, damage to a particular part of a network can cause a cascading of the detrimental effect. For example, a base station damaged by a landslide is no longer safe and a temporary structure may be erected nearby, at a safer location. This base station, however, may be part of a distribution network connecting to two other base stations. In this case the antennas on these other base stations will need realigning to maintain system margin.

8 Examples of disaster relief systems

Examples of disaster relief systems are considered with reference to the work of ITU-T Focus Group on Disaster Relief Systems, Network Resilience and Recovery [b-ITU-T FG].

8.1 Early warning systems

A disaster detection and early warning system is required for preparation before a disaster occurs. During an incident or a disaster, an emergency alert system and an evacuation assistance system are used to evacuate people from potentially dangerous areas and rescue those in danger. A safety confirmation system is utilized to confirm the safety of each person and assist rescue work immediately after an incident and, for a certain period of time, during a disaster. A system supporting health care, and for sustaining the lives of the victims, may also be necessary for a relatively long period of time after an incident. Until now, radio and TV broadcasting, amateur radio and fixed phones have been mainly used for disaster relief systems. New disaster relief systems that employ mobile and digital signalling have recently been introduced and these new types of disaster relief systems should be developed further. In addition, the care of the disabled must also be considered when developing these systems.

8.2 Recovery of the emergency network

Network resilience and recovery depends on a highly-reliable network design, such as multiple network routes. For emergency telecommunications it is useful to establish temporary telephone services by temporarily restoring damaged mobile base stations after a disaster. In addition to the scenarios (or use cases) involving the strengthening of existing networks in operation, it is necessary to consider a complementary approach that mobilizes ICT facilities surviving in the devastated area, connects them with instantly deployable and configurable ICT resources, and then builds local networks to satisfy the urgent need for communication between rescue teams and local citizens in the area.

8.3 Backup of electric power supply

A highly reliable way of guaranteeing an electrical power supply for telecommunication equipment must be ensured by using, for example, multiple electrical distribution routes and an electrical generation system. If automatic power backup systems are not provided (e.g., standby battery, and/or generator) network operators may provide mobile generators which may be rapidly deployed to a disaster area by vehicular transport. An effective way of refuelling electrical power generators after a disaster should also be considered.

9 Additional requirements to maintain essential services carried via the Internet

Internet access is now regarded as an essential service in developed countries. Legacy networks are being transformed to provide these services in addition to traditional telephony services by adding more capacity and functionality.

A question to consider is whether traditional approaches to resilience are sufficient to maintain essential services and, if not, what should be changed.

One example is how to contact the emergency services. In the days before telephony, whistles were used to summon the police. Then, with telephony services, emergency numbers could be dialled. Now that the Internet is becoming universally available, what is the best way to summon an emergency service? It may not be possible for a person, facing a threat to their personal safety, to speak to an emergency service, thus some kind of automated communication service would be a better solution.

10 Electric power grid outages

Loss of electric power has serious consequences on telecommunications and other ICT services which may have either no backup power or backup for a limited time measured in hours.

10.1 Example from Italy: The national blackout 2003 and its consequences for the future

The 2003 Italy blackout was a serious power outage that affected all of Italy for 12 hours and part of Switzerland, near Geneva, for 3 hours on 28 September 2003. It was the largest and most serious blackout in Italy in 70 years, affecting some 55 million people. Similar wide-scale blackouts were also happening in: USA-Canada (2003 north-east – 55 m people), Indonesia (2005 Java – 100 m people), Brazil-Paraguay (2009 – 87 m people), India (2012 – 620 m people), Bangladesh (2014 – 150 m people), Turkey (2015 – 70 m people), Pakistan (2015– 140 m people) and Sri Lanka (2016 – 21 m people).

During the Italian blackout, storms and overloads caused the energy interconnection lines from Switzerland and France to open. Control of the electricity grid was lost in a few seconds, and the lines tripped in a cascading effect.

Throughout Italy, trains and flights were cancelled and road traffic in the entire country was blocked.

In the northern regions, electricity service was restored within a few hours, but the southern-most part of Italy needed much more time to restore service.

Part of the reason causing the blackout was due to a cascade of failures in interdependent networks. As an example, some functions of the energy networks lost communication capabilities, causing a failure of the Internet communication network, which in turn caused a further breakdown of power stations.

Fixed telephone service remained on and running through the operation of its power backups. Some troubles were experienced as many diesel generators needed to be refuelled throughout the country, requiring extra man-hours for the maintenance teams. Service continuity was maintained, and the fixed telecommunications network provided the main means for keeping the population informed and calm.

Mobile telecommunication was the primary resource enabling those not at home to communicate. It suffered immediate problems of traffic overload and later, after a few hours, a significant number of the nodes were lost as batteries were exhausted.

Internet communications services remained on with backup power similar to that of the fixed telephone service, but it suffered troubles as much of the end-user terminating equipment lost power supply as these are not normally provided with power backups such as uninterruptible power supplies (UPSs).

Measures have been taken to avoid a similar event repeating, mainly in the energy sector. Its control and communications systems have been made more resilient and also its connection to the wide area communications service.

Studies have evaluated the behaviour of a similar series of events, if they were to happen today. The present situation of the energy system is much more complex than what it was in 2003 as it now includes a huge number of generators from renewable sources (but these are less predictable). Stability of the energy system depends more and more on coordination among all actors (energy generators, transmission and distribution, and users). If these should fail, then blackouts could be much more catastrophic as chain effects would be multiplied due to the much higher interconnection of all involved systems.

One important message from this is the need to guarantee an end-to-end service and the role key stakeholders' equipment play, such those of electricity, gas, water generation and distribution companies. Such equipment also needs to be able to maintain service in the event of local blackouts as their failure could cause trouble well beyond their location.

ICT services also need to be designed and operated to guarantee both quality and continuity of service, particularly today with the trend towards software defined networks (SDNs) and network function virtualization (NFV). Functions that before were all in the same local system will have some of their functions possibly located in a data centre hundreds of kilometres away. This will pose new challenges to service availability and continuity in case of occurrence of extreme events such as loss of power. Networks as a whole will then have to be designed to include redundancies (of power, equipment, data paths, etc.) so that service can be sustained even if parts of the communications paths have failed (e.g., paths in the backbone connections).

11 Example: Malaysia flood challenges, recovery and mitigation best practices

In Malaysia, the year-end monsoon season typically spells wet weather conditions with heavy rainfall and strong winds sweeping across the nation. December 2014 marked one of the severest flooding incidents, affecting eight states in Peninsular and East Malaysia. The highest recorded rainfall was 255 mm and more than 160,000 people were evacuated from their homes with reports of disaster casualties. See [b-IFRC].

Immediately, access to affected areas was cut-off, with roads, buildings and houses completely submerged underwater. Rescue teams had to rely on alternative transports (boats and helicopters) to reach victims. Electricity was suspended and water resources were affected. Mobile coverage was affected as some of the telecommunication sites were completely "knocked-down" by the flood rendering them out of service.

The work required by network operators to bring back service was challenging due to:

1. Prolonged electricity shutdowns at large areas affecting sites;
2. Closure of access roads and limited alternative transportation (e.g., boats);
3. Dangerous and safety concern to access the affected sites/areas;
4. Site or equipment badly damaged (fully or partially submerged);
5. Limited diesel supply;
6. Information management and site recovery coordination on the ground as the affected sites were unusually and unexpectedly large;
7. Sites located at isolated and remote areas for recovery activity.

Network recovery started with the setting up of an emergency flood command centre to facilitate close collaboration among network operators, facilities providers, rescue teams, and national organizations. After detailed assessment of the situation, services were slowly restored by deploying mobile base stations and mobile generators to cut-off areas. One of the fastest service recovery methods was to explore the domestic roaming feature which allowed affected operators to bring up service in another operators network. In the long run all of the affected sites were required to be rebuilt to ensure continuity of service.

As floods are becoming more of a seasonal event, it is inherent that network infrastructure is designed to be resilient and implemented to mitigate the possibility of flooding. Resilient backhaul is necessary to ensure redundancy and preventing isolation of any part of the network. Physical platforms for cabins, equipment rack and generators are raised with concrete slabs above the expected flood levels. Sensors, as early warning detection systems, play a major role in the assessment and preparation of

current conditions. During the monsoon season, field forces are kept on standby with enough spares, backup generators and diesel fuel to recover the network. Backup batteries for flood-prone sites are also extended beyond the normal service level. Malaysia is currently exploring sustainable energy sources such as hybrid systems, solar implementation and fuel cell solutions to address the issue of powering isolated sites. Should the service coverage go totally down for an area, mobile base stations should be ready to be deployed upon immediate notice. The biggest learning point is coordination between stakeholders and holds the key to ensuring correct propagation of information and sharing of recovery load to hasten the speed of recovery.

12 Example of resilient communications infrastructure: Telefónica Vivo sustainable mobile site in Rio de Janeiro (Brazil)

In an extremely competitive market such as the telecommunications sector, companies that provide these services work hard to maintain and assure its customers quality service without disruption. To do this, the communications infrastructure must be robust and resilient to all types of incidents. The effects of climate change such as flooding or high temperatures present a high risk to the reliable functioning of the communication infrastructure and thus for the provision of critical services.

Faced with this reality, ICT companies such as Telefónica, are starting to take these risks into account by designing new resilient telecommunications infrastructure to cope with climate impacts. The sharing of these designs is key to the entire ICT sector adapting to climate change.

Due to the growth of traffic and deployment of 4G technology for mobile telephony, which occurred primarily in the host cities of the FIFA Confederations Cup that took place in Brazil in 2014, a significant increase in the number of base stations in these cities was needed. Brazil, and in specific the coastal regions, has elevated temperatures during the summer, and most sites require energy consuming climate-control equipment.

The solution used by Telefónica Vivo (the mobile and fixed operator of Telefónica in Brazil) has been the use of public lighting poles to meet the demand of base stations without introducing new elements to the above-ground infrastructure. See Figure 4. Some equipment was located underground to avoid heat exposure to the equipment. The solution below is an example of communications infrastructure which is adapted to the effects of climate change while reducing the visual impact of the antennas.

The solution for urban areas uses existing infrastructure and is a great alternative to building new structures in restricted areas, reducing the visual impact and facilitating additional network infrastructure deployment.

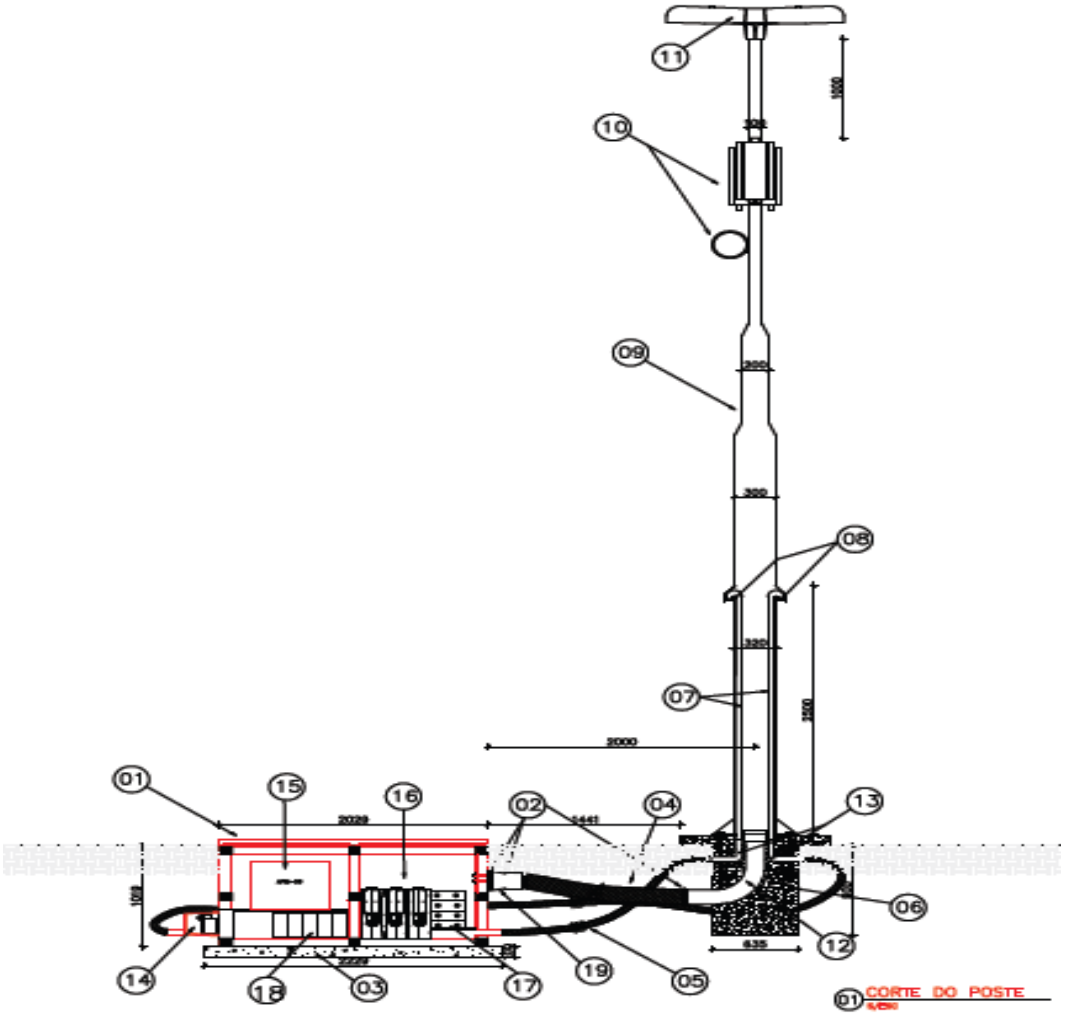

Figure 4 – Use of public lighting poles to include base stations

Key features are:

- Using public lighting infrastructure in standard public areas;
- Accommodation of equipment in the boxes underground.

The lamp post used is manufactured by an approved supplier for Rio Light and required a small adjustment in its interior to create ducts where air circulates and is responsible for cooling of the equipment inside the enclosure.

Equipment is placed inside of a box that is installed underground allowing the integrity of the equipment. The box is hermetically closed so it is resilient to flooding and high temperatures. See Figure 5.

Figure 5 – Underground equipment enclosures

The project was developed by the team of Telefónica Vivo in partnership with a local company specializing in technology "FIBERGLASS" (fibre reinforced plastic glass) and appropriate to the climate conditions of Brazil. Figure 6 shows the evolution of the base station infrastructure.

2011 **2012** **+2013**

Figure 6 – Evolution of the base station infrastructure

Appendix I

Example of a future hybrid satellite/terrestrial system

This appendix refers to a possible future system and does not form an integral part of this Supplement. The prototype technology was produced in the research project BATS (Broadband Access via integrated Terrestrial & Satellite systems), funded under the European Union 7th Framework Programme [b-Project-BATS].

In this example a novel architecture is proposed which combines satellite and terrestrial service delivery, dynamically routing each traffic flow according to its service needs through the most appropriate delivery mechanism to optimise the quality of experience by, for example, routing large packets via a terabit satellite network to reduce end-to-end transmission delays. The combination of two or more networks provides additional capacity by the ability to route traffic via alternative routes and increase resilience through diverse routing.

Satellite based systems have the following advantages compared with a fixed or mobile (terrestrial) telecommunications infrastructure:

– They can cover a wide area;

– They can be deployed rapidly, especially if using satellites already in orbit;

– They are easy to set up and can be reconfigured flexibly, especially using multi-spot beam satellites;

– They are relatively low cost for a rural coverage area, and may have lower greenhouse gas emissions compared to terrestrial systems.

Because satellite-based systems can be set up and configured rapidly, they are particularly suited to respond to disaster situations. This is the topic of an existing Handbook, "Emergency and Disaster relief" [b-ITU-T Handbook] which includes, for example, portable satellite terminals as an integral part of the document.

Examples of communications satellite systems include:

– Geostationary satellite systems: These have a relatively high latency (round trip delay) and cannot be used where short service response times are required.

– Low earth orbit satellite systems: These have a much lower latency but require many more satellites, more frequent hand-overs between satellites and a more complicated and higher cost system.

– Hybrid satellite systems: These utilize a combination of terrestrial and satellite paths to provide users with an interactive broadband service with an acceptable response time.

The architecture of a *hybrid* broadband satellite network is shown in Figure I.1. The main additional elements compared with a conventional geostationary satellite system are the ability to integrate communication paths with different latency, jitter and throughput and present these to the user as a single integrated communications link. This is the function of an intelligent user gateway (IUG) at the user's premises with a corresponding intelligent network gateway (ING) in the network. The use of multiple access connections between an IUG and ING is shown in Figure I.1. It is anticipated that satellite plus one other communications path is provided so that alternative paths are available for different types of traffic. The traffic is classified before transmission and the link with the most appropriate characteristics (in terms of latency, jitter and bandwidth) used to transport each type of traffic.

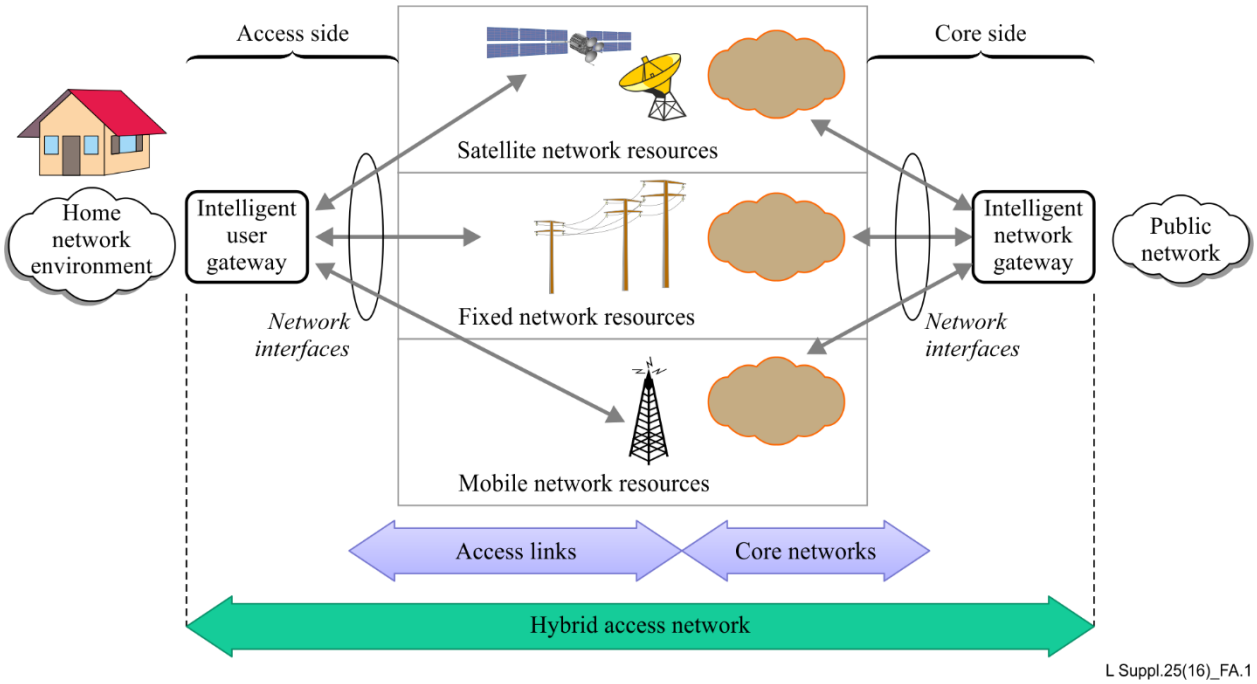

Figure I.1 – Hybrid satellite/terrestrial system architecture

The service provider should manage the multiple access network connections to the IUG as a virtual service provider of both the satellite and terrestrial (fixed or mobile) network. The service provider must be able to monitor the performance of the all types of communication links in order to ensure that a minimum quality of service (QoS) (in terms of latency, capacity and delay) is provided.

The integration of an IUG and ING into a hybrid broadband satellite network architecture is shown in Figure I.2. The IUG is located on the customer premises and provides secured broadband access, cached storage capacity and QoS provisioning. It not only provides an interface to several access links, but the IUG will select access delivery routes in multi-operator and multi-service provider domains, matched to the quality of experience (QoE) needs of the different applications and service components. The IUG would be able to assess in real time the QoS requirements of each application or service component and accordingly make routing decisions to optimize the QoE. It also exploits the storage resources of the IUG for high-bandwidth low-priority traffic caching during off-peak hours, to support applications such as over-the-top (OTT) TV service.

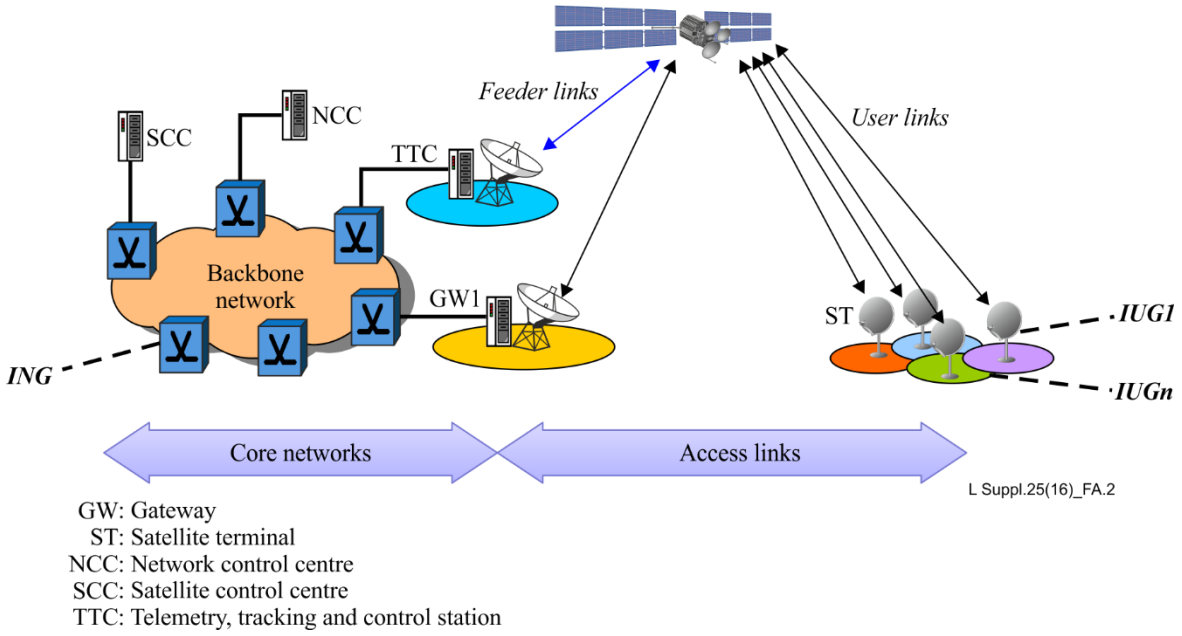

Figure I.2 – Satellite access network architecture connected to an IUG and ING

The ING is a counterpart of the IUG located at the edge of the core network. It is a convergence point for the different user traffic flows handled in the different access links (e.g., satellite, xDSL, mobile network resources). The ING works in a similar way to the IUG to select the relevant individual or combined access links for the forwarding of the different traffic flows for the downlink direction (traffic from the public network to the end-user premises).

Bibliography

[b-ITU-T G.984.1] Recommendation ITU-T G.984.1 (2008), *Gigabit-capable passive optical networks (GPON): General characteristics*, Section 14.
<https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.984.1-200803-I!!PDF-E&type=items>

[b-ITU-T FG] ITU-T Focus Group on Disaster Relief Systems, Network Resilience and Recovery, Homepage.
<http://www.itu.int/en/ITU-T/focusgroups/drnrr/Pages/default.aspx>

[b-ITU-T FG-Gap] ITU-T Focus Group on Disaster Relief Systems, Network Resilience and Recovery (2014), *Gap Analysis of Disaster Relief Systems, Network Resilience and Recovery*.
<https://www.itu.int/en/ITU-T/focusgroups/drnrr/Documents/fg-drnrr-tech-rep-2014-3-Gap_analysis.pdf>

[b-ITU-T Handbook] ITU Handbook (2006), "*Emergency and Disaster relief*", ITU-T, Geneva.
<http://www.itu.int/pub/R-HDB-48>

[b-BridgeWave] BridgeWave Communications.
<http://www.bridgewave.com/products/flexport80.cfm>

[b-BT Wi-Fi] BT Wifi Hotspots in the UK.
<http://www.btwifi.co.uk/find/uk/>

[b-FCC rule] USA, FCC "*FCC adopts rules to help Americans communicate during emergencies*".
<https://www.fcc.gov/document/fcc-adopts-rules-help-americans-communicate-during-emergencies>

[b-IFRC] IFRC, Malaysia: Seasonal Floods 2014 Information bulletin "*Emergency Plan of Action operation update Malaysia: Seasonal Floods 2014*".
<adore.ifrc.org/Download.aspx?FileId=70128>

[b-Overview] Overview of Disaster Relief Systems, Network Resilience and Recovery.
<https://www.itu.int/en/ITU-T/focusgroups/drnrr/Documents/fg-drnrr-tech-rep-2014-1-Overview.pdf>

[b-Project-BATS] Research project BATS (Broadband Access via integrated Terrestrial & Satellite Systems).
<http://www.batsproject.eu/>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	**Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant**
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016