EC-RRG
Electronic Communications
Resilience & Response Group
Protecting Communications

EC-RRG Resilience Guidelines for Providers of
Critical National Telecommunications Infrastructure

June 2021

Contents

1 Introduction

The purpose of these guidelines is to bring together a wide range of advice and guidance on agreed best practice in the establishment and maintenance of resilience within telecommunications networks and services, for those Communications Providers which are considered to be part of the UK's Critical National Infrastructure (CNI), either because of the scale of their operations or because they provide key services to other parts of the CNI. However, these guidelines do not represent regulatory guidance. In particular, they do not seek to clarify compliance with current UK regulation relating to Publicly Available Telephone Services, since such services are provided by a wider group of Communications Providers than form part of the CNI. However, and for the avoidance of doubt, these voluntary guidelines are relevant to both fixed and mobile providers and networks.

These guidelines are not intended to cover all the actions that might be required in the event that resilience has been compromised and emergency remedial action across multiple providers and/or government is required. This topic is covered by the UK Telecommunications Industry Emergency Plan.[1]

They are also not intended to cover any Orders that might be made by government in times of emergency, for example, those made under Part 2 of the Civil Contingencies Act, under Section 94 of the Telecommunications Act or Section 132 of the Communications Act. These guidelines are not intended to be used to specify contractual obligations between Communications Providers and their customers and should not be used for this purpose. However, the Centre for the Protection of the National Infrastructure (CPNI) has published helpful guidance to customers on Telecommunications Resilience and how to approach[2] Communications Providers when seeking to procure resilient services.

[1] There is a national industry wide emergency plan which is owned and managed by the EC-RRG.

[2] Telecommunications Resilience:
https://www.gov.uk/guidance/telecoms-resilience

2 Definitions

In these guidelines, the following definitions apply:

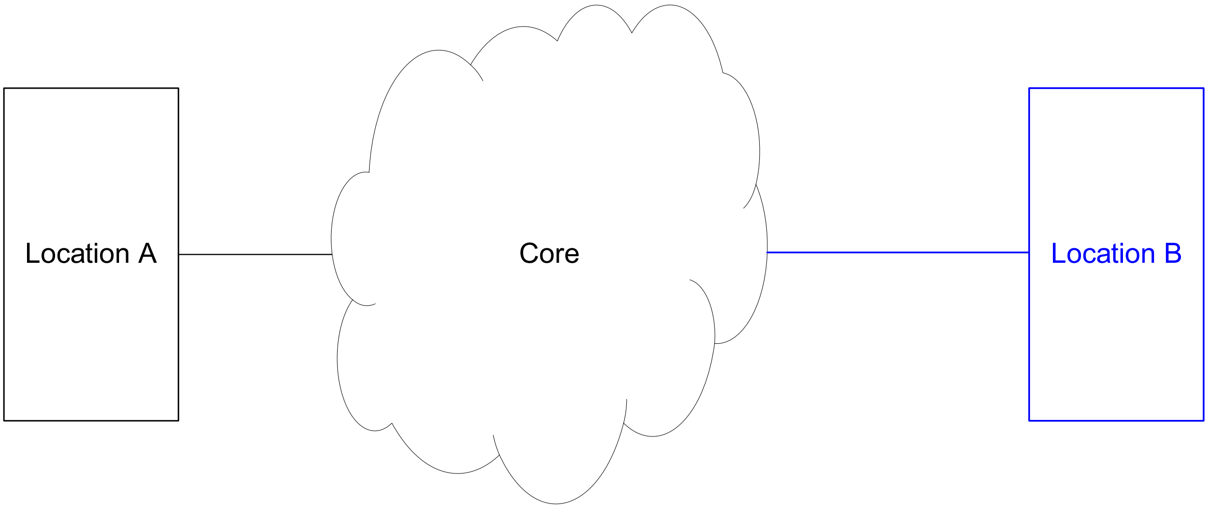
2.1 Resilience

The word ‘Resilience’ is to be interpreted in the broadest sense as the ability of an organisation, resource or structure to be resistant to a range of internal and external threats, to withstand the effects of a partial loss of, or degradation of platform, system or service and to recover and resume provision of service with the minimum reasonable loss of performance.

To enable the provision of service to be resilient the following attributes need to be considered and documented when designing a service:

- Definition of the expected performance metrics and identification of any potential limitations of performance, to enable service levels to be defined
- The understanding of the environment that the service operates in (maintaining Situational Awareness or Context Awareness)
- The environment and location(s) from where the service is supported
- The provision of service which may be composed or programmed on demand and may be dependent on the environment
- The improved efficiencies of the design, the properties of complex systems, close or tight coupling, interdependencies and their emergent properties, their proximity to the failure envelope, balancing with the need to backup, buffer, segregate and ensure capabilities are maintained to mitigate any unforeseen degradation or compromise and to ensure rapid restoration of provision of service
- A capability to monitor the environment to be able to detect and anticipate approaching threats and hazards, including changes in the environment
- A capability to monitor the provision of service, to determine whether service levels are being met, recognising the need to anticipate future events and longer-term performance trends (including event or log capturing)
- Identification of potential limitations of performance, or modes of failure, or degraded operation of the service in order that response and recovery plans can be developed and maintained, being mindful of the likelihood of human error
- How protective measures may mitigate these risks
- A process to review and explore unexpected performance or near misses, which drives a process to learn, adapt and improve future design and provision of service, being mindful that a failure or degradation of a complex system is likely to have complex causes and how to achieve organisational learning

To illustrate a resilient delivery, we will consider the following two examples which are edge cases:

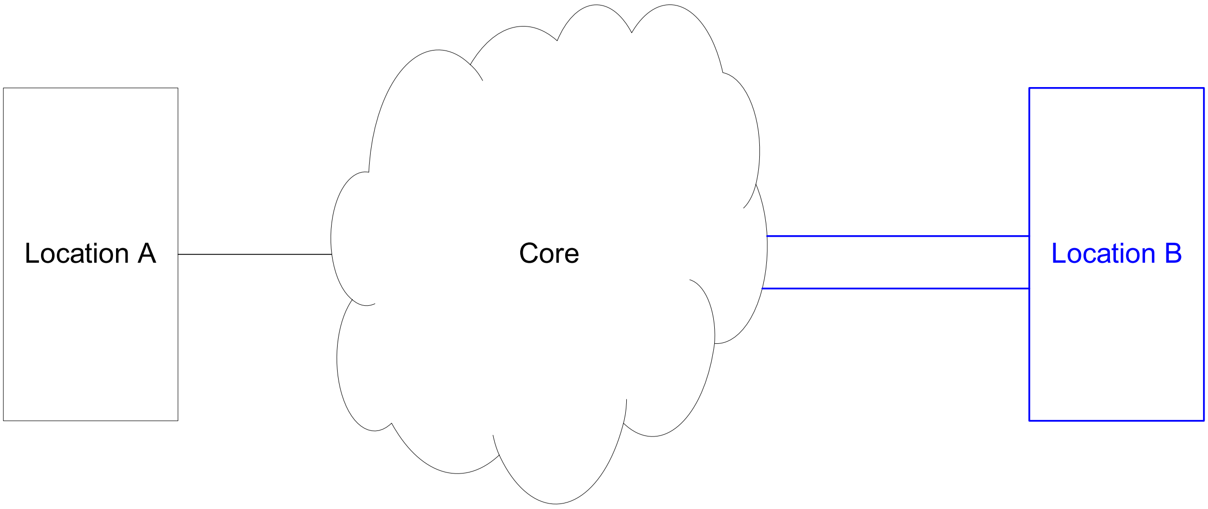


Example 1

In common parlance the provision of service to Location B is often stated to be non-resilient for example 1, whilst in example 2 the service provision to Location B is often said to be resilient.

However, it may be possible for the converse may be true.

If in example 1 the service delivered to Location B is supported by an organisation that has considered and has in place the resilience attributes described in this guidance, then whilst there is the possibility that the service provision may fail to Location B occasionally, the organisational processes will ensure that in any failure, the recovery and resumption of provision of service with the minimum reasonable loss of performance should be achieved whilst;



Example 2

In example 2 the particular provision of service to Location B may appear to be resilient due to having duplicated or diverse delivery of service to Location B, the details of how the delivery is designed and supported, both technically and organisationally, is not clear and may not assist in the recovery and resumption of provision of service with the minimum reasonable loss of performance for all modes of failure (if the attributes in this guidance have not been considered and designed for the provision of service to Location B).

2.2 Communication Provider (CP)

"Communications Provider" means-

a) a provider of a public electronic communications network;
b) a provider of a public electronic communications service; or
c) a person who makes available facilities that are associated facilities by reference to a public electronic communications network or a public electronic communications service;
and who is considered to form part of the CNI.

2.3 Public Electronic Communications Network (PECN)

"Public Electronic Communications Network" means an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public;

2.4 Public Electronic Communications Service (PECS)

"Public Electronic Communications Service" means any electronic communications service that is provided so as to be available for use by members of the public;

2.5 Electronic Communications Network (ECN)

"Electronic Communications Network" means:

a) a transmission system for the conveyance, by the use of electrical, magnetic, optical or electro-magnetic energy, of signals of any description; and
b) such of the following as are used, by the person providing the system and in association with it, for the conveyance of the signals:
   i. apparatus comprised in the system;
   ii. apparatus used for the switching or routing of the signals; and
   iii. software and stored data.

2.6 Electronic Communications Service (ECS)

"Electronic Communications Service" means a service consisting in, or having as its principal feature, the conveyance by means of an electronic communications network of signals, except in so far as it is a content service.

2.7 Associated Facility

"Associated Facility" means a facility which:

a) is available for use in association with the use of an electronic communications network or electronic communications service (whether or not one provided by the person making the facility available); and
b) is so available for the purpose of:
   i. making the provision of that network or service possible;
   ii. making possible the provision of other services provided by means of that network or service; or
   iii. supporting the provision of such other services.

3 Revision

These guidelines will be subject to review and amendment following consultation with the EC-RRG membership.

4 Requirements

This section identifies the scope of requirements that these Guidelines will be required to address.

Subsequent to the previous update of these Guidelines in 2018, there have been a number of significant publications that have addressed risks to Resilience for future 5G and Full Fibre networks:

- Future Telecoms Infrastructure Review - describing the future Socio-Economic Dependency on 5G and Full Fibre Networks
- Supply Chain Review - detailing the increase in security and resilience risks associated with 5G and Full Fibre Networks
- Telecommunications Security Requirements - identifying a two phased approach to Risk Mitigation for 5G & Full Fibre Networks
- ENISA 5G Threat Landscape - summarising the network and service asset groups in 5G and Full Fibre Networks that have a high dependency on resilience

It is also the case; that in the UK, the initial deployments of 5G and Full Fibre Networks will be occurring within the same timeframe as existing network transformation projects are scheduled to complete:

- PSTN Switch-Off Complete - 2025
- High Risk Vendors Removed - 2027

With specific reference to the transformation from Legacy to All IP (Next Generation Networks), it is vital to ensure that the Best Practice developed by the CP Community during this transformation, is carried forward as 5G and Full Fibre networks are being developed and deployed.

The following sections provide further details on the scope of requirements that these Guidelines need to address. For a high level description of how Legacy to All IP network transformation will be extended to support 5G and Full Fibre networks, please refer to annex C.

4.1 The Supply Chain Review & Telecom Security Requirements

The Supply Chain Review (SCR)[3] states that a technical pre-condition for secure 5G and Full Fibre networks is to provide a clear statement of what 'good' looks like in relation to network security and resilience.

The SCR focused on telecoms Critical National Infrastructure (CNI) supporting public telecommunications networks and services and covered terrestrial infrastructure and those parts of the network most critical to the operation of 5G and Full Fibre.

[3] DCMS - Supply Chain Review: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf

The SCR has identified that 5G and Full Fibre networks create new challenges for security and resilience, as the technical characteristics of 5G increase the risk profile of these networks compared to previous generations of networks.

5G networks will be based on software running on commodity hardware and the speed, scale and processing power of these technologies will enable a wide range of new services, in addition to enabling the migration of 'core' functions closer to the 'edge' of the network in order to reduce latency.

While previous mobile generations connected people to people, 5G has the potential to connect a vast network of people, objects and communication systems (e.g. internet of things), including in critical sectors.

This brings a new dimension to security risks, given the greater dependence that UK CNI is likely to have on 5G infrastructure compared to 3G/4G.

The specific risks identified in the SCR include the uplift required for 5G Architecture and the subsequent dependency on dense fibre deployments to support enhanced RAN and Edge capabilities:

- Network Functions Virtualisation (NFV) and the associated requirements for Management and Network Orchestration (MANO) will underpin the critical functions of the core, and therefore they must comply with the highest levels of security
- Mobile core functions may move from centralised locations to local aggregations sites - requiring enhanced security and availability capabilities at lower levels in the network hierarchy

The SCR also focused on the sustainable development of diversity within the supply chain - entailing greater need for multi-vendor Integration and the use of software-based interfaces to enable:

- software-based innovation in core network functions, and
- open architectures in access networks and small cell technologies.

However, enabling Integration will need to be considered at the same time as the need to Segregate different domains throughout the 5G architecture, in order to meet the extensive requirements identified in the Telecommunications Security Requirements (TSR) for containment and isolation of 5G and Full Fibre network components supplied by High Risk Vendors.

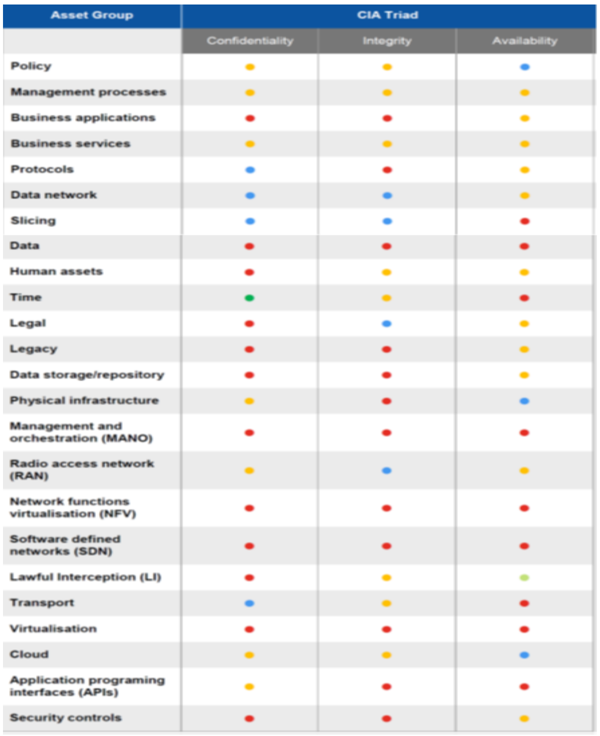
In their 2020 '5G Threat Landscape' - ENISA[4] have taken into account the role of Assets and Asset Groups in maintaining the security-related properties of confidentiality, availability and integrity.

An initial assessment of their importance has been developed, where the emphasis has been given to asset groups responsible for maintaining the overall security and availability of the 5G infrastructure.

[4] ENISA - 5G Networks Threat Landscape (Dec 2020): https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/at_download/fullReport

In their report, ENISA identified the following areas as potentially having a very high impact on Availability :

- Virtualisation
- Management & Orchestration
- Software Defined Networks
- Slicing
- Data
- Transport
- APIs



Asset Group	CIA Triad		
	Confidentiality	Integrity	Availability
Policy	🟡	🟡	🔵
Management processes	🟡	🟡	🟡
Business applications	🔴	🔴	🟡
Business services	🟡	🟡	🟡
Protocols	🔵	🔴	🟡
Data network	🔵	🔵	🟡
Slicing	🔵	🔵	🔴
Data	🔴	🔴	🔴
Human assets	🔴	🟡	🟡
Time	🟢	🟡	🔴
Legal	🔴	🔵	🟡
Legacy	🔴	🔴	🟡
Data storage/repository	🔴	🔴	🟡
Physical infrastructure	🟡	🔴	🔵
Management and orchestration (MANO)	🔴	🔴	🔴
Radio access network (RAN)	🟡	🔵	🟡
Network functions virtualisation (NFV)	🔴	🔴	🔴
Software defined networks (SDN)	🔴	🔴	🔴
Lawful Interception (LI)	🔴	🟡	🟢
Transport	🔵	🟡	🔴
Virtualisation	🔴	🔴	🔴
Cloud	🟡	🟡	🔵
Application programing interfaces (APIs)	🟡	🔴	🔴
Security controls	🔴	🔴	🟡

As defined in the Future Telecoms Infrastructure Review (FTIR), Full Fibre is a key enabler of future economic development as well as 5G technologies:

- providing symmetrical speeds and lower latency
- enabling more corporate systems and services to be hosted in the ‘cloud’
- and delivering high speed and high capacity fronthaul / backhaul capabilities.

The above not only increase operational efficiency but also create a key dependency on network availability and reliability.

The full fibre market will also encourage smaller, sub-national, operators to develop their own share in the business connectivity market, and they will need to ensure they are providing the necessary levels of security and resilience particularly for critical services.

5 Regulation

The national regulator for the communications sector in the UK is Ofcom, who will decide whether any given provider is compliant with obligations that are set out in UK legislation. These guidelines do not address compliance to this legislation or regulations.

6 Guiding Principles

Given the broad definition of resilience, it can be seen to embrace:

a) Good network design;
b) Effective operational processes for network operations, management and maintenance;
c) Business continuity planning and disaster recovery;
d) Appropriate processes to respond to a range of contingent risks.

All Communications Providers should maintain an ongoing programme of risk assessment and make plans and investments commensurate with the identified risks, taking into account both the likelihood of events and the impact of their occurrence. Communications Providers should take a holistic view of resilience, so that it is seen as an integral part of a set of wider company processes, for example:

a) Overall company Risk Management (ISO31000)
b) Quality Management (ISO9001)
c) Information Security (ISO27001)
d) Business Continuity Management (ISO22301)

There should be management commitment to all these processes, with a clear line of responsibility and chain of command from the Board level right down to operational delivery. In many cases, Communications Providers are not wholly responsible for all parts of the service they deliver. For example, they will often rely on interconnecting networks to reach all their customers, or be reliant on some common external facilities (e.g. the DNS system), or may procure underlying network services or infrastructure from other providers. In such cases, the overall resilience of their service is dependent on these other parties.

Communications Providers may seek Service Level Agreements and contractual arrangements to meet their overall resilience requirements, but it is far more effective to ensure that all such external suppliers take a similar and complementary approach to resilience management, as legally binding commitments might be of little real value in a crisis.

Endeavours should be made to regularly review these topics with their suppliers, partners or peers with a view to jointly understanding risk[32] and agreeing the optimal management of those risks.

a) Security and Resilience
b) Business Continuity
c) Disaster Recovery
d) Quality of Service management
e) Emergency Planning[5]

[5] Providers of Publicly Available Telephone Services have obligations relating to Emergency Planning under condition A4 of the Conditions of Entitlement. They also have obligations under the Civil Contingencies Act 2004 as Category 2 responders: https://www.legislation.gov.uk/ukpga/2004/36/contents

7 Risks to Resilience

7.1 Generic

While it will be for each provider to assess its own risks and appropriate measures to provide and maintain resilience, there are a widely accepted set of risks that Communications Providers face.

In summary, they can be grouped into 6 headings:

a) Physical Threats
b) Personnel Threats
c) Cyber or Technological vulnerabilities
d) Loss of key inputs
e) System/Logical failings
f) Electronic 'interference'

Industry should continue to be guided by the planning assumptions relevant to national risks such as major power loss or pandemics.[6]

7.1.1 Physical Threats

These include:

a) Natural phenomena (Extreme weather, earthquake, flood and lightning);
b) Fire
c) Explosions, in particular those caused by gas leaks;
d) Damage caused by accidents, vandalism, internal sabotage and terrorism.

7.1.2 Personnel Threats

These include:

a) Insider threat (including the supply chain)
b) Human Error[7]
c) Training, key skills, knowledge or resource availability
d) Malicious acts and Hostile reconnaissance
e) Negligence

7.1.3 Cyber or Technological Vulnerabilities

These include:

a) System vulnerabilities (including software)
b) Interworking or cascade vulnerabilities
c) Capacity management/Overload controls
d) Inappropriate protective controls to protect sensitive assets
e) Separation or Segregation of networks, particularly management or control networks
f) Review, testing and management of change (detection and prevention of misconfiguration)
g) Hacking, Electronic interference (malicious or accidental)
h) TEMPEST or other malicious acts

[6] National Risk Register: https://www.gov.uk/government/publications/national-risk-register-2020

[7] Managing Human Error & the Swiss Cheese model of accident causation (James Reason): https://post.parliament.uk/research-briefings/post-pn-156/

7.1.4 Loss of Key Inputs

Telecommunications depends on the continuous availability of many ‘key inputs’, amongst which the most critical are:

a) Electrical Power
b) Fuel (for backup generators and vehicle fleet)
c) Human access (to operational installations)
d) Materials

7.1.5 System/Logical Failings

To prevent being vulnerable to the failure of a single part of the system, telecommunications companies are advised to assess the risks and invest, where practical, in duplicate or triplicate back-ups for their equipment (redundancy) and diverse transmission routings. Thus the ‘logical’ architecture of the service will be more resilient than the simple physical layout. But sometimes, due often to human error, these logical configurations can themselves fail to provide the expected level of security. The key is to avoid, wherever possible, ‘single points of failure’.

However, not all parts of the network can be made resilient and, in these cases, the complementary processes of restoration and repair have to be strengthened.

As complexity and synergies of systems increases their scale and reliability, the experience of the organisation and operators in managing these systems becomes more limited, as may be the knowledge of where the ‘edge of the envelope’ is when operating the system. This may result in systems unknowingly being operated in environments where stability and predictability of the system is limited and may result in degradation of performance or inability to recover stability promptly.

7.1.6 Software Failures

All telecommunications networks are reliant on software-controlled equipment, and no software is immune from errors and operational failings. Unlike personal computers, it is not acceptable for a telecommunications network to crash and stop responding altogether.

A particularly worrying form of software failure is called a ‘systemic’ or ‘common-mode’ failure, where a software error in one network node causes the same fault to occur in other connected nodes, leading to a ‘runaway’ failure of an entire network .

7.1.7 Hacking, Electronic Interference (Malicious or Accidental)

Telecommunications networks, especially those increasingly using IP technology, can be vulnerable to conditions entering the system via the network itself. Increasingly, these can be malicious in intent. A wide range of types of threat fall into this category, including:

a) Inappropriate signals injected by users, either too high a voltage or at the wrong frequency;
b) Electromagnetic Pulses and Emissions (EMP and TEMPEST[8]);
c) Similar signal pickup problems caused by radio interference, e.g. from amateur radio transmissions;
d) Traffic overloads often stimulated by advertising campaigns and TV based promotions or new products or services (updates to software etc.);
e) Denial of Service attacks – malicious attempts to damage a service, sometimes by traffic overload, sometimes by the transmission of ‘malware’ (malicious software);

[8] TEMPEST and Electromagnetic Security: https://www.ncsc.gov.uk/scheme/tempest-and-electromagnetic-security

f) Other impacts of 'malware' , such as viruses, worms and trojans;
g) Hacking, including attempts to subvert the proper operation of the billing system in networks;
h) The transmission of specifically crafted signalling messages, designed to cause mis-operation of the network

7.2 All IP

The following specific risks to resilience for All IP Networks (Single Network Platform) have been summarised[9]

Although All IP networking simplifies the development of multiservice converged networks supporting data, voice and video applications; by providing a common IP-based packet infrastructure, it imposes a series of design constraints that have to be met in order to make that infrastructure resilient.

- Common Transport Network
- Centralised Control Plane
- Single Management Domain

7.3 5G & Full Fibre

The infrastructure supporting Network Functions Virtualisation (NFV-I) adds new functional layers which will have an impact on reliability and availability. While new resilience mechanisms and recovery techniques have been developed, the new layers also bring new failure modes and these changes will impact resilience characteristics of the network and services supported.

The following specific risks to availability for 5G Networks have been summarised from [10]

- Virtualisation
- Management & Orchestration
- Software Defined Networks
- Slicing
- Data
- APIs

7.3.1 Impact of Virtualisation

The Virtualization of network functions increases availability and integrity requirements for shared physical resources, some of which will be placed in remote locations.

Relevant vulnerabilities include:

- Improper protection of access to physical interfaces;
- Shared resource contamination;
- Mechanisms for Hardware-Based Root of Trust (HBRT);
- Hypervisor vulnerabilities enabling cross-contamination of shared resources;
- Infrastructure hardware availability

7.3.2 NFV & MANO Risks / Vulnerabilities

The following areas of vulnerabilities have been identified for NFV Management and Network Orchestration functions:

[9] ENISA - Enabling & Managing End-to-End Resilience: https://www.enisa.europa.eu/publications/end-to-end-resilience/at_download/fullReport

[10] ENISA - 5G Networks Threat Landscape (Dec 2020): https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/at_download/fullReport

- Management Interfaces / APIs
- Service Based Interfaces of NFV components
- Data and Information Protection for NFV components
- Hardening for NFV components
- Virtualisation Platform for Virtualised Network Functions
- Affinity of NFV-I control and security functions to the virtualisation fabric under administration

The NFV-MANO function should have the capability to recreate VNF's automatically after a failure, such as a Virtual Machine (VM) failure.

7.3.3 Multi-Access Edge Computing (MEC)

Being based on virtualization and containerization, MEC is subject to a number of vulnerabilities emerging from these technologies. Examples include:

- possible contamination of shared hardware resources,
- abuse of privilege elevation vulnerabilities of containers with higher levels of privileges,
- dependencies to central orchestration functions,
- high data and session volumes that can be subject of attacks,
- use of open-source APIs.

Vulnerabilities in the virtualization platform used for MEC can also include:

- inadequate isolation of resources in operating system / container layers and
- vulnerabilities specific to cloud technologies widely used in MEC implementations.

8 Specific Recommendations

8.1 Design

8.1.1 Generic

8.1.1.1 Physical

a) A secure environment is a key factor in the maintenance of an adequate telecommunications service. The protection given to a building should be assessed and complement CPNI's protective security guidance"[11]

b) Wherever reasonable, essential equipment should not be concentrated, particularly in one building, to the extent that overall network security is jeopardised. Where essential equipment is co-located (for example, at multiprocessor sites), priority should be given to physical separation, such as a fire break, to reduce the possibility of common mode failure.

c) Underground line plant, buried at a depth where intrusions are unlikely, is preferable to aerial line plant.

d) The location of all external line plant such as underground and aerial cables should be notified to the relevant authorities as and when appropriate.

e) Suitable processes should be in place to co-ordinate the activities of the various utilities and highway authorities to ensure that risk of damage is minimised.

f) All sites, including radio mast sites, need to be secured against malicious attack and other forms of physical interference. Sites should also be capable of withstanding relevant environmental conditions. In particular, antenna masts should be designed to withstand likely wind and ice loading.

g) Where appropriate, diverse entry and exit points, e.g. to sites or buildings, should be provided (including cable entries).

h) Where appropriate, use should be made of diverse duct tracks or routes (NB: Physical separation on its own does not deliver guaranteed availability, and this is usually achieved by a combination of physical separation, redundancy and resilience.

i) Public telephone boxes should be positioned to minimise risk, for example from road accidents or vandalism. Street furniture such as cabinets should be similarly positioned and also be locked or sealed.

j) Poles should ideally be placed in the lowest risk positions consistent with their use. The positioning of aerial cables and drop-wires is subject to broader regulation and must be installed to ensure adequate clearance of vehicles, land and buildings. Poles should be regularly surveyed to ensure their physical integrity and to assess new risks, e.g. tree growth.

k) Where ventilation or air conditioning is used, single failure should not hazard the facility.

l) Essential cooling for facilities should be appropriately secured against failure.

m) Buildings should be secure against entry by unauthorised people. An adequate level of building security shall be demonstrable and commensurate with to the assessment of levels of risk and vulnerability. Secure entry systems, movement detectors and video surveillance may be necessary, and both perimeter and cellular security may be appropriate in large buildings.

n) Equipment should be carefully sited within buildings to provide physical separation and protection where required.

[11] CPNI's protective security guidance:
https://www.cpni.gov.uk/building-0

o) Processes should be in place to reduce the risk of equipment failure due to building and civil engineering works. Communications Providers should make information available on planning consents and cable routing (where necessary providing a helpline to deal with inquiries). Communications Providers should keep themselves informed about activities of other parties which may present a risk to network security.

p) Where appropriate, suitable detection and extinguishing systems for fire, detection systems for explosive and asphyxiating gases and floods are recommended. For fire detection, current experience suggests that aspirating systems are superior to fixed head detectors, particularly where airflows are influenced by forced air conditioning. Fire extinguishing systems (for example water, misting or gas dumping) may be appropriate in certain circumstances but current experience suggests that none of these are particularly suitable for very large operational areas.

q) Where normal maintenance access to a site may be jeopardised because of bad weather, arrangements for use of suitable alternative transport should be covered by the contingency plan (e.g. four-wheel drive vehicles, ' snowcats' and helicopters). At sites prone to flooding, building utilisation should be such that the least critical functions are performed in the areas of highest risk.

r) For sites hosting or supporting critical services, where these locations are within the Environment Agencies Extended Flood Outline, or where sites have experienced flooding historically, special considerations should be made to ensure the critical services can be maintained during a flooding incident (the service may be supported by delivery from an alternative site which should not be exposed to the same set of risks as the primary site) the impacts of flooding to key inputs should also be considered (Energy inputs such as Electricity, Fuel oil and Human access)

8.1.1.2 Key Inputs: Energy

a) The power supply to key equipment should not be interrupted in the event of a mains power supply failure.

b) The mains supply should be secure and steps taken to ensure that it is reliable. For major sites, it may be appropriate to acquire diverse feeds of mains supply.

c) The standby power supply should be of sufficient capacity to fully support the operational power load in the period between power failure and the cut over to any alternative supply which is available.

d) Where power is provided by batteries, the battery capacity should be specified to maintain service for an appropriate duration at any stage in the battery design life.

e) The duration and reason for the chosen duration should be documented. All batteries should be maintained to manufacturers' recommendations, taking account of expected lives as well as any recommendation to fully discharge batteries on a regular basis.

f) Standby power systems should be exercised to ensure that they perform satisfactorily under failure conditions. Wherever possible, the security of mains supply should be supplemented with an alternative supply, e.g. diesel generators. These should be regularly tested and supported by an appropriate maintenance regime.

g) Supporting processes should be in place to support extended power supply failures, for 7 days minimum for disruption to power supplies.

h) At sites where it is not practical to provide an alternative on-site supply (i.e. diesel generators), battery capacity should be designed to cover the maximum likely interruption of the mains supply or the time to travel to site with portable generating equipment.

i) There should be adequate arrangements to ensure that a supply of fuel for back-up generators is available, with contracts in place for replenishment.[12]

8.1.1.3 Key Inputs: Human access and inputs

Systems should be designed to maximise the potential for remote operation. Designs for redundant networks should consider the possibility of loss of human access to a site. In cases where human access is temporarily restricted, procedures should be in place to notify staff who would normally work at a given building or site. Contingency plans should cover the liaison with emergency responders concerning access to maintain essential services.[13]

Human operators in control centres may often have dual roles which are not recognised as being conducted in tandem:

- Operator
- Defender

The requirement to manage these workloads in tandem may not be adequately considered when reviewing or planning work schedules, particularly during peak times.

Considerations should also be made to the risks identified in the National Risk Register, for example Human pandemics which may have a direct bearing, but also Animal health (which may result in control cordons restricting access) or Seismic/Volcanic activity (which may result in people being stranded or prevented from travelling to site or spare part availability) When designing provision for alternative sites for fallback of control centres or other operational centres, their location should be considered, being cognisant that this capability may need to be maintained in the event of a loss of connectivity, consultation is recommended with the communication service provider to ensure expectations of communications provision or coverage are realised at the fallback site for the scale of fallback anticipated.

Human inputs are critical both in the design of systems, their operation, maintenance and in the review of their performance;

Design, operation and maintenance:

Complex systems are constantly evolving and being updated, consequently the capability, skills and expertise to design, operate and maintain these systems needs this parity to be maintained. This complexity results in the workforce with different levels of training, skills, knowledge and expertise, resulting in the need to manage succession planning carefully.

Review of performance:

Bias[14] unless managed carefully may devalue or negate post incident reviews, knowledge of the outcomes may lead investigators to draw out certain factors as salient either as pre-cursors or causal, leading to inaccurate or 'poisoned' analysis, this may result in important situational or human factors not being adequately considered and addressed in the analysis, the subsequent report and action plan.

[12] Preparing for and responding to energy emergencies: https://www.gov.uk/guidance/preparing-for-and-responding-to-energy-emergencies

[13] Preparation and planning for emergencies, responsibilities of responder agencies and others: https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-responsibilities-of-responder-agencies-and-others

[14] Emergency planning college: Bias https://www.epcresilience.com/EPC.Web/media/documents/Papers/Occ15-Paper-AUG-2016.pdf

8.1.1.4 Key Inputs: Materials

Adequate stocks of spare parts and consumable materials should be kept on site or at a convenient depot within a short travelling time to site. Additionally, contracts may be in place with suppliers to hold buffer stocks on behalf of the provider. Particular care should be taken for items sourced from overseas in case of transport or communication disruptions. Security risks posed by the supply chain should be considered.[15]

8.1.1.5 System/Logical Failings

Overall resilience of the network and services should be delivered through an appropriate combination of resilient equipment, redundancy, restoration, repair and review:

a) Resilient equipment means that it is designed to be inherently reliable, secured against obvious external threats and capable of withstanding some degree of damage;
b) Redundancy means that back-up systems duplicating the functionality of the systems are available to take over in the event of failure;
c) Restoration means that the capabilities are in place to replace a failed system with a working one;
d) Where redundancy and restoration are not possible, repair processes are critical; and
e) It is acknowledged that redundant design is easier to achieve in the core or long-distance networks, where switches can provide mutual redundancy. Closer to the customer (for example at a local concentrator or multiplexer), fast restoration and repair become more critical.
f) Complex systems comprise of many layers including defences, a complete or catastrophic failure is a result of multiple failures of defence both technical, human, organisational, including policy, procedure, training etc. small, innocuous or latent vulnerabilities, may have built up over time to contribute to or exacerbate the failure. These vulnerabilities may constantly change over time, due to constant changes and improvements in the technologies and/or the systems concerned.
g) It should be recognised that redundant elements of a system do fail and or are taken out of service for planned maintenance, the system should be designed to operate to the specifications of the design during these dynamic operational activities.
h) Review or root cause analysis of catastrophic or complex failures will identify multiple contributions to the failure (isolation of a single root cause should not be possible), the constant dynamic of system operations should be recognised in any analysis of any failure. The opportunities presented when a ‘near miss’ occurs should be considered in that it is likely that the failure of many defensive layers may be identified[7,16], analysed and acted upon, before a similar future event may cause a catastrophic failure.

In particular, Communications Providers should:

i. Use reliable apparatus and systems (sourced from capable suppliers) designed to prevent or withstand the effects of extreme conditions, including the loss of public power supplies;

[15] Supply chain risk management:
https://www.cpni.gov.uk/supply-chain
https://www.ncsc.gov.uk/collection/supply-chain-security
https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns#section_7

[16] Lockheed Martin 4.5 Measure resilience:
https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf

ii. (Give particular attention to the security of 999/112 emergency and safety of life traffic, for example by using techniques such as priority routing, repeat attempts, alternative routing and trunk reservation, and by avoiding dependence on a single set of premises for dealing with emergency traffic;
iii. Have a recovery plan in place against the event that network failure occurs; and
iv. Consider the security of both traffic and signalling links.

Signalling routings should be engineered to avoid known problems caused by asymmetric and circular routings, which can occur where SS7 Signal Transfer Points (STPs) are used, or when IP BGP configurations are changed.

8.1.1.6 Software Failures

Where equipment is software controlled, the software should be designed to be 'non-stop' or to restart automatically. It should be designed to minimise the possibility of a software error propagating throughout the system or to other equipment and be secured against unintended external interference.

In order to avoid 'common mode' or cascade failures, consideration should be given to dual plane or dual meshed networks provided by different suppliers.

8.1.1.7 Electronic 'Interference'

a) Communications Providers should plan accordingly to mitigate these threats. Such threats include:
    i. electrical conditions – It is expected that Communications Providers will use apparatus at network interfaces that can withstand or prevent onward transmission of electrical signals or conditions that are outside normally expected operating values;
    ii. signalling – It is expected that Communications Providers will minimise the impact of inappropriate signalling messages which may cause mis-operation of the network or billing systems; and
    iii. traffic loads – It is expected that Communications Providers will apply network management controls to limit the impact and onward transmission of excessive traffic volumes, but no more than is reasonably required to maximise the establishment of effective calls or timely data connections.
b) Communications Providers should consider what protection may be necessary on metallic circuits from accidentally applied voltages, current surges associated with earth potential differences and lightning strikes.[17]
c) Terminal equipment (TE) may cause a safety hazard by presenting an excessive voltage to the network. The presentation of high voltage to the network termination is clearly only applicable to fixed networks and should only occur after serious TE failure. The threat this presents to the network should be limited to the local loop, as the network should be self-protecting to prevent more extensive damage and reduce the risk to network maintenance staff.
d) Communications Providers should be aware that TE may under certain circumstances inject incorrect signalling information. Conducted or radiated emissions including those from TE may affect fixed networks. They should penetrate no further than the local loop, albeit possibly affecting adjacent circuits.
e) Communications Providers should also be aware that under certain circumstances, service-affecting problems can be caused by ingress into the telecommunications

[17] https://www.ena-eng.org:
EREC S36 Issue 2 Identification and recording of 'hot' sites - joint procedure for Electricity Industry and Communications Network Providers

system of radio signals. The use of mitigating measures (e.g. filters) may be useful to resolve such problems.

8.1.1.8 Inappropriate use of Signalling Protocols

a) Communications Providers should comply with any relevant technical networking standards, incorrect signals received from outside can interfere with the correct operation of the network. Such signals might be benign in intent and be caused by accidental miss-operation of other equipment. However, they may also be caused by deliberate attempts to interfere with the network, for example to avoid the proper charging for network services (phone fraud), to deny service to others, or to corrupt stored data or software. Multiple levels of security may be needed to counter such threats, including signalling 'policing', firewalls, etc. including liaison with relevant information exchanges

b) TE may under certain circumstances inject incorrect signalling information. The network should be self-protecting and ignore incorrect signalling from TE which does not conform to the expected protocols. Nonetheless, such signals may interfere with or mask legitimate information. Correctly formatted but erroneous signalling may be more dangerous to the network, for example malfunctioning automatic dialling equipment congesting the network with unwanted calls.

c) Communications Providers are encouraged to implement Calling Line Identity (CLI) in accordance with relevant Codes of Practice to assist, with tracing the source of interfering signals and fraudulent or malicious calls.

d) Communications Providers should consider appropriate measures to ensure that their networks can be protected from signalling problems in an interconnected network. Screening (also known as policing) is a technique that can be used, if appropriate, at the edge of the network to protect it from mis-operation of connected networks. Candidate areas for screening that Communications Providers should consider as necessary might be:

    i. Interconnect screening or monitoring – there are good grounds for providing screening of an interconnect link so that only agreed use of the interconnect is allowed, monitoring of protocols such as SS7 or BGP to ensure anomalous traffic or requests are detected and managed appropriately

    ii. Policing is also used to reduce the incidence of false 112/999 calls to Emergency Organisations. Communications Providers should ensure that genuine emergency calls are not rejected by this policing.

e) Access screening may be inherent in the protocol conversion done in the traditional telephone network by the local exchange, but with more transparent IP networks, specific access screening measures may be needed.

8.1.1.9 Terminal Equipment

Instances have been given above where TE may pose a threat to network integrity. Physical disconnection of fixed line TE can protect the integrity of the network from risks posed by TE.

8.1.1.10 Excessive Network Loading

a) Networks need to be protected from overload conditions. Overloads may be caused by excessive loads caused by media, disaster, live streaming, software updates or games releases.

b) Network traffic management (NTM) is a set of tools and techniques for detecting, monitoring and controlling network traffic to protect the network from abnormal loads, while at the same time optimising network performance. While NTM is capable of dealing with mass calling behaviour, it is recognised that complete service denial or disconnection may be required to control excessive traffic from (or to) a single customer.

c) Communications Providers should adhere to the following NTM principles in protection of essential service:
   i. Maximise the number of trunks filled with effective calls (i.e. calls which can be carried to their destination), rather than non-effective calls (i.e. calls which encounter congestion and cannot be carried to their destination);
   ii. (Give priority to single link calls, rather than calls going via alternative routes. During overload, more calls attempt to go by alternative multi-route links, which greatly increases the possibility of these calls blocking other call attempts. All or a portion of alternative route traffic can be blocked;
   iii. During abnormal overload conditions, use any temporary idle capacity in the network to reroute traffic;
   iv. Prevent switching congestion caused by large traffic or data volumes, to prevent the spread of congestion to connected systems; and
   v. Give priority to terminating traffic over origination of new traffic or data flows.

d) Communications Providers should give effect to these principles by:
Protective controls that remove traffic from the network as close as possible to its origins during overload, such as ‘call gapping’; and
Communications Providers should have:
   i. An NTM centre to provide real time surveillance of the access and transport network and to implement traffic controls;
   ii. Arrangements in place with their customers for the notification of planned mass calling events e.g. TV show phone-ins;
   iii. Arrangements in place to inform interconnected Communications Providers of planned and detected mass calling events;
   iv. Knowledge of national holidays and festivals (e.g. Christmas Day, New Year’s Eve);
   v. Knowledge of holidays and festivals in distant countries to which they operate direct links; and
   vi. An awareness of, in real time, news reports that may stimulate traffic (e.g. natural disasters).

e) It is accepted that in some cases, Communications Providers with small networks consisting of only one or two switches may choose not to invest in NTM facilities but instead rely on controlling their interconnect with other networks that do provide NTM.

f) Network caching of common media feeds may mitigate the impacts of live streaming of events etc.

g) It is recognized that congestion can be created in one network, and have an impact on a competitor's network due to network interconnection. If steps are taken in the affected network to reduce the impact of excessive load, typically by network controls, it is conceivable that another Communications Provider may have cause to complain that its ability to carry revenue-earning traffic is restricted. Conversely if no action is taken the affected network could fail. It is important for Communications Providers to understand that good network traffic management actually maximises the effective (i.e. revenue-generating) call capacity of the network. It is therefore expected that:

   i. All Communications Providers will document what congestion protection measures will be used (for example: call gapping, alternative routing and priority techniques) and in what circumstances. Any such documentation should be made available to other Communications Providers with a legitimate interest;

ii. (All Communications Providers will also document what measures will be used to ensure the priority of 999/112 traffic, particularly during congestion periods; and

iii. Interconnects, transit or peering connections will be dimensioned to avoid congestion

8.1.2 All IP

8.1.2.1 Resilience Issues for IP networks

a) IP based networks (and some other data systems) present an increased level of threat from electronic interference because there is no physical separation of the communications paths and signalling paths as there is in traditional telephone networks with common channel signalling.

b) Traditional IP networks exhibit significant levels of inherent resilience, but nevertheless like any network can have single points of failure, particularly at the edge. The resilience of IP networks is also traditionally dependent on the whole resource of the public Internet, much of which may be outside the management control of a given Communications Provider. Changes in routing patterns to reflect available resources can take a considerable time to stabilise (convergence time) and this can be detrimental to services requiring very high levels of availability. Communications Providers should therefore plan their resilience measures to provide managed domains under their own control with predictable and rapid configuration arrangements. IP reconfiguration can be avoided, in part, by utilising the restoration capabilities of any underlying transport layer, whether traditional SDH/ATM or Optical Switching, but steps should be taken to prevent 'races' between the different restoration arrangements.

c) Although IP networks can work with random interconnectivity, resilience is assisted by providing a defined hierarchical architecture to the network, as between, for example, edge, metro and core nodes. Similar links within the hierarchy should use similar bandwidths, or the value of restoration routings will be diminished. 'Short cuts' across the hierarchy should be avoided. By creating network routings which are inherently predictable, Communications Providers can avoid the need for complex modelling of network behaviour.

d) Core managed domains benefit from the use of Interior Gateway Protocols with link state routing protocols such as IS-IS and OSPF. Load sharing across multiple equal cost paths should be used wherever possible. Link costings and metrics should be designed so that routers lower in the hierarchy are never used to tandem traffic between routers higher in the hierarchy.

e) Border gateways not only separate internal and external routing domains, but can provide important firewall capabilities. Deep packet inspection can be used to provide more detailed screening of anomalous signals which should be monitored and investigated

f) Aside from its other advantages, Multi-Protocol Label Switching (MPLS) can aid resilience by separating traffic of different levels of importance and providing highly predictable network routings.

g) Communications Providers should take full account of advice and warnings promulgated by the government's Computer Emergency Response Team (CERT) now part of the National Cyber Security Centre NCSC.[18]

[18] NCSC:
https://www.ncsc.gov.uk

h) Communications Providers should take full account of guidance on the deployment and management of Border Gateway Protocol, used in the Internet.[19]
   i. Communications Providers should take appropriate precautions to guard against and respond to hacking and electronic attack. Communications Providers are encouraged to make use of appropriate industry fora to co-operate on these issues, in particular the CPNI and NCSC Security Information Exchanges.[20]
   ii. Expansive controls that re-route traffic from overloaded routes or failures to other parts of networks that are under-loaded with traffic because of different busy hours, such as 'alternative routing'.

i) Communications Providers should ensure a technical congestion control processes are in place to enable graceful control of overload or congestion events[21].

j) This is also relevant to the control of session-based connections in IP networks, such as telephony. However, there are a number of differences with Legacy networks including:
   i. To a degree, the TCP/IP protocol has an inbuilt ability to pace connections according to the load on the system;
   ii. Unlike Legacy networks, IP networks can carry many classes of traffic, with different holding times and arrival behaviours (often fractal in character);
   iii. Different Qualities of Service can be defined for different classes of service, so pre-emption is a possible technique to manage excessive loads, with delay tolerant services giving way to 'real-time' services.

8.1.3 IMT2020 (5G & Full Fibre)

Guidelines for considering Resilience issues within IMT2020 Networks are summarised below from requirements identified in:

- Network Functions Virtualisation (NFV) Resiliency Requirements[22]
- Resilience of NFV MANO Critical Capabilities[23]

8.1.3.1 Resilience Principles in NFV Environments:

The same level of Service Availability will be required in virtualised deployment scenarios as in traditional node deployment. The following sections identify the basic principles recommended as guidelines for building a resilient NFV system:

- Prerequisites
- Trade-Offs
- Enablers
- System Behaviours

a) Prerequisites
   i. The transition from purpose-built hardware to virtualised network creates new failures modes which can impact the quality of delivered service. Appropriate

[19] BGP guidance:
https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk
https://doi.org/10.6028/NIST.SP.800-189

[20] Information sharing:
https://www.ncsc.gov.uk/cisp

[21] NCSC Secure design principles:
Make disruption difficult - NCSC.GOV.UK

[22] ETSI - gs_NFV-REL001 - Network Functions Virtualisation (NFV) Resiliency Requirements (2015):
https://www.etsi.org/deliver/etsi_gs/NFV-REL/001_099/001/01.01.01_60/gs_NFV-REL001v010101p.pdf

[23] ETSI - gs_NFV-REL007 - Resilience of NFV MANO Critical Capabilities (2017):
https://www.etsi.org/deliver/etsi_gs/nfv-ifa/001_099/007/03.01.01_60/gs_nfv-ifa007v030101p.pdf

challenge models should be developed so that potential adverse events and conditions during system operation can be detected and remediated.

   ii. The resiliency of services is dependent on the reliability of the underlying NFV-I; expressed as mean time to failure (MTTF), mean time to repair (MTTR). The resiliency mechanisms used to maintain availability of the Virtualised Network Functions (VNF) should use protection schemes such as (active-active, active-standby) and support failure recovery strategies such as state re-creation.
   iii. NFV-MANO needs to be highly reliable to support automatic NFV operation, e.g. rapid service creation, dynamic adaptation to load, or overload prevention.
   iv. Failures of any NFV-MANO component should be isolated within this component and should not impact any operational VNF.
   v. The NFV-MANO components should support mechanisms to recreate any failed component along with its original state prior to failure; this includes support for recovery from total component failure.
   vi. The VNFM, as a dynamic extension to the NFV-MANO subsystem, needs to be re-started after a failure and then start its state re-creation mechanism without impacting the VNF operation.
   vii. Network resiliency requirements for Services should be established using dependability metrics such as expected Service Availability and Reliability (e.g. defects per million based on anomalies such as dropped calls, etc.).

b) Trade-Offs
   i. Service Availability is a function of the infrastructure availability and can be impacted by long error detection latencies and remediation times. The placement of VNFs in a configuration should be optimised so that there is a balance between the number of components involved (to minimize detection and remediation time) and the ability to maintain the independence of resources (to avoid simultaneous failures).
   ii. For most VNFs state management is a critical contributor to their resiliency and session-state management is a key design issue. Virtualisation provides the ability to design services with distributed or centralized data repositories, and access latency and consistency of the state data will affect the how it is stored the methods used to achieve service resiliency.

c) Enablers
   i. Resiliency of network functions deployed on NFV-infrastructure is increased as new or more resources can be rapidly requested from the infrastructure.
   ii. The ability to rapidly increase of the number of active service instances on demand can be used to mitigate unusually high service demands.
   iii. VNFs can be distributed across multiple NFVI-PoPs to increase spatial diversity or distributed across multiple cloud providers to increase operational diversity.

d) System Behaviours
   i. NFV-MANO should be used to determine VM state and load. NFV-MANO functions include overload control, load balancing, optimal placement of resources, and provides the ability to assign traffic to under-utilized VMs or create new VMs to minimize dropping of traffic.

8.1.3.2 Resilience principles in Multi-Access Edge Computing (MEC)

As more critical assets are moved out to the edge of the network, then the physical, personnel security and resilience of these assets should be assessed, as the assurance and protection that was offered in core sites may not now be sufficient to adequately protect these assets, the following should be considered:

- Power resilience

- Access control and security monitoring
- Environmental conditions
- Support of assets at the edge and associated risks

8.1.3.3 Service Availability

NFV can enhance Service Availability by dynamically assigning available resources to a more demanded service or flexibly adjusting limited resources from one service to another:

a) The NFV-I and NFV-MANO shall support multiple levels of service availability.
b) Within each service availability level, the NFVI and NFV-MANO shall support multiple grades of service depending on the service (voice, video, web-browsing, etc.)
c) The NFVI and NFV-MANO shall support options for including various service types and possible grades within a service availability level depending on the SLA between a service provider and customer.
d) It shall be possible to continue to provide the service with reduced or limited capability under abnormal network conditions.
e) Under failure or excessive load conditions, it shall be possible to support migrating or scaling out the VNFs onsite (on the same or different VNF infrastructure) or on a separate VNF infrastructure at a different site.

8.1.3.4 Fault Management

The NFV Resiliency Requirements[23] introduces a concept of the fault → error → failure chain which applies for any system, sub-system or service instance in the context of NFV, and can be any component of the NFVI, the VNF, or the NFV-MANO system.

A resilient NFV system is defined by a set of mechanisms that reduce the probability of a fault leading to a failure (fault-tolerance) and reduce the impact of an adverse event on service delivery.

The required mechanisms are identified by developing and analysing challenge models and consist of passive and active components:

- Passive mechanisms are primarily structural and include redundancy and diversity
- Active mechanisms consist of self-protection mechanisms operating in the system that defend against challenges

Within the NFV Resiliency Requirements[23], Resiliency in the event of a challenge is identified as an aspect of Quality of Service (QoS) and characterized as the combination of reliability and availability:

- where reliability is the measure of a service continuing to function satisfactorily once it has started;
- and availability is the measure of a service being available when a user requests it, i.e. if the quality is degraded beyond a certain level, the service becomes unavailable.

8.1.3.5 Failure Prevention

Organisations should have a robust problem management and root cause analysis process to ensure lessons are identified from ‘near misses’ or actual failure and that lessons are organisationally learnt as an outcome of this process, in addition organisations should take up opportunities to participate in information exchanges, to enable sharing of threat awareness and learning opportunities from other participants.

Failure prevention in NFV identifies measures for avoiding:

- errors during the system planning, design and implementation phases; and
- failures once the system is operational.

Failure prevention during system planning, design and implementation phases includes the use of the appropriate design margins, affinity and anti-affinity design rules (to circumvent single point of failure) and quality assurance measures, such as software quality control and testing.

Failure prevention during the operational phase requires monitoring the system load and its health, predicting when a failure may occur, and taking appropriate operational measures to prevent its occurrence.

a) Failure Containment
   i. Dedicated resources (e.g. CPU core, memory, disk storage and IO) should be assigned to a VM for containment of VM failures.
   ii. Flexible resource allocation mechanisms should be implemented to enable the VIM to set policies to ensure failure isolation under a variety of configurations and workloads.
   iii. Shared resource policies should define the maximum and minimum amount of resources for each VM to help containment of a VM.
   iv. Segregation or segmentation may reduce the risk of cascade type failures and enhance the capability of containing any compromise within the segregated asset (reducing the “blast radius[24]” of compromised assets).
   v. Micro-segmentation (isolation of workloads) should be policy based.
   vi. For VM’s and containers, the purpose, sensitivity and threat posture of data assets should be assessed and consideration as to whether to host on the same [operating system and] host kernel to simplify in-life management, there should be logical separation of all instances that have sensitive data, when containerized, the management of containers should be automated where possible.
   vii. The possibility of attacks from other VM’s within the network should be considered, hypervisor security may mitigate some of these risks, encryption may reduce the risks of physical access to the hardware.

b) Failure Prediction
   i. Real-time resource usage (disk usage, CPU Load, memory usage, network IO and virtual IO usage loss rate, available vCPUs, virtual memory) should be provided to VIM at configurable intervals.
   ii. Failure prediction should include trend identification and analysis collected data on resource usage (e.g. memory, file descriptors, sockets, database connections) to predict resource exhaustion.
   iii. A VNF and the supporting infrastructure should have their own self-diagnostic functionality in order to provide their health information to the VIM.

c) Overload Prevention
   i. Elastic resource management (scale up / scale out) in a cloud environment is a powerful feature for dynamically scaling services according to demands. However, elastic resource management should not be used as a replacement for traditional overload control mechanisms for highly dynamic Telco traffic.
   ii. Planned CPU headroom in virtualised environments should be monitored as customer usage grows

[24] Further discussion on managing the blast radius: https://www.atlanticcouncil.org/wp-content/uploads/2021/03/BROKEN-TRUST.pdf

   iii. The overload control in VNF should be implemented in a virtual environment even though elastic resource management could be applied for capacity scaling. The load in guest OS might not the unique parameter for indicating VNF load situation because the performance and load in the hypervisor can have an impact on the VNF performance as well.

d) Single Point of Failure Prevention
   i. Single points of failure should be avoided at any level, e.g. inside VNF, between VNF, VM, hypervisor, virtual and physical IO, networking, etc. Multiple VNFCs provided with the same functionality should be deployed in different VMs and located in different hypervisors and different geographic areas.
   ii. VMs that host the VNFCs implementing the same functionality should be deployed following anti-affinity policies to prevent a single point of failure.
   iii. Additional optimisation should be considered when making decisions on geographical distribution, with consideration for factors such as state synchronization, legal constraints, etc.
   iv. The implementation of redundancy for considerations of service continuity is a typical method for preventing a single point of failures in current systems. In the virtualisation environment, those methods could be applied for providing high availability service for supporting different resiliency classes of NFV services.
   v. VNFs with the same functionality should be deployed in independent NFVI fault domains to prevent a single point of failure for the VNF. In order to support disaster recovery for a certain critical functionality, the NFVI resources needed by the VNF should be located in different geographic locations; therefore, the implementation of NFV should allow a geographically redundant deployment.
   vi. The transport network including the virtual network should provide alternative paths for accessing the same VNF instance to prevent a single point of failure.

8.1.3.6 Failure Detection and Remediation

When a Network Function is executed in a virtualised environment, mechanisms for reliability and availability used in the non-virtualised environment may still be applicable. Two important aspects of the migration to a virtualised environment should be considered:

- availability gained by running two server instances in a load sharing cluster can only be preserved if the virtualisation layer runs the two virtualised instances on two unique underlying host server instances (i.e. anti-affinity).
- the NFV-I adds new functional layers which will have an impact on VNF reliability and availability as they contain new failure modes.

a) Hardware Failure Detection
   i. Hardware failure detection is the responsibility of the Hypervisor.
   ii. The Hypervisor shall report all failures detected to the VIM for subsequent processing, decision making, and/or logging purposes.
   iii. NFV-MANO functions shall monitor the resources provided to a VNF and shall, in case of a failure in NFVI, take the necessary actions to ensure the continuation of the affected service. The availability requirements stated by the VNF in the VNFD shall be taken into account.
   iv. VNFD policies shall be supported to enable a VNF to register a request for specific hardware failure notifications from the NFV-MANO[23].

b) Fault Correlation
   i. In the presence of one or more failures in a system, these failures should be identified first locally at each layer and then across subsystems.
   ii. Fault correlation processing shall be kept distributed as much as possible and avoid propagating large number of failure notifications to a centralized entity by sending locally correlated reports only, to avoid bottlenecks in the system.
   iii. The fault correlation function should classify and categorize failure reports in the system, e.g. according to global severity.
   iv. Correlated failure reports should be communicated via a standard failure reporting mechanism to other layers within the system and/or to external correlation engine.

c) VNF Failure Detection & Remediation
   i. The NVFI layer shall provide indication of hardware and environmental events to the VIM for the purposes of VIM proactively migrating VNFs away from the faulty hardware.
   ii. NFV-MANO shall take corrective action in the event a failure is reported from the NFVI layer, including actions such as:
      - VNF migration for VNFs that provide support for live migration.
      - VNF capacity reduction in the event that switching capacity has been diminished.
      - Removing a failed hardware entity from service and identifying it as unavailable.

8.1.3.7 Deployment and Engineering Guidelines

Resiliency considerations in NFV move from physical network nodes that are highly available to highly available end-to-end services, comprised of virtualised Network Functions running on an abstracted pool of hardware resources. Ensuring end-to-end Service Availability is the responsibility of the underlying infrastructure; i.e. the Network Function Virtualisation Infrastructure (NFV-I),

a) NFV-I should provide support for a range of HA mechanisms, such as redundancy, heartbeats, data synchronization, clustering and periodic snapshots or lock-step shadow copies to provide stateful service recovery.

b) Various types of redundancy methods can be used to provide high availability:
   i. k:n cluster redundancy: configure a cluster of n+k instances for handling the traffic that is shared among instances per pre-configured algorithms, for a planned capacity of n instances (and the k instances provide standby redundancy).
   ii. Active-standby: instances can be configured for lock-step mirroring for lossless transition (hot standby); or periodic snap-shots to restore service to a previous point in time with some loss in state information (warm standby) or to be started after a failure is detected in the active instance (cold standby).

c) Restoration
   Virtualised Network Functions (VNFs) typically form a sequence in a Service Chain where the links between them are referred to as a VNF Forwarding Graph (VNF FG). A failure recovery process scenario can be described as follows:
   - A failed VNF in a Service Chain is detected by appropriate failure detection methods.
   - A redundant standby VNF is identified. This can be either located on-site or at a remote location.

- The VNF FG is reconfigured by replacing the failed VNF with the redundant standby VNF.
- After the challenge or threat is over, the VNF FG may need to be reconfigured back to original status, particularly for the cases where the standby VNFs are located in remote NFV-I Nodes. The VNF FG is reconfigured by instantiating a new VNF at the original site which then replaces the redundant VNF.

d) Network Operator policy for the number of redundant standby VNFs will depend on the type and criticality of the VNFs in question; e.g. highly critical VNFs supporting Level 1 or Level 2 type services and customers may be set at 1+1 levels of on-site redundancy.

e) Redundant standby VNFs shall not reside on the same servers as the operational VNFs; they should be instantiated on different servers as ensured using anti-affinity rules.

f) For any VNF of a VNF-FG, a redundant standby VNF instance should be pre-identified such that the VNFs in the VNF-FG can be reconfigured by replacing the failed VNF with the standby.

g) Depending on the type of VNF, it may be necessary to reconfigure the Service Chain back to its original state prior to the failure. This process should be carried out without interruptions in service

h) Disaster Recovery
Network Operators should develop Disaster Recovery requirements and NFV-MANO should contain Disaster Recovery policies such that:

    i. Regional disaster recovery sites are designated that have sufficient VNF resources and comply with any special regulations including geographical location.
    ii. Prioritized lists of VNFs that are considered vital and need to be replaced as swiftly as possible are defined. These critical VNFs need to be instantiated and placed in the required standby mode in the designated disaster recovery sites.
    iii. Processes to activate and prepare the appropriate disaster recovery site to "takeover" the impacted NFVI-PoP VNFs; including:
        - bringing the set of critical VNFs on-line,
        - instantiation/activation of additional standby redundant VNFs,
        - restoration of data and reconfiguration of associated service
    iv. The designated disaster recovery sites should have the latest state information on each of the NFVI-PoP locations in the regional area conveyed to them on a regular basis.
    v. Appropriate information related to all VNFs at the failed NFVI-PoP should be conveyed to the designated disaster recovery site at the specified frequency intervals.

8.2 Operate

8.2.1 Network Management Systems

(embracing operations, administration and maintenance) allow the remote control and surveillance of communications networks.

Network management plays a vital role in maintaining resilience by providing data on events and alarms in the network, allowing the Communications Provider to take corrective actions as required.

The appropriate use of statistical data collection is an essential part of network management. Properly designed network management and procedures should mitigate losses due to internal and external events.

8.2.2 Operational Processes

Communications Providers should have effective operational processes in place, covering at least the following areas:

a) fault management;
b) planned works and planned maintenance;
c) configuration/change management;
d) performance management;
e) security management; and
f) traffic management.

8.2.3 Fault Management

For fault management to be effective, Communications Providers should have systems and processes for fault detection, fault monitoring, finding the cause of faults (Root Cause Analysis), bypassing faults to maintain network performance and fault fixing.

It is considered that:

a) Communications Providers should be fully informed about the status of its network at all times, including the status of the network itself and all related buildings and equipment on which the network is dependent;
b) Communications Providers should make use of information derived from customer-reported faults and complaints to identify network faults;
c) competent personnel, data and technical equipment should be available for fault management 24 hours a day;
d) there should be points of contact and escalation procedures to guarantee an equitable and timely response to faults;
e) a clear process should be in place for the systematic analysis of the causes of faults, for example: observation of symptoms, development of a hypothesis, testing of the hypothesis and the formation of conclusions;
f) Communications Providers should develop and operate a maintenance manual including agreed response times for different fault conditions as well as indicative restoration or repair times and procedures; and
g) Communications Providers should prioritise service restoration over clearance of faults not affecting service.
h) In the case of interconnected Communications Providers, it is expected that:
    i. any party becoming aware of an interconnect service fault will inform all other associated operators, and
    ii. in such an event, prompt action to resolve the fault should be taken by the party in whose system the fault has arisen.
    iii. The management of planned maintenance and faults between interconnected operators should be part of more general operations and maintenance (O&M) procedures between interconnected operators.

8.2.4 Notice Periods

Communications Providers should provide reasonable notice to the affected parties of any planned work (including maintenance) that carries significant risk of impairment to essential services . Except is when an emergency change is required to maintain the security or stability of the network.[25]

8.2.5 Change and Configuration Management

Good configuration/change management entails keeping a reliable inventory of network resources and having documented robust processes for the allocation of resources and management of changes that may pose significant risks to the continued delivery of services.

8.2.6 Performance Management

Effective performance management involves the use of data from the network management system and elsewhere to monitor network performance, to gauge performance against specified standards and to manage call carrying capacity to meet specified grades of service. On this point, reference should be made to other sections in these guidelines relating to traffic management .

8.2.7 Security Management

Effective security management in this context involves personnel, systems and processes that control access to both the network itself and the network management system and related assets. This includes user authentication, encryption, and access management processes. The security management regime should have a holistic approach across Physical, Personnel and Technological or Cyber realms.[26]

8.2.8 Risk Management

Effective risk management in this context involves assessing the design requirements of process, procedure, networks, systems and services, identifying any vulnerabilities or shortfalls assessing potential impacts and where appropriate designing mitigating controls to manage those risks where they have been assessed as posing a significant threat to continued operations.

Risk management is operated in the light of the necessary ambiguity of both organisational and regulatory environment, which when considered alongside timescale and resourcing challenges, are a part of any efficient, economic and agile service delivery. These challenges presented to operational teams needs to be considered.

Actions during day to day operations involve risk management in an environment that involves uncertainty which changes moment by moment, it should be noted that adverse decisions in hindsight often appear to be very clearly poor ones, however optimal decisions which are taken are often not fully appreciated or recognised.

8.2.9 Traffic Management

Real time traffic management involves the ability to gather data from various parts of the network to allow judgements to be made concerning real time call routing options. This may also include the gathering of data from signalling links, PSTN/Internet gateways and interconnect routes with other Communications Providers. A network management centre should not be a potential cause of catastrophic failure of the network. Communications Providers should consider the desirability of geographically separate network management centres, based on an analysis of costs, benefits and risks.

[25] Planned outage notification to customers ITU-T M1541:
https://www.itu.int/rec/T-REC-M.1541/en

[26] Security guidance:
https://www.cpni.gov.uk
https://ncsc.gov.uk

8.2.10 Testing

Communications Providers should have procedures for testing the network, including provocative testing of network components as appropriate. It is recognised that it is impossible to test something as complicated as a modern telecommunications network with complete certainty.

Therefore Communications Providers should be able to demonstrate that potential failure scenarios have been envisaged and that contingency plans for service restoration have been prepared tested and are in place. The objective of the contingency plan should be to maintain the Communications Provider's ability to fulfil, as a minimum its service obligations in the event of network failure .

8.3 Measure

Proposals describing a standardised method for Measuring the Resilience of Networks, Services and Applications are summarised from the following references:

- ENISA - Measurement Frameworks & Metrics for Resilient Networks & Services - Technical Report[27]
- RECODIS - Disaster-Resilient Communication Networks: Principles and Best Practices (2016)[28]

8.3.1 Measurement Framework

Resilience evaluation is more difficult than evaluating networks in terms of traditional security metrics, due to the need to evaluate the ability of the network to continue providing an acceptable level of service, while withstanding challenges.

RECODIS[28] proposes a framework for measuring network resilience by developing constructs of dependability and survivability.

Dependability measures, such as reliability (the probability that a system will remain operational for a specified period of time) and availability (the probability that a system is up at a particular point in time), as well as performability (measures of performance degradation), are used to characterize the resilience and survivability of communication networks.

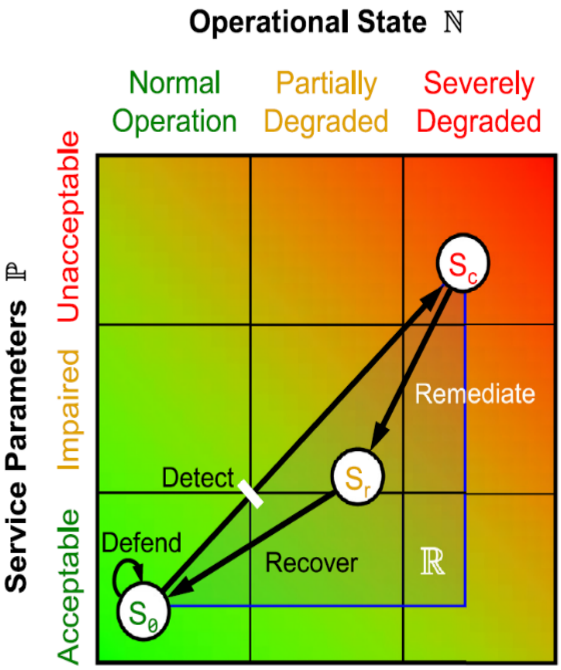
[27] ENISA - Measurement Frameworks & Metrics for Resilient Networks & Services - Technical Report: https://www.enisa.europa.eu/publications/metrics-tech-report/at_download/fullReport

[28] RECODIS - Disaster-Resilient Communication networks: Principles and Best Practices (2016): https://eprints.lancs.ac.uk/id/eprint/126743/1/Disaster_Resilient_Communication_Networks.pdf

8.3.2 Service Parameters & Operational State

RECODIS[28] also describes the ResiliNets initiative, which has proposed a model for resilience evaluation and measurement as shown in the figure.

The horizontal axis is the operational state of the network, ranging from normal operation (e.g. all links and components operational as designed) through partially degraded to severely degraded . As the network is challenged, the network state moves from S_θ to the right, and a resilient network infrastructure resists the degree of movement to the right.



For example, an overprovisioned richly connected network with diverse paths will remain operational under challenges that cause nodes and links to fail.

Network users, however, care about the service delivered rather than the state of the underlying infrastructure. This is captured by the vertical axis representing acceptable service (normal operations) through impaired service (usable, but poorly) to un- acceptable.

The D^2R^2 ResiliNets strategy (Defend, Detect, Remediate and Recover) is overlaid on the figure. The initial state of acceptable service under normal operations is S_θ. As long as resilience defences hold this will remain the case.

Monitoring of network operational state and service quality will detect when a challenge causes a transition toward impaired service or degraded operations; toward for example, S_C.

This transition triggers remediation mechanisms throughout the network, in all affected components and protocols to improve service and operations; toward for example, S_r.

When the challenge is repelled or ends, and the infrastructure is restored or replaced, the systems recovers to S_θ.

These resilience evaluation and measurement techniques as described in RECODIS have been incorporated into the resilience requirements specification for ETSI Network Functions Virtualisation[23] (NFV).

9 Business Continuity and Emergency Planning

It is not intended that these guidelines cover all aspects of Business Continuity and Emergency Planning.

The EC-RRG has developed a series of Best Practice statements in this area. These are appended at Annex A. Many of these are similar to statements within these guidelines, but cover more aspects of Business Continuity and Emergency Planning.

10 Conclusions

These guidelines should provide appropriate guidance for Communications Providers to decide how to establish and maintain appropriate levels of resilience in their networks consistent with being part of the CNI.

11 Annex A - Business Continuity and Emergency Planning

11.1 Industry Standards

ID	Industry Standard
UKBC 1-1	Network Operators and Service Providers should formally document their Business Continuity process. Key areas for consideration include: Process Description, Plan Scope, Assumptions, Dependencies, Responsibility, Risk Assessment, Business Impact Analysis, Prioritisation, Plan Testing, Training and Plan Maintenance.
UKBC 1-2	A successful Business Continuity Plan requires executive support and oversight. Network Operators and Service Providers should establish an executive steering committee (composed of executive managers and business process owners) to provide guidance and direction to the planning team.
UKBC 1-3	The Business Continuity Plan for Network Operators and Service Providers should address critical business processes (e.g., Call Completion, 999 Emergency Services, Provisioning, Maintenance, etc.), support functions (IT, Sourcing, Logistics, Buildings, etc.), Revenue Collection with the key business partners.
UKBC 1-4	The Business Continuity Plan for Network Operators and Service Providers should be formally reviewed on an annual basis to ensure that the plans are up-to-date, relevant to current objectives of the business and can be executed as written.
UKBC 1-5	The Business Continuity Plan for Service Providers and Network Operators should include a Business Impact Analysis (BIA) of the loss of critical operational support systems and/or applications and a Risk Assessment of potential loss due to man-made and natural disasters.
UKBC 1-6	During Incidents which result in the invoking of the Business Continuity Plan, Service Providers and Network Operators should establish a designated Emergency Operations Centre. This centre should contain tools for coordination of service restoration including UPS, alternate means of communications, maps, and documented procedures to manage business interruptions and/or disasters.
UKBC 1-7	Service Providers and Network Operators should establish a geographically diverse back-up Emergency Operations Centre. The diverse centre must have no dependency on the main designated Emergency Operations Centre, and the two centres must have no risks which could simultaneously affect both centres.
UKBC 1-8	Incident coordination and control in the emergency operations centre and at the incident site should be achieved through mirroring the three-tier Incident Command System used by the Emergency Services in the UK.
UKBC 1-9	Service Providers and Network Operators should regularly exercise their Disaster Recovery Plans. Exercise scenarios should include natural (e.g. flooding, fire) and man-made (e.g., nuclear, biological, and chemical) disasters.
UKBC 1-10	Service Providers and Network Operators should designate personnel to be responsible for producing and maintaining the Disaster Recovery Plans.
UKBC 1-11	Service Providers and Network Operators should make use of multiple alternative communication devices, systems and service providers for use by their critical people during emergencies.

ID	Industry Standard
UKBC 1-12	Service Providers and Network Operators should develop company specific protective measures that correlate with the threat levels identified by the UK Security Services.
UKBC 1-13	Service Providers and Network Operators should review their insurance requirements in order to maintain Business Continuity in the event of massive property damage or loss, incapacitation of senior officers, and other interruptive situations.
UKBC 1-14	Service Providers and Network Operators should conduct risk and threat analysis at critical network sites.
UKBC 1-15	Diagrams and drawings of network sites should be included in Business Continuity plan documentation. Drawings should be kept up to date as network changes occur.
UKBC 1-16	Service Providers and Network Operators should develop processes or plans to quickly account for all employees in or near the impact area of a disaster.
UKBC 1-17	Service Providers and Network Operators should have documented plans or processes to assess the damage to network elements, external plant, building infrastructure, etc. for implementation immediately following a disaster.
UKBC 1-18	Service Providers and Network Operators should always emphasise employee and public safety during all phases of recovery from an incident or disaster.
UKBC 1-19	Service Providers and Network Operators should maintain their participation in The UK Telecommunications Industry Emergency Planning Forum (EC-RRG) which includes advisory sessions, exercises, and training. They should review existing and proposed best practices and consider implementation.
UKBC 1-20	Service Providers and Network Operators establish liaison points with the relevant authorities (for example, Lead government department via EC-RRG or Local resilience forum's), such that in the event of a CBRNE related incident, response may be appropriately co-ordinated and trained responders engaged by those agencies may support any required installation/repair or related activity.
UKBC 1-21	Service Providers and Network Operators should provide disaster recovery contact information to the Industry Regulator for inclusion in the UK Plan for the Telecommunications Sector, and update this contact information as changes occur or at the request of the Regulator.
UKBC 1-22	Service Providers and Network Operators should implement development of a vital records program to protect those records that may be critical to restoration efforts
UKBC 1-23	Service Providers and Network Operators should identify key individuals within their organisations that are critical to disaster recovery efforts. Planning should consider maximizing the availability of these individuals.
UKBC 1-24	Service Providers and Network Operators should develop disaster recovery plans that consider simultaneous Industrial Action during a period of disaster recovery.
UKBC 1-25	Service Providers and Network Operators should consider creating a threat and risk assessment team to quickly determine appropriate actions both pro-active or re-active to address potential or real threats
UKBC 1-26	Service Providers and Network Operators should create a remote system access strategy for use during disaster recovery.
UKBC 1-27	Exchange buildings should be equipped with on-site UPS systems and emergency power generation capability to provide an ongoing power

ID	Industry Standard
	supply in the event that commercial power is interrupted in order to ensure continuity of services. Periodic maintenance routines of the batteries and power generators including, but not limited to engine runs should be performed to assure stand-by power reliability.
UKBC 1-28	Service Providers and Network Operators should run preventative maintenance programs for network site support systems including emergency generators, UPS, DC plant, HV, and fire suppression systems
UKBC 1-29	Service Providers and Network Operators should ensure that an adequate number of portable power generators are available consistent with the size of the company's network operation and with due regard to the regularity of mains power failure.
UKBC 1-30	Service Providers and Network Operators should ensure adequate fuel, emergency maintenance and a defined re-supply plan are available for emergency power.
UKBC 1-31	Service Providers and Network Operators should enter into Mutual Aid agreements with partners best able to assist them in a disaster situation.
UKBC 1-32	The Business Continuity Plan for Service Providers and Network Operators should include a list of critical Equipment and third-party suppliers and business partners. In addition, it should contain an assessment of their ability to respond to a disaster and a review of individual contracts to determine what level of service is available during a disaster.
UKBC 1-33	Network Operators should develop a strategy for the deployment of emergency mobile assets such as switch equipment, transmission, cellular equipment, masts, microwave radio assets, Power Generators, for emergency deployment and service augmentation.
UKBC 1-34	Network Operators should ensure that all emergency mobile assets are maintained at the same level as the existing network infrastructure. Hardware and software maintenance should be assigned to designated technicians with the expectation that the emergency mobile assets will always have the most current hardware and software and be immediately available for deployment.
UKBC 1-35	Disaster Recovery exercises should include trial deployment of emergency mobile assets and should be conducted to train as many technicians and support personnel as possible in as realistic a manner as possible.
UKBC 1-36	Each Network Operator should determine in advance whether they will use line of sight systems (microwave radio, satellite communications systems etc.) to re-establish communications. If these technologies are to be deployed it is recommended that contingency designs be developed for each technology in advance, with personnel trained to install and optimize the systems. Lists of key personnel and telephone numbers for site access should be established to satisfy the ability to access this requirement.
UKBC 1-37	Service Providers and Network Operators should make use of disaster recovery management models with escalation procedures that provide a clear escalation path to executive levels both internally and externally.
UKBC 1-38	Service Providers and Network Operators should, during times of disaster, communicate the disaster response status frequently and consistently to all appropriate employees - so that they all understand what processes have been put in place to support customers and what priorities have been established in the response.

ID	Industry Standard
UKBC 1-39	Service Providers and Network Operators should verify that their Equipment Suppliers have escalation processes for support during disasters, including contacts with Logistics (who know what spare equipment is available in various depots, and how to ship it), Manufacturing (who may need to adjust the priority of what's being built and/or shipped) and Sales (who need to communicate their response plan and determine the customers' needs)
UKBC 1-40	Service Providers and Network Operators should have contact lists for the various specialist functions needed during disasters, so that equipment and skilled specialists can be deployed to disaster sites in the most significant cases.
UKBC 1-41	Service Provides and Network Operators should ensure their Equipment Suppliers provide a "Disaster Information Checklist", which will provide a set of questions which the Service Provider would address immediately after a disaster and then inform the Equipment Supplier to facilitate equipment delivery
UKBC 1-42	Service Providers and Network Operator should consider deploying advanced technologies to address critical needs when responding to disasters.
UKBC 1-43	Service Providers and Network Operators should ask their Equipment Suppliers, during their response to major disasters, to ensure that the escalation point within their organisation has a specific channel for dealing with requests relating to disaster events.
UKBC 1-44	Service Providers and Network Operators should ask their Equipment Suppliers to provide a "Disaster Recovery Services Checklist" giving a listing of all the Equipment Supplier's professional services which the Service Provider or Network Operator may require during an event.
UKBC 1-45	Service Providers and Network Operators should develop plans or processes so that resource needs, identified through damage and resource assessments, can be escalated up the company chain of command, with suppliers, or through mutual-aid partners
UKBC 1-46	Service Providers and Network Operators should consider, when/where feasible, maintaining sufficient hardware spares for critical elements to continue service after an incident without the need to obtain spares from Equipment Suppliers.
UKBC 1-47	Service Providers and Network Operators should develop processes to routinely archive system media backups and provide for storage in a "secure off-site" facility which would provide geographical diversity.
UKBC 1-48	Service Providers and Network Operators should consider supplementing media backup storage with full system restoration capability for media, services or systems with documented restoration procedures that can be tested and utilized at an alternate "hot site", in case of total failure of the primary service site.
UKBC 1-49	Service Providers and Network Operators should consider, where feasible, utilizing multiple communication carriers to provide diverse connectivity between service nodes reducing single points of failure.
UKBC 1-50	Service Providers should consider alternative carrier/transport methods such as satellite, microwave or wireless to further reduce point of failures or as "hot transport" backup facilities
UKBC 1-51	Service Providers and Network Operators should periodically test new and existing business critical systems for capability limitations to avoid impaired operation during disasters.

ID	Industry Standard
UKBC 1-52	Service Providers and Network Operators should engage in pre-construction site selection processes to ensure network sites are not built in locations at a high risk of natural or man-made hazards.
UKBC 1-53	Fire detection and suppression systems should be installed at all network sites.
UKBC 1-54	Service Providers should use applicable engineering and construction standards in the building of network facilities.
UKBC 1-55	In recovery situations network build standards should be such that they do not interfere with other infrastructure.
UKBC 1-56	Service Providers and Network Operators should ensure deployment of resilient communication systems to appropriate Disaster Recovery personnel.
UKBC 1-57	Service Providers and Network Operators should work collectively with local, regional and central government organisations and other utilities to develop processes for efficient communications and coordination, as required under the regulations and guidance arising from the Civil Contingencies Act 2004[29]
UKBC 1-58	Service Providers and Network Operators should work with government and other utilities in the development of any Emergency Communications Networks in order to provide a process for key utilities and government emergency responders to communicate during disaster events
UKBC 1-59	Service Providers and Network Operators should make information available to contractors and other bodies on cable routes, in order to minimise the likelihood of damage and cable cuts when excavation is undertaken.
UKBC 1-60	Service Providers and Network Operators should ensure that Service Level Agreements for repair are reviewed and the associated records and data bases are reconciled annually
UKBC 1-61	Service Providers and Network Operators should establish and maintain an interface with local, regional and central government agencies to ensure effective support is available upon request as part of disaster recovery.
UKBC 1-62	All Service Providers and Network Operators should introduce network controls on public networks in order to control congestion and ensure that emergency calls (999) receive proper priority during emergency situations.
UKBC 1-63	Service Providers and Network Operators should implement consistent network management controls between operators, in order to promote reliability of the interconnected network.
UKBC 1-64	Network Operators and Service Providers should identify and manage critical network elements and architecture that are essential for network connectivity and customer services. In each case, considering security, redundancy and diversity.
UKBC 1-65	In order to facilitate asset management and increase the likelihood of having usable spares in emergency restorations, Network Operators and Service Providers should maintain "hot spares" (circuit packs electronically plugged in and interfacing with any element management system, as opposed to being stored in a cabinet) for mission critical elements. To determine appropriateness of this standard, certain factors

[29] Emergency Preparedness: https://www.gov.uk/government/publications/emergency-preparedness

ID	Industry Standard
	should be considered, including redundancy, single points of failures for critical customers, etc.
UKBC 1-66	In preparation for predicted natural events, e.g., ice, snow, flood, hurricane, Service Providers and Network Operators should consider preparing and moving standby generating capacity and verifying the proper operation of all their subsystems.

12 Annex B – Resilience Design Principles

12.1 Design Principles

The following sections have been collated from References 10, 16, 23-24, 28, 31-34; to identify a common set of design principles applicable to resilience requirements within Legacy, All IP and 5G / Full Fibre Networks.

As identified by ENISA in - *'Enabling & Managing End-to-End Resilience*[9], The primary principle of resilient network design is to maximise availability by enabling :

- fault tolerance at the node level and
- redundancy at the topology level.

12.1.1 Situational Awareness

Whilst it is very important to maintain general situational awareness[30] of the environment that the system or service is operating in, it is also important to maintain contextual awareness of the specific system or service and particular threats that may be posed and the current security posture, the following should be considered to ensure the system or service does not impede this being monitored by the managing organisation and is considered in the design stage:

- The system or service or its components may well have been compromised from the outset (in the supply chain) or may be currently compromised without being detected.
- Understanding of the current attack surface[31] and security posture
- Current status of resources and their connectivity in real time
- Live tracking or forecast of natural events
- Live tracking of threat actors and their activities or adverse events (adversary oriented analysis) adversaries will also evolve to adapt to their operating environment.
- Dynamically produced and automatically managed threat data
- Visualisation of information to assist in rapid assimilation and comprehension
- Fusion of information to assist in holistic review and management and to support the development of a joint understanding of risk and the current situation (information

[30] Emergency planning college: https://www.epcresilience.com/EPC.Web/media/documents/Papers/Occ12-Paper.pdf

[31] Attack Surface: https://www.crestresearch.ac.uk/comment/cyber_security_attack_surface/

picture), both within the organisation and to facilitate this understanding with partners (transboundary information sharing)[32]

12.1.2 Separation: Layers & Domains

A hierarchical approach is critical for an operator of network infrastructure (design for defence in depth), as it significantly simplifies traffic management in the network, reduces the time needed to determine failures and the constrains the impact of an outage.

It is recommended in RECODIS[28] to use a hierarchical architecture composed of three layers to develop an End-to-End resilient network :

- backbone network (Core),
- distribution network (Metro),
- access network (Access).

This allows for functional division of the layers depending on the tasks they perform throughout the network. Each layer is composed of:

- passive components — premises for backbone nodes, together with the necessary infrastructure to ensure secure and reliable functioning of active components; cable and ducts; optical fibre cables; passive accessories for fibre optics radio links; and,
- active components — active devices that aggregate and transmit traffic from lower layers.

In All IP networks the network resiliency features should span Layer 2 and Layer 3 boundaries and should be deployed throughout the Core / Metro / Access hierarchy.

Very high network availability is achieved by controlling overall network failure rate through configuration of device-level redundancy to increase hardware Mean Time Between Failures (MTBF).

The use of Load sharing in high availability network design significantly reduces the cost of provisioning device level redundancy

The following should be considered:

- Multiple distinct authentication layers or challenges to validate identities at a session level
- Whitelisting to prevent un-approved or unvalidated builds, or access to assets
- Use privileged accounts, access, or function is minimised and used only for privileged use
- Fusion of intrusion detection systems across networks/layers and hosts
- Analysis of the assets within the layers or instances with a view of their criticality and sensitivity and how protection may be co-ordinated and consistent or uniform
- Protection of layers or instances commensurate to the criticality and sensitivity of the assets that are contained within those layers or assets
- Design that defines appropriate cryptographic and spatial separation (including security, management and non-security, non-management, live and development or lab functions)

[32] Understanding and decision making:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/584177/doctrine_uk_understanding_jdp_04.pdf
https://www.jesip.org.uk/uploads/resources/JESIP-Joint-Doctrine.pdf
https://www.crestresearch.ac.uk/comment/joint-decision-making-real-world-emergencies/
https://www.ncsc.gov.uk/collection/cyber-security-design-principles/establish-the-context-before-designing-a-system

- Organisational units supporting the service need to be defined to ensure training, exercising planning, guidance and oversight is maintained
- How both internal and external support may be facilitated during a crisis or emergency situation, when other telecommunication assets may have been compromised

As identified in RECODIS[28] - Multilevel resilience is provided by a combination of factors within the following contexts:

- Protocol layers - in which resilience at each layer provides a foundation for the next layer above, and
- Planes - data, control, and management.

As the complexity of networks increases with components being assigned to stratified layers, slices and domains, this may be used to isolate subnetworks or simplifying and automating where there are common function, where communication is required between entities, there will be requirement to protect the communications and the associations between the entities involved, it will be likely that cryptographic protection will be utilised.

Organisations should assess the likelihood that the algorithms used may become compromised or depreciated, due to technological developments, as a result the designs must consider how certificates can be revoked and replaced in a timely manner, efficiently and securely whilst bearing in mind these certificates may be used at many layers or slices of abstraction and provide redundant and diverse service options, which will require careful management should expiry be coincident or certificate revocation and renewal be required urgently. The design must clearly identify where certificates or cryptographic algorithms are used (particularly within the hardware, which may need hardware or firmware updates to replace or update the algorithms).

Consideration should be made when isolating instance and guest OS's to reduce the risk of side channel or timing attacks and the risks of escape out of the guest OS to compromise the hypervisor.

In this complex environment there are challenges in detecting and recognising complex and vague signals as situations unfold particularly with the tight coupling of systems and the entanglement of their related processes, this complexity needs to be considered when designing how the service will be monitored and managed.

12.1.3 Redundancy: Systems & Paths

12.1.3.1 Redundancy

RECODIS[28] refers to the replication of entities in the network, generally to provide fault tolerance. In the case that a fault is activated and results in an error, redundant components are able to operate and prevent a service failure.

Two forms of Redundancy are identified in RECODIS; spatial redundancy and temporal redundancy :

- Examples of Spatial redundancy are triple-modular redundant hardware and parallel links and network paths.
- Examples of temporal redundancy are repeated transmission of packets, periodic state synchronisation, and periodic information transfer.

The following should be considered:

- Backup or archive information should have protection and separation commensurate with criticality or the sensitivity of the information being stored (risk of compromise of the live system and how the risk of backups or archives being compromised may be mitigated)
- Requirements for backup or archives should be defined in policy and design, backups should be periodically verified by testing procedures for restoration from backup.[33]
- In the event of failure, the capability must be maintained for the VNF's to be migrated to another VM or hardware whilst maintaining its configurations.
- Surplus capacity should be maintained and managed, in order to mitigate the risk supply chain disruptions, loose coupling, such that elements depend on each other to the least extent practicable, (JIT deliveries of hardware or other services)
- Alternative security mechanisms in the event of failure or capacity restraints

12.1.3.2 Diversity
RECODIS[28] identifies Diversity as being closely related to redundancy, but also includes the key goal of avoiding fate sharing.

Diversity consists of providing redundant elements, nodes or paths from alternate suppliers, so that when a challenge impacts a particular component, the alternate elements, nodes or paths will avoid fate sharing and can prevent degradation from normal operations.

Diverse alternatives can either be simultaneously operational, in which case they defend (S_θ) against challenges, or they may be available for use as needed to remediate (S_r).

CP's should retain the ability to ascertain and trust where the geo[graphic] location of information assets are or may be located, both in normal and failure modes, to ensure compliance is assured to relevant legislation, regulation or contractual obligations

The following diversity options should be considered:

- Architectural diversity
  to minimise common mode failure – common vulnerabilities
- Design diversity
  this may increase complexity and cost
- Synthetic diversity
  e.g. randomisation of addressing to make analysis difficult
  this may increase complexity and cost
- Information diversity
  improve situational awareness
- Path diversity
  provide alternative routing, especially for internal C3 (Command, Control & Communications)
- Supply chain diversity
  different suppliers for critical components, ensuring sources are separate

[33] NCSC backup guidance: Action 1 Make regular backups:
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks#makeregularbackups
https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

12.1.4 Hardening and Protection

Ensuring the System and Service (and its supporting functions) has hardening or protection which is commensurate with its criticality and/or with its sensitivity, that this has been applied in a co-ordinated, consistent and effective manner, orchestration is important both in the configuration and reconfiguration of services, but in response, to avoid cascade failures or gaps in coverage of service or monitoring.

The network assets or components shall always be hardened to vendor guidelines

Exercising or red teaming should be used to validate protection and for training and awareness of the supporting organisations

Where possible the designs should be simplified and the attack surface reduced, this should enable more effective defence and monitoring.

12.1.5 Data & State: Replication, Synchronisation and Integrity

RECODIS[28] identifies that State management is an essential part of any large complex system, and is related to resilience in two ways:

- first, the choice of state management impacts the resilience of the network, and
- second, resilience mechanisms themselves require state and it is important that they achieve their goal in increasing overall resilience by the way in which they manage state.

The modes of failure of any large complex system are likely to be complex also and challenge the organisation(s) that operate and maintain it, significant near misses[16] and service failures should be analysed to determine root causes, including human factors, to ensure that the opportunity for organisational learning[34] is optimised. Complex technical interactions should be modelled particularly when challenges or perturbations of the environment are likely.

The ETSI NFV Resilience Requirements[22] state that for a high availability solution, failure detection, isolation and recovery should be automatic and reliable, and employ a range of high availability mechanisms, such as redundancy, heartbeats, data synchronization, clustering and periodic snapshots or lock-step shadow copies to provide stateful service recovery.

- "Stateless" service continuity typically applies to transaction services such as DNS. Each transaction is independent, but if the server goes down then the service is unavailable. In this case, it is sufficient to restore only the functionality (and the configuration) at the same or a different site.
  This type of protection mechanism provides stateless resiliency. If there is no state information to maintain (i.e. a stateless service) or if it is acceptable to initialize the service at the time of the failure (e.g. by expecting end-user's retry access), then the offered service is initialized after the failure recovery.
- "Stateful" service continuity typically applies to continuous services such as a voice call. In order to maintain on-going calls, all the session states in all of the involved functional nodes has to be maintained. In this case, it is not sufficient to restore only

[34] Organisational learning:
https://www.crestresearch.ac.uk/comment/power-decision-making-emergencies/

functionality and configuration, but all the latest session states also need to be restored.
This type of protection mechanism provides stateful resiliency, i.e. on-going E2E service sessions are maintained after the failure recovery with no or minimum interruption.

Provenance tracking, services shall always be validated and assured by ensuring the provenance of the build components, preferably by cryptographic techniques (hashes or digital signatures, or by supply chain risk management for other components), out of date or stale images/builds shall be removed from repositories to reduce the sprawl of images and the risk of human error.

Software images of an unknown provenance should never be loaded into an organisation's registry, to avoid poisoned images, software packages and all their dependencies should be loaded in their organisations registry to avoid dependency confusion and potential exploitation

The evolution of networks the applications and services support have resulted in an increasingly rapid change of entities where possible the update of these should be templated to build standards and automated to reduce the risk of human error and to enable rapid change.

In the disposition phase data protection and retention requirements should be considered to ensure that appropriate protection is maintained.

Acquire behavioural information for the system or service and validate the current live service to this baseline or emergent criteria

12.1.6 Load Sharing & Balancing

Load sharing and balancing includes a range of traffic management techniques used to ensure concurrent use of configurations that contain active / active elements such as redundant nodes and paths.

This can be used to support autonomic recovery from a challenge, in that protocols operating in a layer above the failed element are able to immediately effect re-direction of traffic onto the remaining active element in the event of a node or path failure.

Maintaining two (or more) active paths to support a traffic flow will create specific capacity planning and management requirements, and to maintain resilience the design must consider the ability to respond appropriately to excessive loads.

Excessive loads may be stimulated by updates or patches for example; where demand for resources may impact other services, then throttling or resource consumption controls should be considered. Critical services shall always be prioritised.

NFV-MANO[23] functions must have the capability to support capacity management per instance.

Service level agreements must identify where pre-emption of resources may impact provision of service. (in order to maintain priority services)

The following adaptive options should be considered:

- Dynamic reconfiguration
  responding to cyber events by dynamically changing configurations including organisation or personnel
- Dynamic resource allocation
  e.g. responding to cyber events by dynamically rerouting, changing organisation or personnel, pre-empting assets
- Adaptive management
  e.g. re-instantiation or resetting or redeployment of assets when anomalous behaviour is detected, reducing attack surface in the light of a potential threat

13 Annex C - Network Transformations

This section summarises some examples of Resilience best practice design principles that were employed by Industry as transformation from Legacy to All IP (Next Generation Networks) progressed.

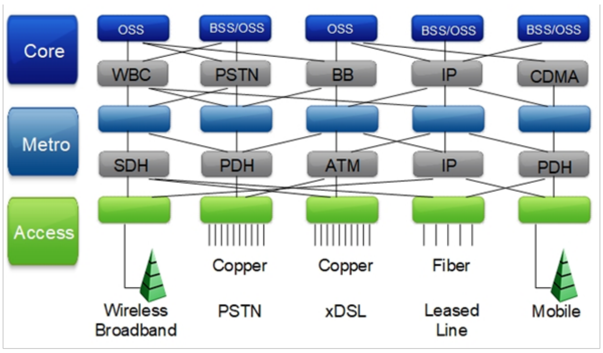
Although network transformation to All IP is due for competition in the UK by 2025, the Telecommunications Sector has already had to initiate further transformation activities such as Virtualisation, which not only meet current needs but provide the foundation for enabling the development of future services as defined by the ITU IMT-2020 and 3GPP 5G programmes.

A high-level description of the role virtualisation plays in enabling transformation to 5G is also provided, to re-enforce the need for detailed consideration of best practice resilience design principles as these deployments are progressed.

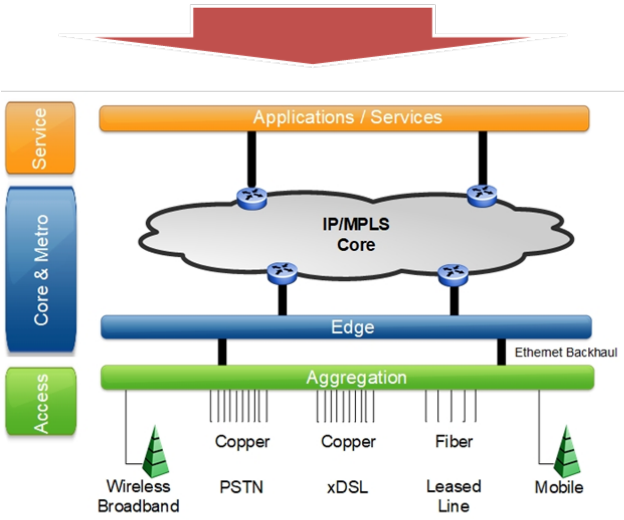
13.1 Legacy to All IP

The principal purpose of the transformation from Legacy to All IP Networks, was to remove the vertically integrated hardware and software silos that were required to provide individual services, and replace them with a horizontally layered; service agnostic, Single Network Transport Platform, on which all existing services such as the PSTN and Broadband could be provided as well as new services developed.

- Separate service-specific core networks
- Separate service-specific access nodes.
- Network Transport and Service intelligence are separated.



- Network Transport Layer is Agnostic to requirements of Application and Service Layers
- Single IP-based core network transports traffic between access points
- New Layer aggregates traffic from multiple access networks.



As a Single Network Platform, Next Generation Networks (NGN) were designed to support the following requirements for all Services :

NGN Requirements	Description
Quality of Service	Provide differentiated service to selected traffic, depending on the individual requirements of different types of service & meet SLA requirements. Support configuration of traffic paths to measure their performance to achieve latency, jitter, loss and throughput targets.
Availability & Resilience	Recover from network outages with multi-homing being supported where feasible. Support a convergence time of 50 msec or less to ensure continuity of a voice session that includes a path in the legacy PSTN.
Scalability	Scale effectively to support expansion or contraction of services and ensure Service, Control and Transport Layers continue to function as a single network.
Performance & Throughput	Sufficient bandwidth to be able to guarantee a committed level of performance for the full service portfolio of end users as well as future growth.
Congestion	Handle unpredictable surges in traffic using appropriate load and overload controls and prevent congestion collapse.
Control	Support mobility of users and devices utilising dynamic QoS Policy Decision and Enforcement
Interconnect	Support a Multi Service Interconnect between Operators through provision of standardised interfaces for Media, Signalling, Management, Overload Control, Numbering, Testing, Performance and Security.
Security	Guarantee the Confidentiality, Integrity and Availability of specific services.
Management	Provide management of the Network using a separate data communications network (DCN) to Support network control and provide visibility of network performance.

Additionally, NGN architecture typically made a distinction between "Network Infrastructure" and "Service Infrastructure“ in order to maintain the network layer as service agnostic.

Services were represented within the network only as a traffic mode or class, and the network infrastructure was engineered to support traffic classes with specific requirements in terms of availability, performance and security.

With the exception of Public Voice Service (PSTN) requirements for legacy signalling, network infrastructure was not designed to meet individual needs of specific services.

13.1.1 Network Infrastructure

Network Infrastructure contained all elements that made up the Core, Edge and Access Layer capabilities as well as those that provided Network Intelligence and Service Control

The Network Infrastructure contained data that had "internal significance" only and the characteristics of this data were described as "Static" - in that any form of change was subject to constraints and needs to be sequenced and controlled (specifically routing state within the Core and Edge Networks).

13.1.2 Service Infrastructure

Service Infrastructure was provided by elements that support Virtual Local Area Networks (VLANs) and Virtual Private Networks (VPNs) for services such as Broadband, IPTV, Corporate Layer 2/3 Networks.

Service Infrastructure contained data that had "external significance" only and the characteristics of this data were described as "Dynamic" - in that the data was visible to third parties (customers / external systems) and could be changed autonomously.

13.1.3 Layering and Abstraction

The isolation, layering and abstraction constructs described above were utilised by a Traffic Engineering capability in the Core, and were fundamental in terms of supporting the resilience of the Single Network Platform; and its ability to prioritise the availability of specific services, in the event of platform, system or network failures.

13.2 5G and Full Fibre (IMT-2020)

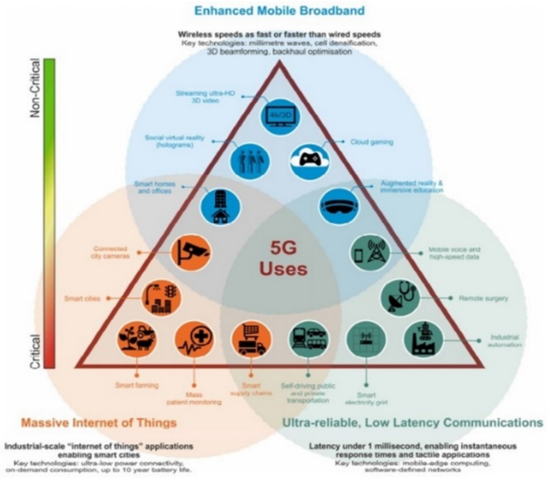
Over the last decade clearly identified trends have emerged within the Telecoms sector, which were recognised as exceeding the ability of next generation networks to support dynamic service creation in a cost-effective manner. These trends included:

- Explosive growth of data traffic;
- Massive increase in the number of interconnected devices;
- Continuous emergence of new services and application scenarios.

The main drivers behind the anticipated traffic growth included increased video usage, device proliferation and application uptake. Estimates within ITU-T Reports indicated that global traffic growth between 2020 to 2030 could be anywhere in the range of 10-100 times 2015 levels.

The ITU & 3GPP have classified the service categories that will drive this demand:

- Enhanced Mobile Broadband (Mobile Broadband, UHD / Hologram, High-mobility, Virtual Presence / Augmented Reality / Virtual Reality)
- Ultra-reliable Low Latency Communications (Industrial Automation, Drone / Robot / Vehicle Control, Medical / Emergency Applications)
- Massive Machine Type Communications (Smart Cities, eHealth, Wearables, Smart Supply Chains, Agriculture)

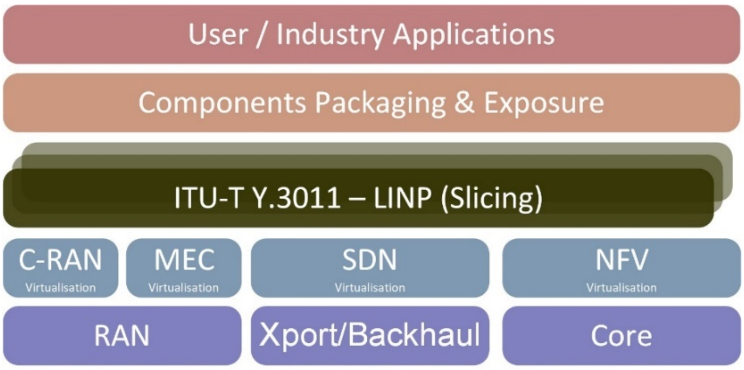

Enhanced Mobile Broadband
Wireless speeds as fast or faster than wired speeds
Key technologies: millimetre waves, cell densification, 3D beamforming, backhaul optimisation
Non-Critical
Critical
Streaming ultra-HD 3D video
4k/3D
Social virtual reality (holograms)
Cloud gaming
Smart homes and offices
Augmented reality & immersive education
Connected city cameras
5G Uses
Mobile voice and high-speed data
Smart cities
Remote surgery
Industrial automation
Smart farming
Mass patient monitoring
Smart supply chains
Self-driving public and private transportation
Smart electricity grid
Massive Internet of Things
Industrial-scale "internet of things" applications enabling smart cities
Key technologies: ultra-low power connectivity, on-demand consumption, up to 10 year battery life.
Ultra-reliable, Low Latency Communications
Latency under 1 millisecond, enabling instantaneous response times and tactile applications
Key technologies: mobile-edge computing, software-defined networks

It was determined by the ITU that the then current Industry approach to network and service architecture would not be able to scale to meet the demands being created by these future service categories. The approach adopted to address this issue was to extend the original IMT-2000 programme for 3G / 4G and develop requirements and solutions for Access & Core capabilities under the IMT-2020 (5G) programme.

IMT-2020 systems differentiate themselves from 4G systems not only through further evolution in radio performance but also through greatly increased scalability, delivered by an infrastructure engineered to provide 'deep programmability'.

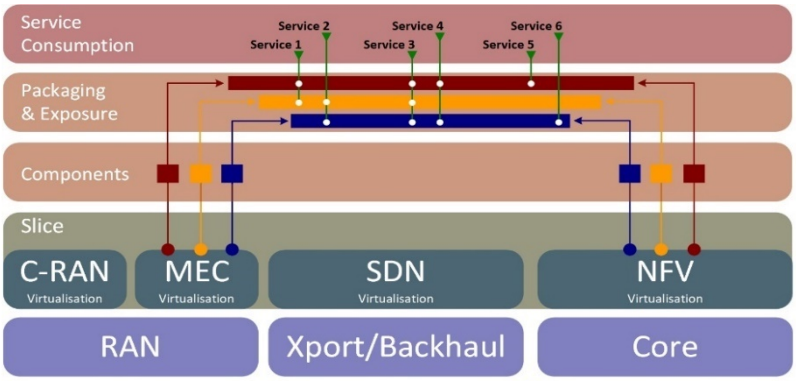
Deep programmability within IMT-2020 is driven by software. Network functions are run over Cloud Computing Infrastructure and at a number of points of presence; specifically, at the edge of the network in order to meet performance requirements. As a result, IMT-2020 is heavily dependent on technologies such as:

- Network Functions Virtualization (NFV),
- Software Defined Networking (SDN),
- Mobile Edge Computing (MEC), and
- Cloud RAN (C-RAN).



ITU-T SG13 – IMT2020

Further layers of abstraction are built on top of the Virtualisation Layer and are the means by which network services are instantiated as collections of software components; representing virtualised network functions, which are then orchestrated to either compose or support user applications.



IMT2020 – Service Composition

Programmability of the Infrastructure is the key enabler that delivers this capability and is controlled from a dedicated Management and Network Orchestration (MANO) domain.

14 Document Control

Doc History	Comment	Version	Date of Issue
Draft 1	For comment	v0.1	15 June 2005
Draft 2	Minor amendments	v0.1	25 July 2005
		v0.2	24 October 2005
Draft 3	Document renamed and relationship to regulation clarified. Further minor amendments for IP environment	v0.3	11 January 2006
	Removal of OFCOM Ownership comments	v0.3	12 January 2006
	TI-EPF Comments: Addition of Optical (Section 2.5) Explicit inclusion of Fixed and Mobile	v0.4	30 March 2006
	Change Title	v0.5	3 April 2006
	Add TI-EPF Logo	v0.6	24 April 2006
	Update for EC-RRG	v0.7	March 2008
Version 1	Update for EC-RRG. To be moved to Version 1.0	v0.8	TBC
Version 2	Updated spring 2018 and agreed by EC-RRG June Plenary 2018 updated August 2018 on	v2.0	30 August 2018 (Rob Willis DCMS)
Version 3	Introduction of resilience requirements for IMT2020 (Virtualisation, Software Defined Networking, 5G) and Full Fibre	v3.0	22 June 2021
	Document classification downgraded from OFFICIAL to PUBLIC	v3.1	20 August 2021

15 References

[1] UK Telecommunications Industry Emergency Plan:
There is a national industry wide emergency plan which is owned and managed by the EC-RRG.

[2] Telecommunications Resilience:
https://www.gov.uk/guidance/telecoms-resilience

[3] DCMS - Supply Chain Review:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf

[4] ENISA - 5G Networks Threat Landscape (Dec 2020):
https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/at_download/fullReport

[5] Providers of Publicly Available Telephone Services have obligations relating to Emergency Planning under Condition A4 of the Conditions of Entitlement. They also have obligations under the Civil Contingencies Act 2004 as Category 2 responders:
http://www.legislation.gov.uk/ukpga/2004/36/contents

[6] National Risk Register:
https://www.gov.uk/government/publications/national-risk-register-2020

[7] Managing Human Error & the Swiss Cheese model of accident causation (James Reason):
https://post.parliament.uk/research-briefings/post-pn-156/

[8] TEMPEST and Electromagnetic Security:
https://www.ncsc.gov.uk/scheme/tempest-and-electromagnetic-security

[9] ENISA - Enabling & Managing End-to-End Resilience:
https://www.enisa.europa.eu/publications/end-to-end-resilience/at_download/fullReport

[10] ENISA - 5G Networks Threat Landscape (Dec 2020):
https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/at_download/fullReport

[11] CPNI's protective security guidance:
https://www.cpni.gov.uk/building-0

[12] Preparing for and responding to energy emergencies:
https://www.gov.uk/guidance/preparing-for-and-responding-to-energy-emergencies

[13] Preparation and planning for emergencies: responsibilities of responder agencies and others:
https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-responsibilities-of-responder-agencies-and-others

[14] Emergency planning college (Bias):
https://www.epcresilience.com/EPC.Web/media/documents/Papers/Occ15-Paper-AUG-2016.pdf

[15] Supply Chain risk management:

https://www.cpni.gov.uk/supply-chain
https://www.ncsc.gov.uk/collection/supply-chain-security

[16] Lockheed Martin Measure resilience (4.5 near misses):
https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf

[17] Rise of Earth Potential at Electricity Stations:
https://www.ena-eng.org
EREC S36 Issue 2 Identification and recording of 'hot' sites - joint procedure for Electricity Industry and Communications Network Providers

[18] NCSC:
https://www.ncsc.gov.uk

[19] BGP guidance:
https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk
https://doi.org/10.6028/NIST.SP.800-189

[20] Information sharing:
https://www.ncsc.gov.uk/cisp

[21] NCSC Secure design principles:
https://www.ncsc.gov.uk/collection/cyber-security-design-principles/making-disruption-difficult

[22] Network Functions Virtualisation (NFV) Resiliency Requirements (2015)
ETSI - gs_NFV-REL001 - Network Functions Virtualisation (NFV) Resiliency Requirements (2015):
https://www.etsi.org/deliver/etsi_gs/NFV-REL/001_099/001/01.01.01_60/gs_NFV-REL001v010101p.pdf

[23] Resilience of NFV MANO Critical Capabilities (2017):
ETSI - gs_NFV-REL007 - Resilience of NFV MANO Critical Capabilities (2017)
https://www.etsi.org/deliver/etsi_gs/nfv-ifa/001_099/007/03.01.01_60/gs_nfv-ifa007v030101p.pdf

[24] Further discussion of managing the blast radius:
https://www.atlanticcouncil.org/wp-content/uploads/2021/03/BROKEN-TRUST.pdf

[25] Planned outage notification to customers ITU-T M.1541:
https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-M.1541-201101-I!!PDF-E&type=items

[26] Security guidance:
https://www.cpni.gov.uk
https://ncsc.gov.uk

[27] ENISA - Measurement Frameworks & Metrics for Resilient Networks & Services - Technical Report:
https://www.enisa.europa.eu/publications/metrics-tech-report/at_download/fullReport

[28] RECODIS - Disaster-Resilient Communication networks: Principles and Best Practices (2016):
https://eprints.lancs.ac.uk/id/eprint/126743/1/Disaster_Resilient_Communication_Networks.pdf

[29] Emergency Preparedness:
https://www.gov.uk/government/publications/emergency-preparedness

[30] Emergency planning college:
https://www.epcresilience.com/EPC.Web/media/documents/Papers/Occ12-Paper.pdf

[31] Attack Surface:
https://www.crestresearch.ac.uk/comment/cyber_security_attack_surface/

[32] Joint understanding of risk and decision making:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/584177/doctrine_uk_understanding_jdp_04.pdf
https://www.jesip.org.uk/uploads/resources/JESIP-Joint-Doctrine.pdf
https://www.crestresearch.ac.uk/comment/joint-decision-making-real-world-emergencies/
https://www.ncsc.gov.uk/collection/cyber-security-design-principles/establish-the-context-before-designing-a-system

[33] NCSC backup guidance: Action 1 Make regular backups:
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks#makeregularbackups
https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

[34] Organisational learning:
https://www.crestresearch.ac.uk/comment/power-decision-making-emergencies/