

RESISTO:

D2.4_TELECOMMUNICATION SYSTEM MODEL AND INTERFACES - FIRST



RESISTO

D2.4 – TELECOMMUNICATION SYSTEM MODEL AND INTERFACES -FIRST

Document Manager:	Mirjam FEHLING-KASCHEK	Fraunhofer	Editor
--------------------------	------------------------	------------	--------

Project Title:	RESilience enhancement and risk control platform for communication infraSTructure Operators
Project Acronym:	RESISTO
Contract Number:	786409
Project Coordinator:	LEONARDO
WP Leader:	BTC

Document ID N°:	RESISTO_D2.4_190524_01	Version:	1.0
Deliverable:	D2.4	Date:	24/05/2019
		Status:	APPROVED

Document classification	Public
--------------------------------	---------------

Approval Status	
Prepared by:	Mirjam FEHLING-KASCHEK (Fraunhofer)
Approved by: (WP Leader)	Zhan CUI (BTC)
Approved by: (Coordinator)	Bruno SACCOMANNO (LDO)
Security Approval (Security Advisory Board Leader)	Alberto BIANCHI (LDO)

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Mirjam Fehling-Kaschek, Jörg Finger, Katja Faist	Fraunhofer	Scientific Researchers
Giuseppe Celozzi, Cosimo Zotti	TEI	Contributor
Marius Iordache, Horia Gunica, Carmen Patrascu	ORO	IP Experts/PM
Cosimo Palazzo, Federico Colangelo, Marco Carli	RM3	Contributors
Maria Belesioti	OTE	Contributor
Zhan Cui	BTC	Contributor

DISTRIBUTION LIST

Name	Company / Organization	Role / Title
PMT	RESISTO CONSORTIUM	NA
Markus MULLER	EC DG REA	EC Programme Officer
General Public	NA	NA

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
0.1	10.10.2018	23-29	3.4	ORO's examples of realistic network designs
0.2	19.10.2018		all	Added contents EMI, RM3
0.3	25.10.2018		all	EMI implemented changes/comments from EMI, ORO, ALB
0.9	12.11.2018		All	Release for SAB review
1.0	24.05.2019		All	Final release

COPYRIGHT STATEMENT



© 2018-2021 This document and its content are the property of the RESISTO Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the RESISTO Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the RESISTO Partners. Each RESISTO Partner may use this document in conformity with the RESISTO Consortium Grant Agreement provisions.

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Program, under the Grant Agreement No 786409.

The views and opinions in this document are solely those of the authors and contributors, not those of the European Commission.

PROJECT CONTACT



LEONARDO
Via Puccini – Genova (GE) – 16154 – Italy
Tel.: +39 348 6505565
E-Mail: bruno.saccomanno@leonardocompany.com

RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

Communications play a fundamental role in the economic and social well-being of the citizens and on operations of most of the CIs. Thus they are a primary target for criminals having a multiplier effect on the power of attacks and providing enormous resonance and gains. Also extreme weather events and natural disasters represents a challenge due to their increase in frequency and intensity requiring smarter resilience of the Communication CIs, which are extremely vulnerable due to the ever-increasing complexity of the architecture also in light of the evolution towards 5G, the extensive use of programmable platforms and exponential growth of connected devices. The fact that most enterprises still manage physical and cyber security independently represents a further challenge. RESISTO platform is an innovative solution for Communication CIs holistic situation awareness and enhanced resilience (aligned with ECSO objectives). Based on an Integrated Risk and Resilience analysis management and improvement process availing all resilience cycle phases (prepare, prevent, detect, absorb, etc.) and technical resilience capabilities (sense, model, infer, act, adopt), RESISTO implements an innovative Decision Support System to protect communication infrastructures from combined cyber-physical threats exploiting the Software Defined Security model on a suite of state of the art cyber/physical security components (Blockchain, Machine Learning, IoT security, Airborne threat detection, holistic audio-video analytics) and services (Responsible Disclosure Framework) for detection and reaction in presence of attacks or natural disasters. Through RESISTO Communications Operators, will be able to implement a set of mitigation actions and countermeasures that significantly reduce the impact of negative events in terms of performance losses, social consequences, and cascading effects in particular by bouncing efficiently back to original and forward to operational states of operation.

EXECUTIVE SUMMARY

A holistic system model of the telecommunication infrastructures is required by the technical tools implemented into the RESISTO platform throughout the project. The goal is to provide such a model, which serves as starting point for the more refined implementations in following work packages and is constantly updated and improved based on the feedback of the refinements.

This deliverable summarizes the status of the model definition and implementation. To this end available modelling approaches have been reviewed and assessed regarding their usability for RESISTO. A realistic model implementation depends on information provided by the communication operators. Therefore, a collection of specific input gathered on the end users infrastructures is included in this deliverable. Finally, first details regarding the implementations are presented.

It should be noted, that the deliverable represents the current status of Task 2.3 at halving interval. The work is ongoing and final results will be presented in the deliverable at the end of this task.

CONTENTS

ABBREVIATIONS	9
1. INTRODUCTION.....	10
2. RISK AND RESILIENCE MANAGEMENT	11
3. ASSESSMENT OF MODELLING APPROACHES REGARDING THEIR USABILITY FOR RESISTO	13
3.1. Conceptual models	13
3.1.1. OSI model	14
3.1.2. SysML	15
3.2. Network/graph models.....	16
3.2.1. Topological models	16
3.2.2. Flow based models	16
3.2.3. Multi Agent Systems	17
3.3. Geospatial representations	17
4. ACQUISITION OF DETAILED MODEL SPECIFICATIONS.....	18
4.1. Network architectures.....	18
4.1.1. 4G/LTE mobile networks	18
4.1.2. Future network architecture (Ericsson View)	20
4.2. Input collected via other tasks	22
4.2.1. Information provided by guided interviews (Task 2.1)	22
4.2.2. Information provided by Excel template for threat list (Task 2.2)	23
4.3. Examples of realistic network representations.....	24
4.3.1. Network diagrams of Orange Romania's infrastructure	24
4.3.2. Short description of the OTE Network	33
4.3.3. Network diagrams of the BTC infrastructure	37
5. IMPLEMENTATION OF TOOLS.....	45
5.1. Network simulators.....	45
5.1.1. Key concepts	45
5.1.2. Software packages	46
5.1.3. Network traffic models	47
5.2. Mixed Holistic Reductionist – CISI Apro modelling approach	47
6. SUMMARY AND CONCLUSIONS.....	54
6.1. Next Steps	54
7. REFERENCES.....	56

ABBREVIATIONS

2G, 3G, 4G	Second, third and fourth generation of mobile phone systems
API	Application Programming Interface
B2B	Back-to-Back gateway
EU	European Union
GNS3	Graphical Network Simulator
GUI	Graphical User Interface
IOS	Internetwork Operating Systems (Cisco)
ISI	Inter System Interface
LTE	Long Term Evolution (= 4G)
OS	Operating System
PC	Personal Computer
QoS	Quality of Service
SDN	Software Defined Networking
TCP	Transmission Control Protocol
UE	User Equipment
VPN	Virtual Private Network
WP	Work Package

1. INTRODUCTION

The aim of WP2 is the refinement and specification of user expectations and requirements for the RESISTO platform. It was designed to collect the necessary inputs for the implementation of the tools and methods throughout the other work packages. The following tasks are included in WP2:

Task 2.1 Communication operators requirements refinement

Task 2.2 Cyber physical threat, hazard and disruption ranking ontology

Task 2.3 Holistic socio-technical communication infrastructure system modelling

Task 2.4 RESISTO reference architecture for long term preparation and short term disruptions

Task 2.5 Operational use cases and validation plan

This report summarizes the status and results of Task 2.3. The main goal of this task is to provide and maintain a socio-technical telecommunication model. The model is needed as input for all following technical work packages and should be updated and improved during their runtime: starting with the refinements of the tools in WP3-WP5, followed by the platform integration in WP6 and finally the operational validation scenarios in WP7-WP9.

The report is structured as follows:

Section 2 is a literature based summary of work relevant for the objectives of Task 2.3, in particular the resilience management.

Section 3 delivers a summary of modelling approaches relevant for the RESISTO project. The relevance and usability of distinct modelling techniques is assessed with respect to the input needed for the risk and resilience management.

Section 4 gathers specific input for the setup and implementation of the telecommunication model. To gain relevant and tailored information, direct input from the telecommunication partners involved in the project was requested.

Section 5 introduces implemented modelling and simulation tools that will be used for RESISTO.

Section 6 provides the conclusions of this report, including an outlook on the next steps.

2. RISK AND RESILIENCE MANAGEMENT

A detailed introduction into the risk and resilience management is given in [1]. Nine steps were defined to form an iterative resilience cycle, shown in Figure 1.

The modeling of the communication infrastructures can serve as input for several steps, in particular Step 2 and Steps 6 to 9. The most prominent parts where system modeling is necessary are highlighted in red [1].

(2) **System analysis**, comprising the ordered steps

- System (technical) environment and interface analysis
- System boundary definition (spatial, with respect to time, resolution, etc.)
- System interface identification, inter and intra system boundary definitions
- System dynamic behaviour assessment
- **(Top-level) System static and dynamic (graphical) modelling/ representation**

(6) **Overall resilience quantification**, comprising the ordered steps

- Selection of resilience quantities of interest, e.g. based on an assessment of system performance or non-performance functions
- Resilience quantification methods selection
- **System modelling sufficient for methods selected**
- **Application of system resilience quantification methods**
- Overall resilience quantification (taking account of all critical combinations and beyond if necessary)
- Determination of resilience level of system (non-)performance functions taking account of all identified disruptions
- Determination of other resilience assessment quantities needed for assessment, e.g.
 - Mean time till disruption
 - Vulnerability/ What-if-damage in case of disruptions
 - Time to bounce back (better)
 - Performance loss (area of resilience triangle)
 - Relative performance increase after recovery
- Aggregation and Visualization of resilience quantities

(7) **Resilience evaluation**, comprising the ordered steps

- **Resilience performance comparison (e.g. with historic quantities of system performance functions)**
- Illustration of effects of system performance loss
- Selection and application of decision making methods
- Evaluation of the acceptance of the obtained system resilience performance level and system resilience quantities for all identified threats: e.g. in terms of
 - acceptable,
 - improvement as high as reasonably practicable (AHRAP principle of resilience management),
 - not acceptable (must be modified)

(8) **Selection of options for improving resilience**, comprising the ordered steps

- Generation of overview up to inventory of resilience improvement options
- Selection and application of decision making methods for the selection of improvement measures
- Iterative re-execution of the resilience management steps for **assessing the resilience gain**
- Selection of improvement options

(9) **Development and implementation of options for improving resilience**, comprising the ordered steps

- Selection and application of domain-specific standards as far as possible
- Transformation of qualitative and quantitative resilience system performance function descriptions in (multi-) domain-specific traceable technical requirements
- Determination of the resilience levels for subsystems taking account of the system design
- **Design, development, integration and testing of system or system improvements using appropriate and efficient methods that correspond to the resilience level identified**

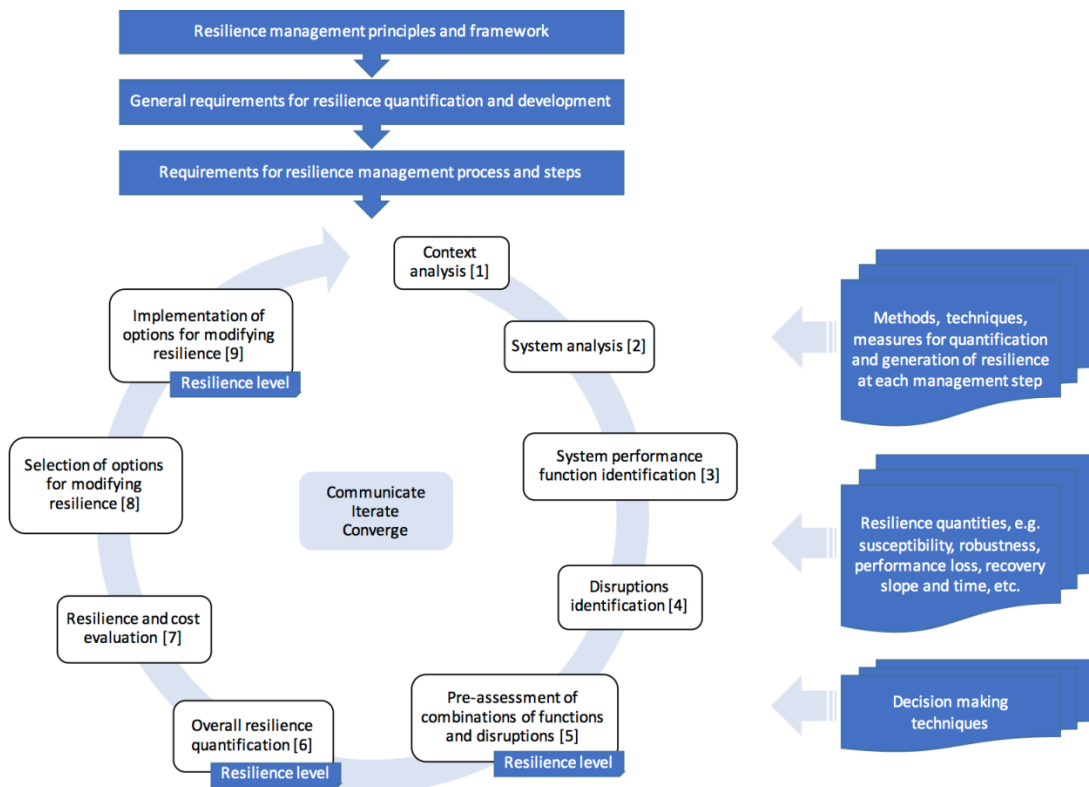


Figure 1 - Generic resilience management process that consists of 9 steps and covers resilience quantification and development [1].

3. ASSESSMENT OF MODELLING APPROACHES REGARDING THEIR USABILITY FOR RESISTO

The general aim of models is to gain a better understanding of the system of interest. This may include a rule based representation of the system to get a structural overview, a geospatial representation to allow for a user-friendly presentation of incidents and situations, or a mathematical model that allows to predict the behavior of the system for certain conditions and events, e.g. network simulations.

A main challenge for all modelling approaches, but in specific mathematical models, is to define how detailed the model should be. To quote G. Box, one of the founding fathers of data-driven mathematical modelling in dynamic systems: “All models are wrong but some are useful” [2]. It refers to the fact that models are by construction a simplification of the reality, neglecting information of the system that is not needed to gain the understanding addressed by the model. In summary, a useful model should identify/capture the main effects of the system allowing to deliver insights about the system. Depending on the system information requested, models of the same system may describe varying sets of elements at a different complexity level.

The usability for RESISTO is evaluated by considering the following two aspects:

- What are the aims of RESISTO, i.e. what tools are provided by the RESISTO platform and which models are needed by these tools? A special focus is set to address all phases of the resilience management process.
- Which models have been historically and scientifically used in the telecommunication sector? This relates to the question, if model specifications and schemes can be found in literature or are available from the end users of the RESISTO platform.

This approach leads to the preselection of the following modeling classes and concepts:

- **Conceptual models** to provide a general overview of the systems and input for Step 2 (*System analysis*) of the resilience management process (Section 3.1).
- **Network models** to provide a realistic model to simulate effects on telecommunication networks (Section 3.2). This can serve as a tool for the resilience quantification, as required by Step 6 (*Overall resilience quantification*), and the selection of improvement options, as required by Step 8 (*Selection of options for improving resilience*) of the resilience management process.
- **Geospatial representations** to provide an intuitive and user-friendly way to present results of the network models on the RESISTO platform (Section 3.3). The geospatial representations can be a useful extension of the network models for Step 6 and 8 and further help on the decision making process in Step 7 of the resilience management process.

3.1. Conceptual models

The aim of conceptual models is to gain a systematic/structured understanding of the system, following rules and standards to allow for a better comparability and easier exchange between different organizations.

Two concepts commonly used in the telecommunication domain are presented in the following: the OSI model, developed specifically for telecommunication and computer networks and the SysML modeling language, which more generally addresses the needs of system engineers in a wider context.

3.1.1. OSI model

The Open System Interconnection (OSI) model was developed in the late 1970s until mid-1980s by the International Organization for Standardization (ISO) and the International Telegraph and Telephone Consultative Committee (CCITT). Its revised version is available within the standard ISO/IEC 7498-1. Its goal is to define standard protocols to allow for the interoperability of communication systems, which are internally based on different methods and techniques.

The model consists of two main components: the reference model defining seven abstract hierarchical layers as shown in Figure 2 and the standardized protocols defining the interchange between different entities/instances within one layer.

The aim of RESISTO is to apply risk and resilience management to existing telecommunication infrastructures. These infrastructures already comply with standards allowing for interoperability between e.g. sub-networks or between operators. Therefore, no dedicated studies of the OSI model are performed in the context of the RESISTO project. Nevertheless, the model is referenced to throughout the project, e.g. in the context of threat classifications in D2.2.

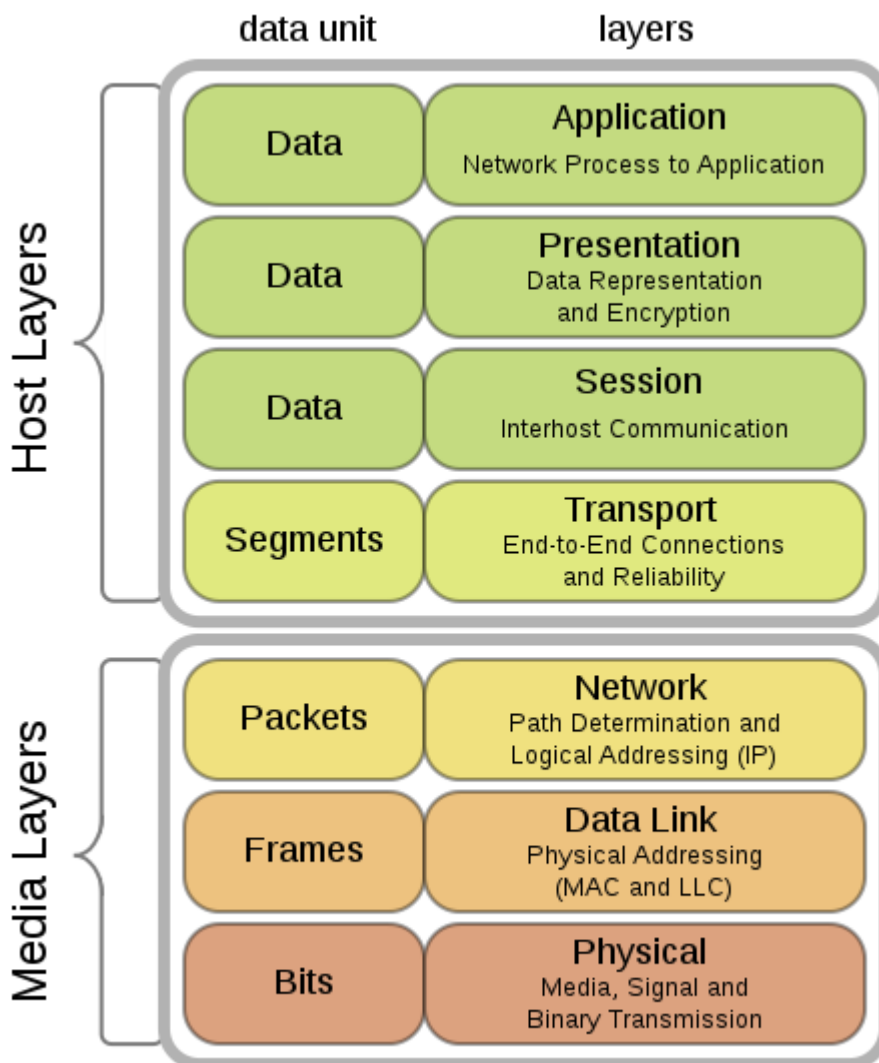


Figure 2 The seven layers defined in the OSI model (https://commons.wikimedia.org/wiki/File:OSI_Model_v1.svg - By Offnfopt [Public domain or CC0], from Wikimedia Commons)

3.1.2. SysML

The Systems Modeling Language (SysML) is aimed at system engineers as a general purpose modeling language supporting analysis, specification, design, verification and validation of complex systems. These systems may include different elements such as hardware, software, data, processes, personnel, and facilities. The main purpose of SysML is to specify and architect systems. The structure and the constituting components as well as the behavior of systems can be modelled. SysML is used in a broad range of industries including among others automotive, rail, aerospace, energy and telecommunication.

SysML is based on the Unified Modeling Language (UML) known from the field of software engineering, but it only uses a subset of UML which is relevant for system engineering. Additionally

SysML extends UML with language features which specifically support systems engineering tasks. Thus the semantics of SysML are more flexible and expressive.

With the requirements diagram a new diagram type is introduced to support requirements engineering. Likewise performance analysis and quantitative analysis is facilitated by parametric diagrams. In a concrete example like modelling a telecommunication system the benefits of SysML compared to UML become apparent. With requirement diagrams functional, performance and interface requirements can be captured and with performance diagrams performance and quantitative constraints like minimum throughput can be defined.

3.2. Network/graph models

The network structure of the telecommunication infrastructures directly implies the use of graph-theory based network models. A broader summary of modelling critical infrastructures, including also other modelling and simulation approaches, is provided in e.g. [3].

Profound introductions to graph theory is given in [4], [5] and of network science in [6], [7]. In this section, the main ideas and concepts important for telecommunication infrastructures are shortly summarized.

In general, a network consists of two kind of constituents:

- nodes representing the components of the system
- edges representing the connections of the nodes

The definition of both sets defines the topology of the network. Generally, two classes of network topologies are considered: physical topologies based on the actual physical construction of the network and logical topologies based on the data flow in the network regardless of the physical connections. A telecommunication infrastructure may consist of several sub-networks of both classes.

3.2.1. Topological models

The telecommunication infrastructure implies the use of topological models, where each node and each edge have a discrete state, which distinguishes in the most cases between failed and normal state [3]. In this model, a node can fail direct in consequence of a disruptive event (e.g. natural hazard, cyber-attack) or indirect as a consequence of a propagated fail, e.g. the source node fails and propagates that failure to its connected nodes.

Based on topological models, an infrastructure can be modelled more or less abstract, depending on what should be analyzed. The adaption of the abstraction level offers possibilities for performance and computation optimizations and thus for faster results. Furthermore, some parts of the network can be modelled more abstract than other ones. E.g. CIs interdependent to the telecommunication grid like the power grid can be modelled with a very high abstraction level and the consequences of failures to such infrastructures can be evaluated easily.

However, topological models cannot provide sufficient information for risk and resilience modelling. Therefore, a combination with some further modelling methods is necessary.

3.2.2. Flow based models

These models consider the flow delivered through the infrastructure. Using flow based models, each node and edge can produce, load and deliver flow [3]. Flow based models can be used as extension for topological models to consider any kind of flow in the network, e.g. electricity in power networks or services in telecommunication infrastructures. In addition, it is possible to model flow in interconnected networks, e.g. from telecommunication infrastructure to other CIs. [8] for example modelled interdependent CIs based on a network flow approach.

3.2.3. Multi Agent Systems

A multi agent system (MAS) is a self-organized system, which can solve difficult problems. In contrast, an agent based model (ABM) is used for evaluating if agents obey their rules in specific simulations or for evaluating the aggregated behavior resulting from individual decisions. This is used often in social science. In RESISTO, a MAS can be used for solving complex problems in the telecommunication infrastructure.

Agents in a MAS are components of a software or algorithm performing an action independently without any support from a central unit [9]. Each component or service in the telecommunication network can be modelled as autonomous acting agent for solving the complex problem of simulation and resilience computation. The problem is then solved by interaction between the concerned agents. After the computation, a result for the property of the whole system is given by the MAS. An advantage of MAS is the possibility of independent and parallel computing by the single agents, which can speed up the process of problem solving.

3.3. Geospatial representations

Representation by Digital Terrain Model (DTM), contour, satellite images.

We assume to overlap satellite images over a DTM to reproduce the territory.

- Applying a vertical exaggeration we can have a better visualization of natural obstacle.
- Operators will have simple understanding how to reach a given node (repeaters) in case of maintenance or inspection. They can estimate the effort to complete a single task depending on the local orography.
- Boundaries of the individual repeaters are represented as a function of distance and local orography.
- We can monitor the repeaters to visualize possible shaded areas due to service interruptions of one or more antennas and make analysis for possible place in which locate redundancy nodes.
- TBD integration with Onos to determine possible shaded area given by orography. Depending on morphological features, a failure of one single repeater could dramatically decrease the signal quality in the neighborhood. Distance couldn't be the primary value to be considered in case of repeaters failure.

To achieve these goal, we suggest to use an open source GIS (e.g. Qgis) that could be customized to the project.

- To represent the DTM, we will need *.xyz file or other ASCII file compatible with a GIS software.
- TBD which grade of precision will be required for the project.

4. ACQUISITION OF DETAILED MODEL SPECIFICATIONS

Aim of this chapter is the collection of specific input for the modelling of telecommunication infrastructures needed for a realistic model implementation. First, a more general introduction to current (4G/LTE) and future network architectures is given in Section 4.1. Feedback from the telecommunication operators was needed for other tasks in WP2, which is partially relevant for the construction of the modelling schemes. An overview on this source of information is given in Section 4.2. Finally, the operators were directly asked to contribute schemes of their infrastructures. These contributions are presented in Section 4.3.

4.1. Network architectures

4.1.1. 4G/LTE mobile networks

Mobile broadband is delivering broadband access wherever you go, and not just at home or in the office, and the majority of these are served by HSPA (High Speed Packet Access) and LTE (Long Term Evolution) networks. People can browse the Internet or send e-mails using HSPA-enabled notebooks, and send and receive video or music using 3G phones. With LTE, the user experience is improving even further supporting demanding applications like interactive TV, mobile video blogging, advanced games or professional services.

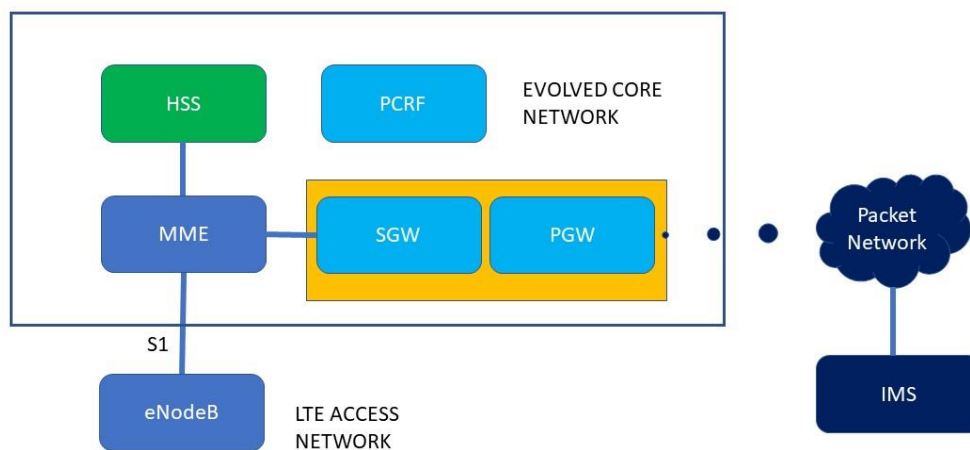
LTE enables operators to offer high performance, mass-market mobile broadband services, through a combination of high bit-rates and system throughput – in both the uplink and downlink – with low latency. LTE infrastructure is designed to be as simple as possible to deploy and operate, through flexible technology that can be deployed in a wide variety of frequency bands. LTE offers scalable bandwidths, from less than 5MHz up to 20MHz, together with support for both FDD (Frequency Division Duplex) paired and TDD (Time Division Duplex) unpaired spectrum. The LTE architecture reduces the number of nodes, supports flexible network configurations and provides a high level of service availability.

Security - Among the objectives of LTE is to provide equal or better security compared to previous generations. One such improvement is that LTE introduces very granular key separation. LTE mandates the use of different session keys for specific protocols and purposes between the terminal and the nodes in the network.

Performance and capacity – One of the requirements on LTE is to provide downlink peak rates of at least 100Mbit/s. The technology allows for speeds over 200Mbit/s and Ericsson has already demonstrated LTE peak rates of about 150Mbit/s. Furthermore, RAN (Radio Access Network) round-trip times shall be less than 10ms. In effect, this means that LTE – more than any other technology – already meets key 4G requirements.

Simplicity – First, LTE supports flexible carrier bandwidths, from below 5MHz up to 20MHz. LTE also supports both FDD and TDD. Ten paired and four unpaired spectrum bands have so far been identified by 3GPP for LTE. And there are more band to come. This means that an operator may introduce LTE in 'new' bands where it is easiest to deploy 10MHz or 20MHz carriers, and eventually deploy LTE in all bands. Second, LTE radio network products will have a number of features that simplify the building and management of next-generation networks. For example, features like plug-and-play, self-configuration and self-optimization will simplify and reduce the cost of network roll-out and management. Third, LTE will be deployed in parallel with simplified, IP-based core and transport networks that are easier to build, maintain and introduce services on.

Wide range of terminals – in addition to mobile phones, computers and consumer electronic devices, such as notebooks, ultra-portables, gaming devices and cameras, incorporate LTE embedded modules. Since LTE supports hand-over and roaming to existing mobile networks, all these devices can have ubiquitous mobile broadband coverage from day one. In summary, operators can introduce LTE flexibly to match their existing network, spectrum and business objectives for mobile broadband and multimedia services.



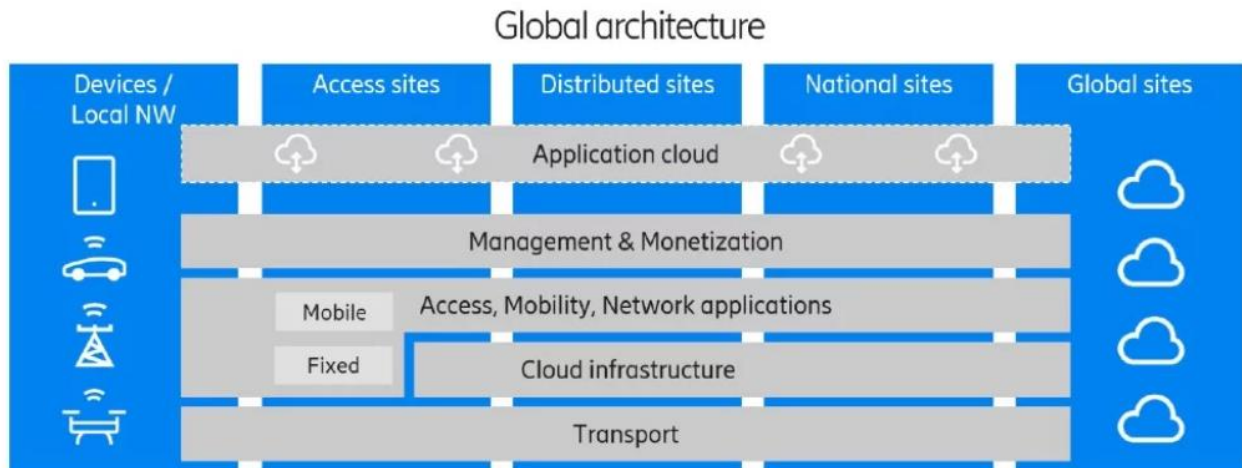
Architecture

In parallel with the LTE radio access, packet core networks evolved to the flat architecture designed to optimize network performance, improve cost-efficiency and facilitate the uptake of mass-market IPbased services. LTE architecture comprises: the LTE base station (eNodeB) and the MME, PGW and SGW. The LTE base stations are connected to the Core Network using the Core Network–RAN interface. This flat architecture reduces the number of involved nodes in the connections. Control signaling – for example, for mobility – is handled by the Mobility Management Entity (MME) node, separate from the Gateway. This facilitates optimized network deployments and enables fully flexible capacity scaling. The Home Subscriber Server (HSS) connects to the Packet Core through an interface based on Diameter, all interfaces in the architecture are IP interfaces.

LTE radio technology

LTE uses OFDM for the downlink – that is, from the base station to the terminal. OFDM meets the LTE requirement for spectrum flexibility and enables cost-efficient solutions for very wide carriers with high peak rates. It is a well-established technology, for example in standards such as IEEE 802.11a/b/g, 802.16, HIPERLAN2, DVB and DAB. OFDM uses a large number of narrow sub-carriers for multi-carrier transmission. The basic LTE downlink physical resource can be seen as a time-frequency grid where each resource element carries QPSK, 16QAM or 64QAM. Advanced antenna solutions incorporating multiple antennas meet mobile broadband network requirements for high peak data rates, extended coverage and high capacity, a family of antenna solutions is available for specific deployment scenarios. LTE can be used in both paired (FDD) and unpaired (TDD) spectrum.

4.1.2. Future network architecture (Ericsson View)



Horizontal domains:

- “Transport” contains functionality for transmission and transport primarily between sites but also within sites
- “Cloud infrastructure” contains functionality for secure processing and storage for both network functionality as well as applications
- “Access - Mobility - Network applications” contains functionality securing fixed and mobile access as well as network integrated applications
- “Management & Monetization” contains functionality to manage and control the network as well as running the business management of customers to the network
- “Application cloud” contains functionality supporting network external applications and is utilizing the Cloud infrastructure for execution and storage

Vertical domains:

- “Devices / Local networks” – The actual device used by a user or a network set-up by a user or enterprise outside the control of the service providers
- “Access sites” – Local sites which are as close as possible to the users
- “Distributed sites” – Sites which are distributed for reasons of execution or transport efficiency or for local breakout
- “National sites” – National sites which are typically centralized within a service providers’ network
- “Global sites” – Centralized sites which are publicly accessible from anywhere, typically a large data center

The future networks will utilize machine intelligence to become a fully autonomous network with closed loop control and policy governance for dynamic behavior. The automation loops will exist on all levels of the network, from the extremely fast radio loops where the analytical data gets old in

milliseconds to the cross-domain optimizations that predicts network traffic and load over long time periods. Predictive analytics will forecast the need and take measures automatically to move workloads or power up and scale out when needed.

The open, exposed and cloudified networks will also be more vulnerable than the closed systems of today. Opensource as well as the technologies and exposure of the network resources to multiple industries will open for attacks and there is a need for an even higher degree of security considerations. The componentization and horizontalization of network functions and infrastructure resources moves part of the security handling from product characteristics to deployment choices.

In the security area, the importance of analytics and machine intelligence will increase for both detection and automatic remedy of security incidents.

The future network architecture will be able to provide for different usage scenarios: high to low capacity, widespread to small area, very dense coverage to spotty coverage, indoor and outdoor etc. The end user requirements that they have to fulfill can be grouped in

- Enhanced Mobile Broadband (eMBB) – also called Evolved Mobile Broadband;
- Massive Machine Type Communications (mMTC)
- Ultra-Reliable and Low Latency Communications (URLLC) – also called Critical MTC.

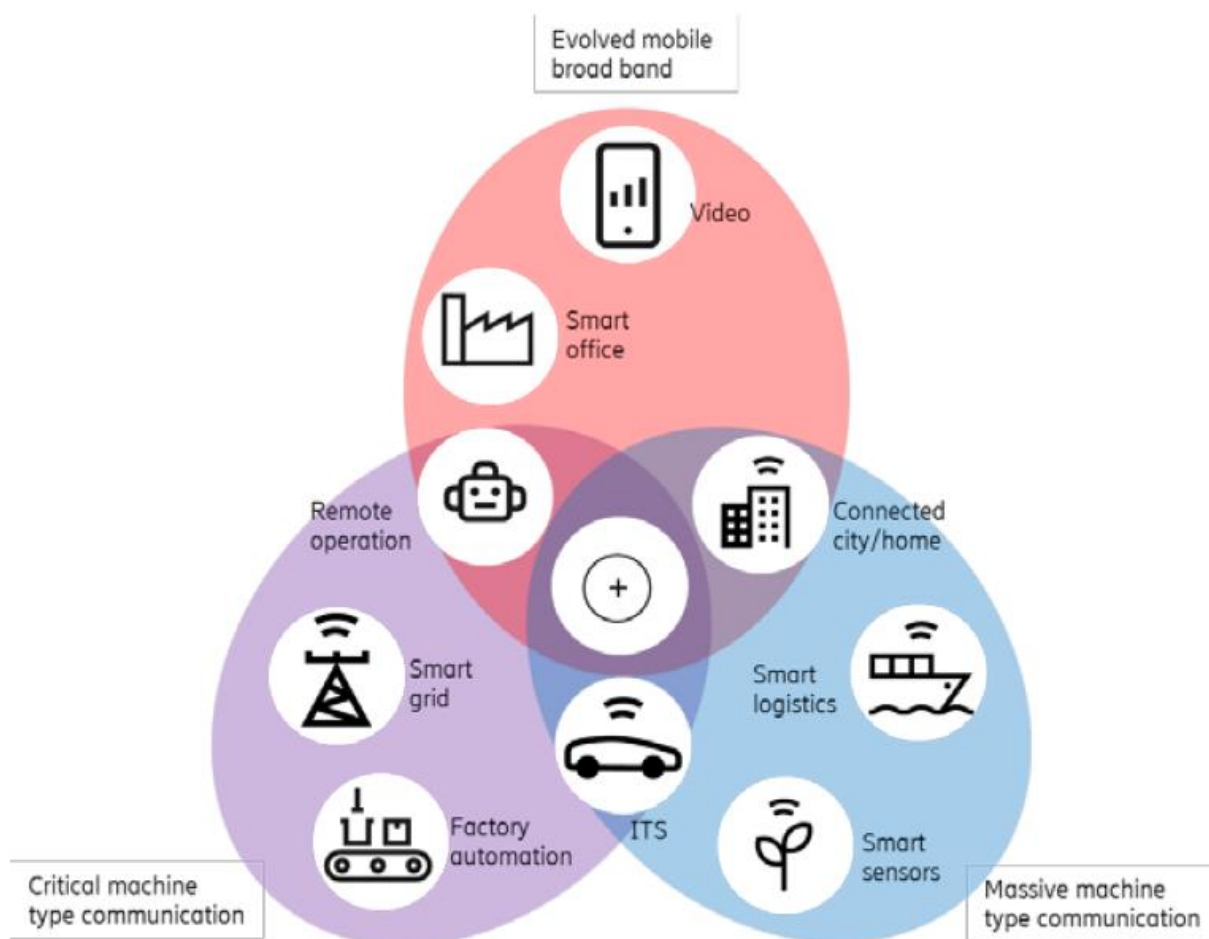


Figure 3: Future network requirements

Based on the principles shown above the 5G architecture can be defined as service-based and the interaction between network functions is represented in two ways. Network functions within the 5GC Control Plane shall only use service-based interfaces for their interactions.

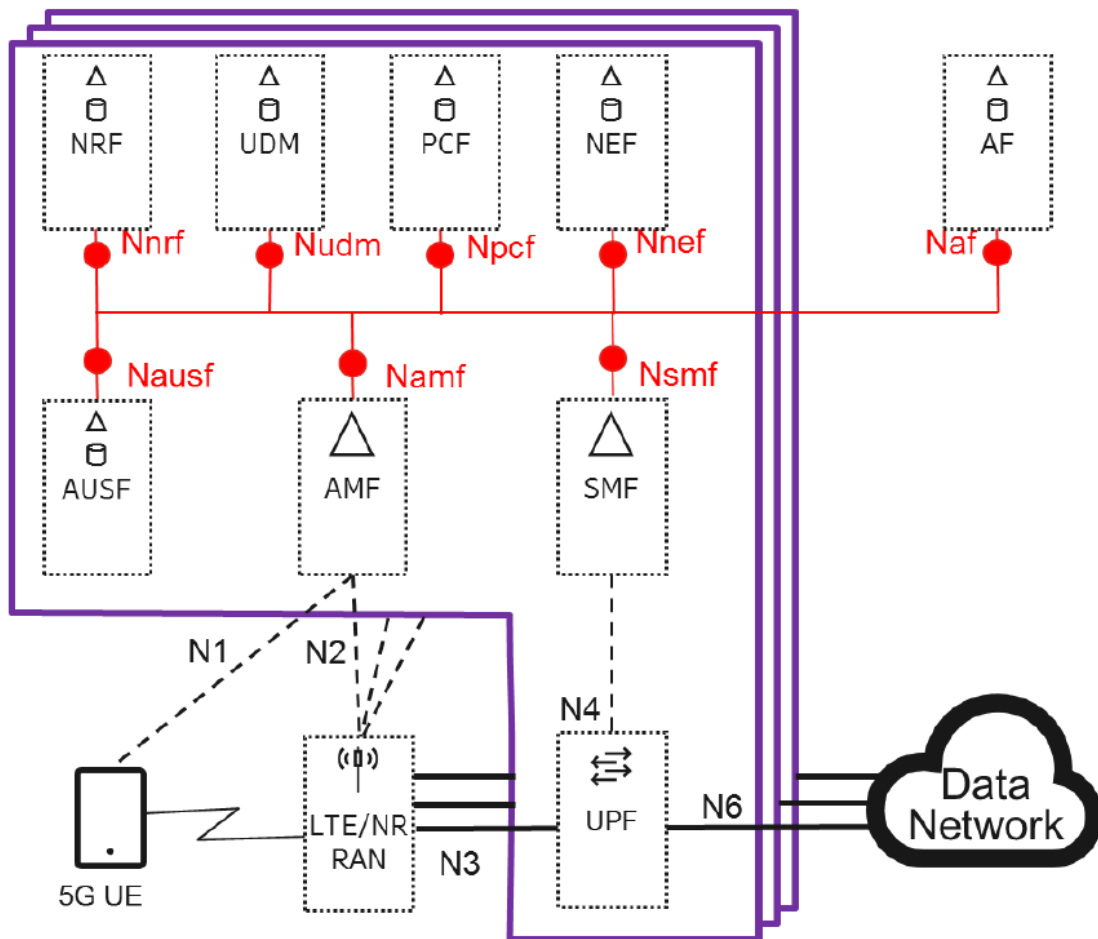


Figure 4: 5G Core architecture

4.2. Input collected via other tasks

Input from the telecommunication operators is gathered in Task 2.1 in form of interviews, see Section 4.2.1, and Task 2.2 in form of a tabular template, see Section 4.2.2. Both tasks are ongoing, meaning that the input is currently collected and will be presented in following deliverables.

4.2.1. Information provided by guided interviews (Task 2.1)

As part of Task 2.1, telecommunication operators were interviewed to refine the requirements of the RESISTO platform. The interviews were structured following the resilience management approach described in Section 2. Therefore, also specific questions were included for defining the system and

modelling approaches, e.g. requesting if graphical representation of the network exists and can be shared.

4.2.2. Information provided by Excel template for threat list (Task 2.2)

Aim of Task 2.2 is to generate a threat, hazard and disruption list for the communication infrastructures. It includes the definition of a profile template, which was implemented as an Excel document.

To allow for thorough analysis of the threats, including the simulation of the response to protection and mitigation processes e.g. via network simulation, detailed information about the threat impact on the system is necessary. The Excel file therefor consists of the following sheets, which are interlinked by references between the tables:

1. System Components
2. System Functions
3. Threats
4. Improvement Measures

In the context of this report, the System Components sheet is of special interest. Each threat from the Threats table is linked to the system components that are directly or indirectly affected. This setup will help to find the relevant components that need to be described by the model and identify a reasonable complexity level for modelling the system. A screenshot of the System Components template is shown in Figure 5.

System Components								
ID	Name	Description	Subsystem	Type	Quantity	Technical characteristics	Interconnections	Comments
SC1								
SC2								
SC3								
SC4								
SC5								

Figure 5: Screenshot of the System Components sheet of the Excel template

The following information is collected for the system components specified in the table:

- ID: a unique identifier for each component
- Name: name of the component
- Description: general information about the component
- Subsystem: a classifier to identify in which subsystem the component is integrated (Radio Network, Optical Network, Satellite Network, Core Network, Data Center, Applications, Internal Network)
- Type: a classifier specifying the kind of the component (Hardware Device, Software Tool, Interconnection, Mechanical, Built structure)
- Quantity: rough number of how many entities are included in the network
- Technical characteristics: information on the component relevant for its functioning and/or assessment of disruption impacts e.g. data rate, physical dimensions, energy consumption

- Interconnections: possible direct linkages to other components of the system
- Comments: any additional information

Additional details on the Excel template are given in the report for Task 2.2: *D2.2 Cyber-physical threat/risk scenarios and pre-assessment*.

4.3. Examples of realistic network representations

4.3.1. Network diagrams of Orange Romania's infrastructure

Orange Romania, leader on Romanian mobile telephony market, is offering to its 10.2 million customers integrated services as voice, high speed Internet (GPRS, EDGE, 3G, 4G and 4G+), fixed telephony and TV.

There were identified several network elements and architectures, as described in WP2/T2.2- hazards and disruptions template:

- Internet Border Routers, the routers deployed at the connection point with upstream Internet providers
- FO Infrastructure, the fiber optical network and all facilities that provide optical connection between different points (core elements, border router)
- Mobile Switching Centers (MSC), the mobile network element that provides control of high-capacity switching in mobile circuit core networks
- Radio Infrastructure (BTS, BSC, NodeB, RNC, eNodeB), the mobile network elements that provides traditional cellular telephony, responsible for handling traffic and signaling in mobile switching subsystem
- Network Security Equipment (IPs, FWs)- security infrastructure that is different for mobile and fixed customers

A. Mobile infrastructure design

Mobile Core Network is deployed according to the 3GPP mobile reference architecture, containing the network elements that provides users' access to the specific services and applications, users being connected via the access network.

High level design of the split functional blocks:

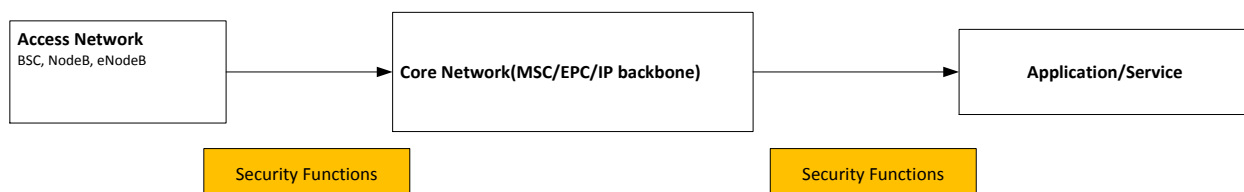
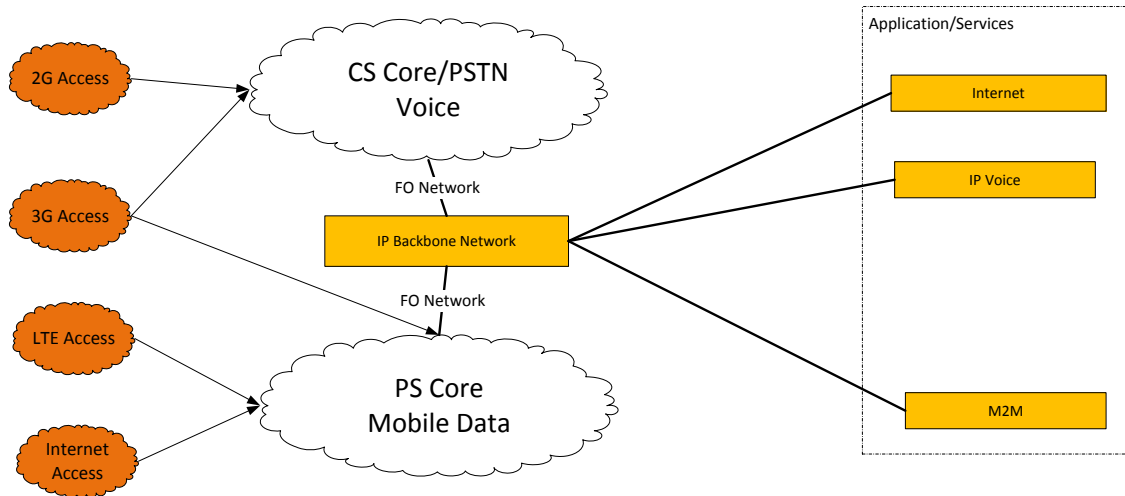


Figure 6 High Level Architecture of mobile operator

The functioning architecture described above is decomposed into a next level of granularity:



Different access technologies are connected to the mobile core network elements through the IP backbone network, requiring severe FO interconnections, as described previously, providing access of the services to different resources

The functional architecture presented is composed by several elements, that ensures the network resiliency and functionality at the lower level of applicability, transport of the data packets (IP networks).

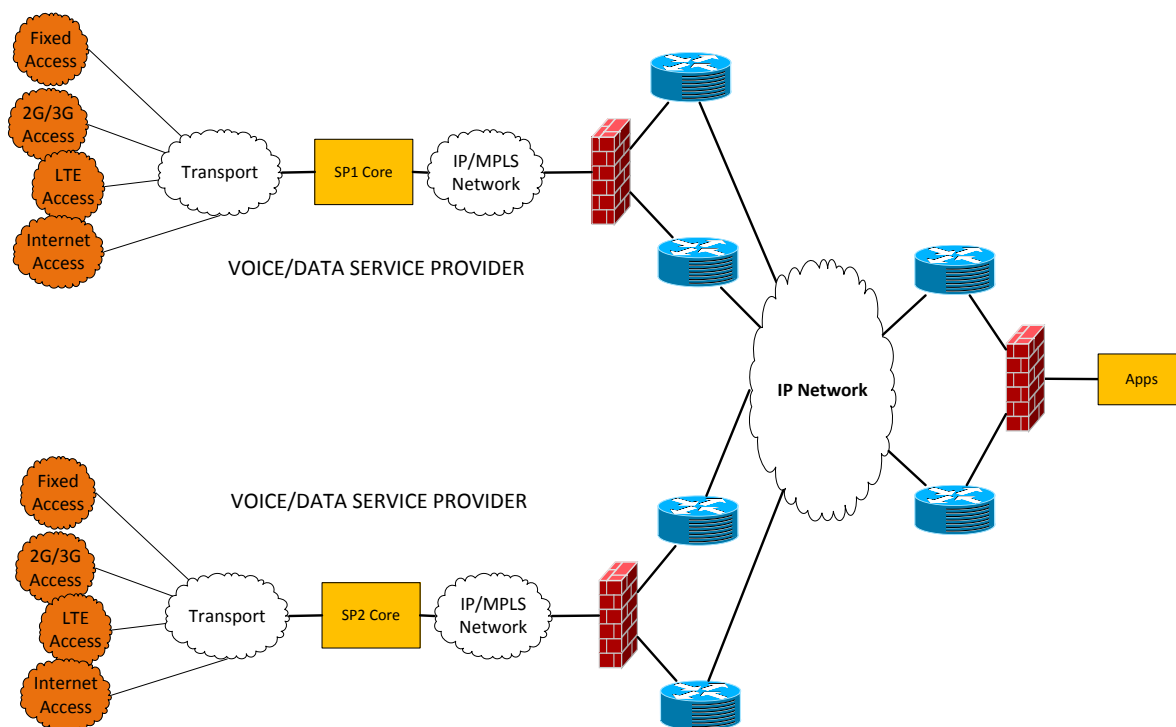


Figure 7 Mobile operator service functional distribution

The main idea, as presented in the previously figure. Is that the services are distributed at the core and transport/network level between different network elements, corresponding to different services within specific geographical area. Any malfunction in the upper layer of the diagram should not impact the functioning of the others services, excepting signaling propagated errors in the network.

Inside the Service Provider network, there are defined several hierarchical levels of infrastructure, Access, Distribution and Core (*descriptions and roles of each segment will be appended/updated in the next version of the document*).

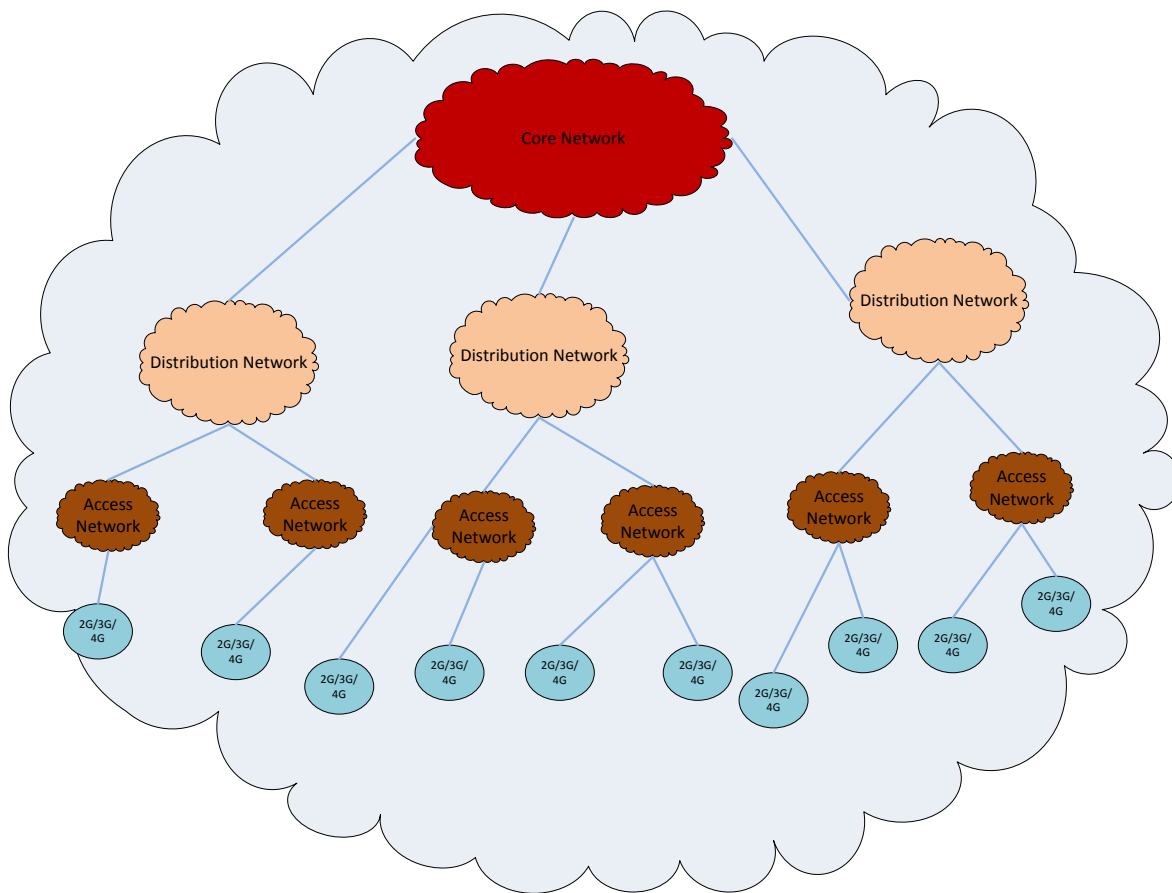


Figure 8 Hierarchical network distribution

Each layer of access network is resilient connected to the distribution and each distribution layer is resilient connected to the core, resiliency being assured mainly at the transport level.

The blocks and network elements (physical or virtualized) which are composing the service logic are distributed as follows:

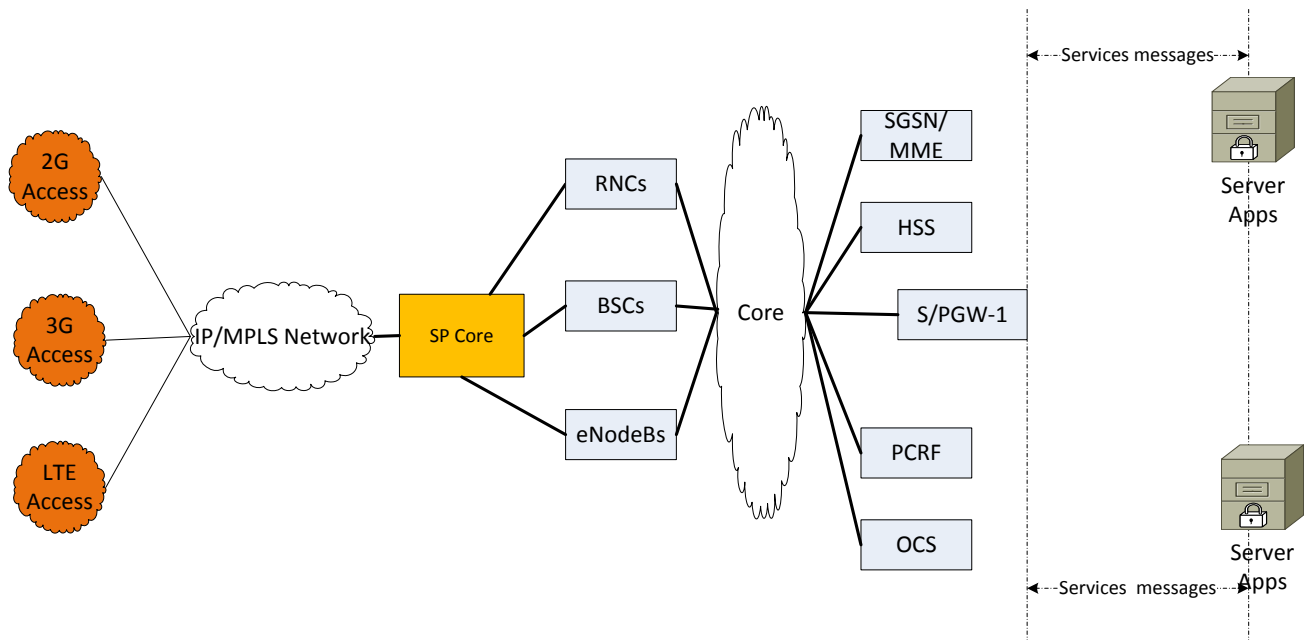


Figure 9 Mobile Operator Core service split

The IP/MPLS network, the Service Provider(SP) Core is providing at the high level point of view the connection between the access part (2G/3G/4G) and the core part, adding some specific particularities in terms of subscriber database, management entities, anchoring points, policy charging rules and the charging systems.

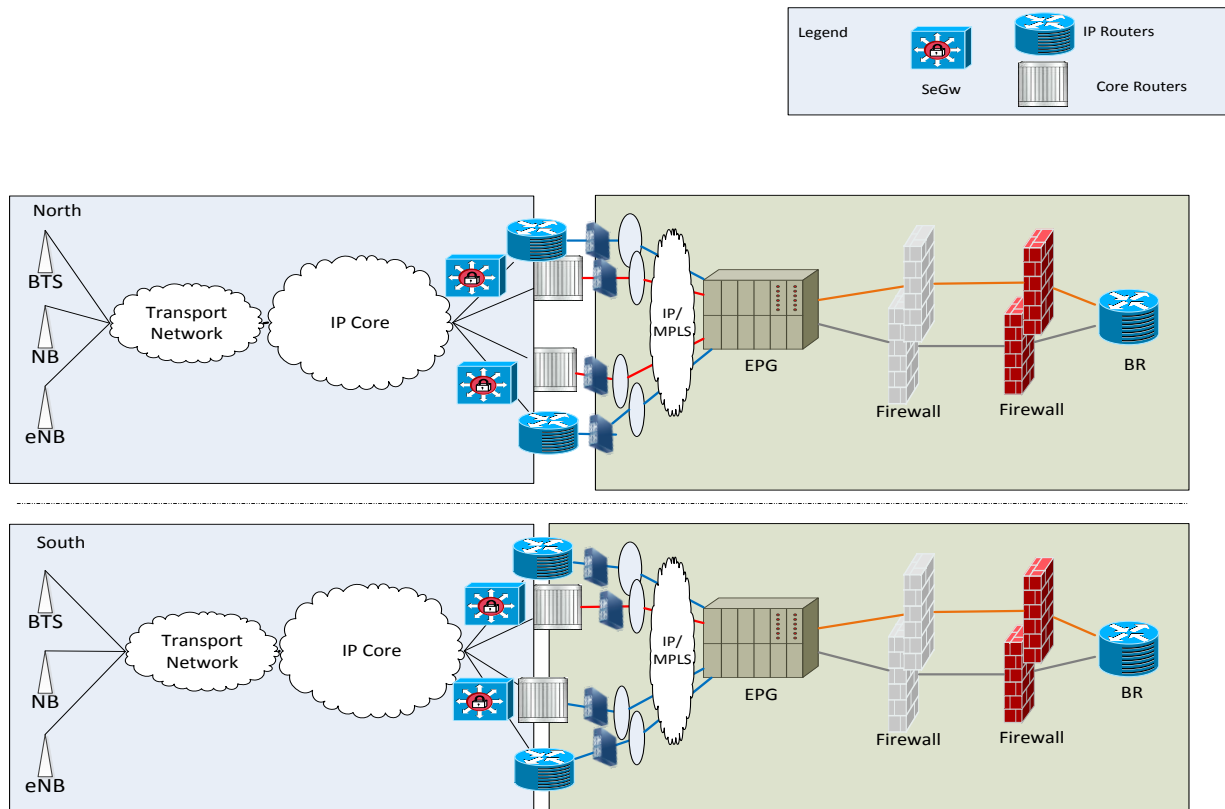
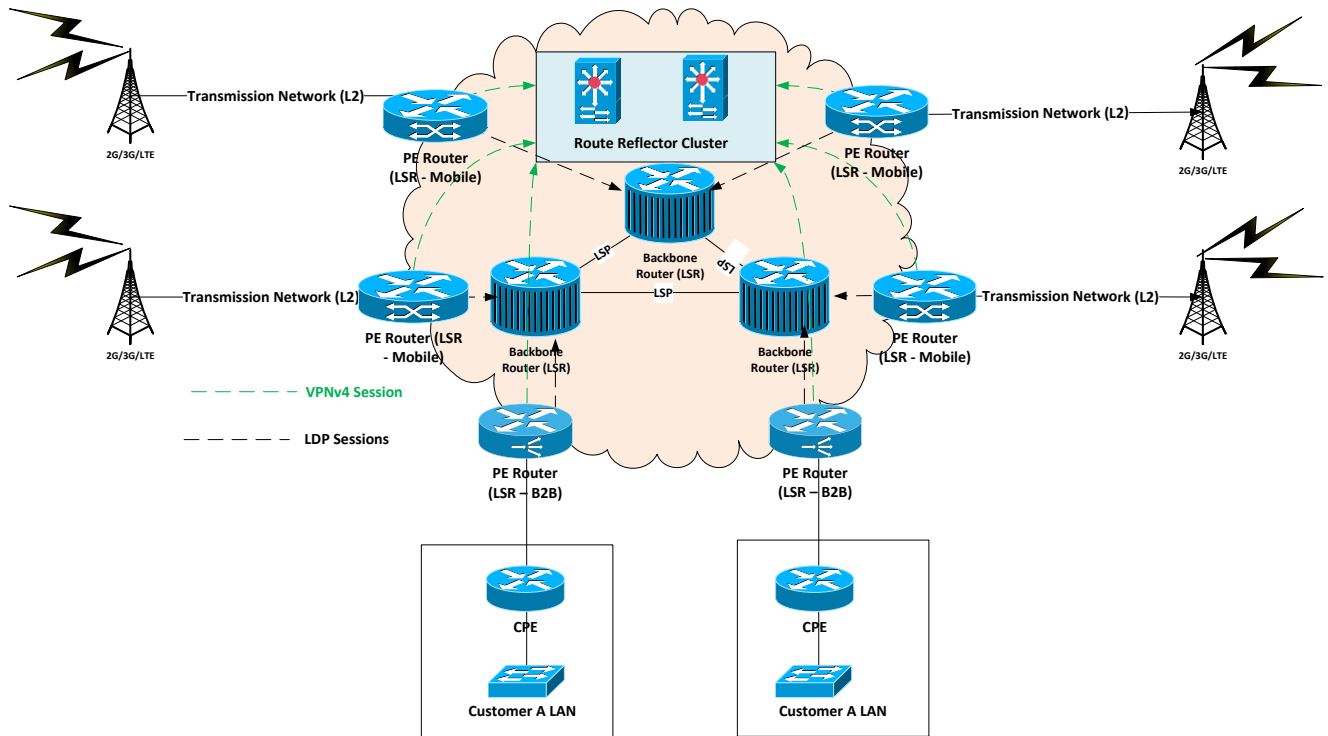


Figure 10 Mobile data core network architecture

For clarification purposes, the entire network system defined for core network element, as EPC (MME, SP-GW), HSS, MSC are under a rule of resiliency and redundancy at network level, as presented and at application level.

B. Fixed services infrastructure design

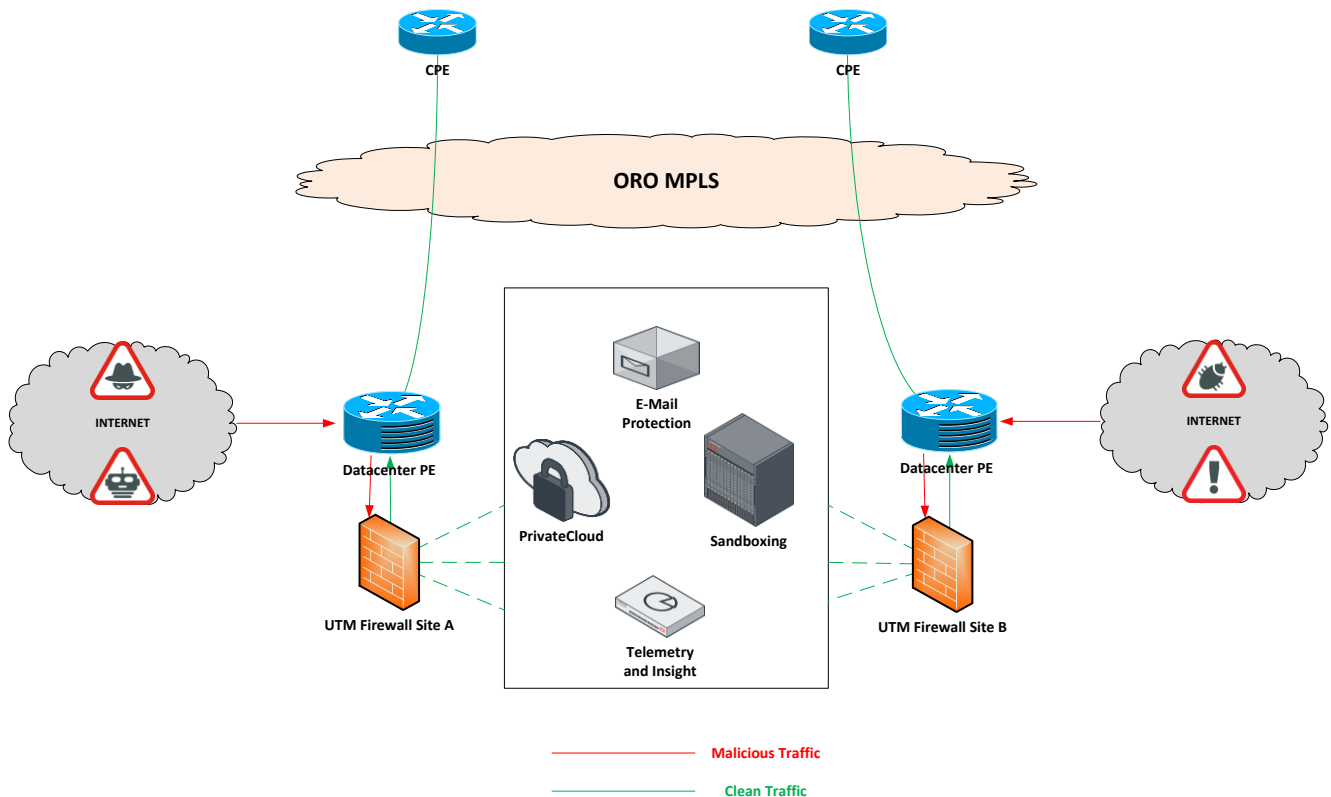
➤ General backbone network design



Network is composed of Backbone nodes that are pure LSR routers. BGP free core is achieved using redundant clusters of Route Reflectors – One cluster for Fixed B2B network and another cluster for Mobile Networks.

The B2B and Mobile networks are completely separate towards the access zone. Services are delivered using MPLS layer 2 and layer 3 VPNs.

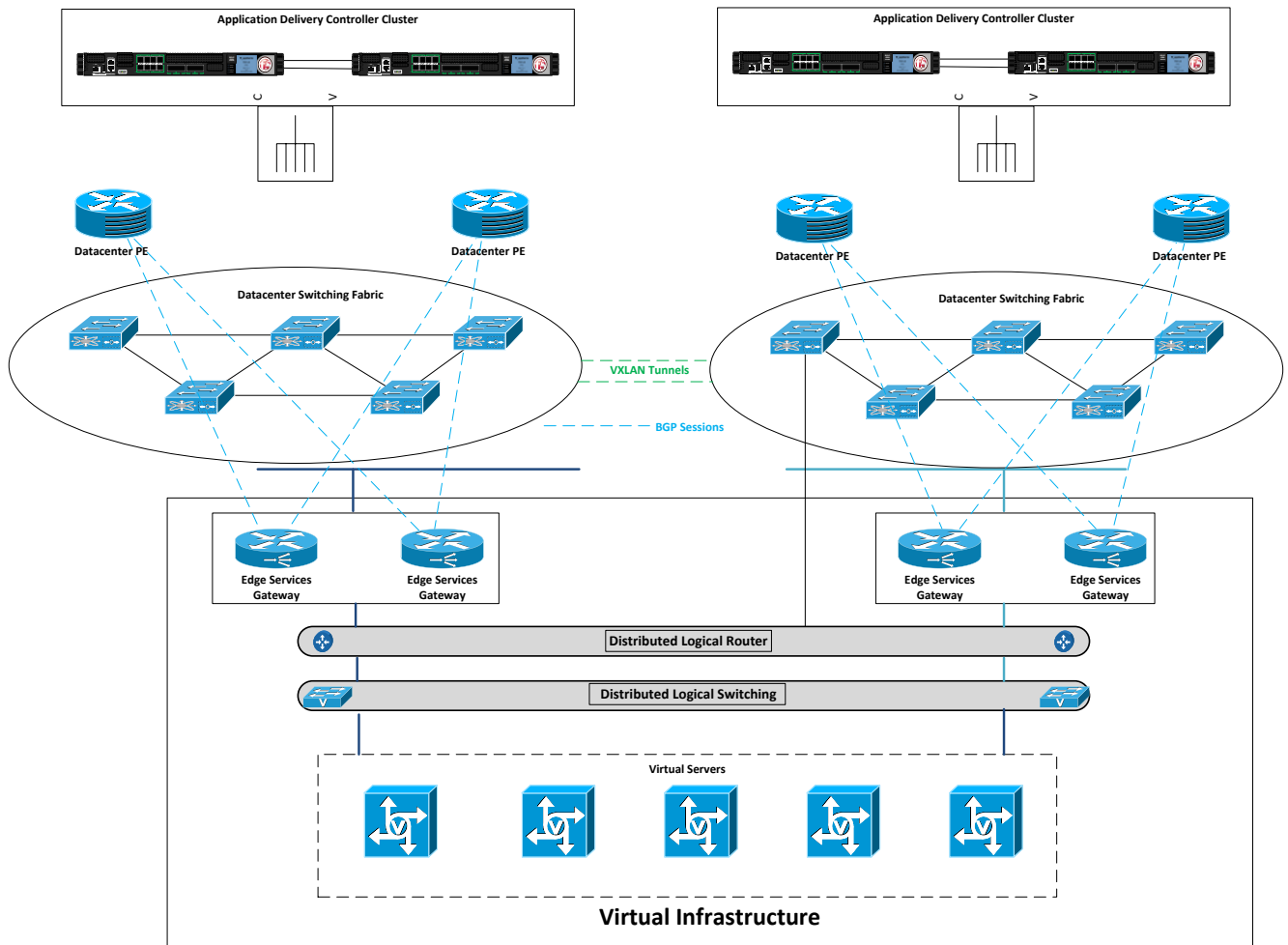
➤ Customer Internet Security



B2B Traffic is routed through centralized firewalls that are layer 7 content aware and offer unified threat management (UTM). Among the protection services we enumerate: Web Application Firewall, Antivirus, DoS/DDoS protection, Intrusion Prevention Systems, E-mail filtering.

Using next-generation event correlation and telemetry data – constant network and client vulnerability scans take place and proactive countermeasures are constantly deployed – all this being assured by a dedicated Security Operation Center.

➤ Datacenter Design



Datacenter infrastructure is designed with two things in mind – Resiliency and Scalability . At the top of the chain there are application delivery controller clusters that offer service multiplexing and high availability using inter-site health check and service monitoring .

Traffic then passes through the switching fabric which is also VXLAN aware for ease of transport and service encapsulation. Inter-site virtual machine redundancy is achieved using distributed logical constructs – Distributed Routers, Switches .

Automatic re-route of traffic is done using separate edge services gateways that assure service resilience using BGP as the dynamic routing protocols.

4.3.2. Short description of the OTE Network

Introduction

OTE Group is the largest telecommunications provider in the Greek market and together with its subsidiaries, forms one of the leading telecom groups in South-eastern Europe. The Group consists of the parent OTE S.A. Company and its subsidiaries, offering fixed telephony (telephony, data and leased lines), broadband, ICT, television and mobile telephony services in Greece and Romania, as well as mobile services in Albania. The Group is also engaged in providing additional services, such as ICT solutions, real estate, maritime communication services and professional training. In 2017, the companies in which OTE Group participates employed 20,305 employees.

OTE S.A. is the parent company of the OTE Group and the main fixed telephony operator in Greece. It offers broadband, ICT services, fixed-line telephony, television, data and leased lines. COSMOTE S.A., a subsidiary of OTE, is the leading mobile service provider in Greece. OTE Group also established COSMOTE as the single commercial brand for all fixed, mobile, internet and television products in the Greek market, so that all customers can enjoy an integrated communication and entertainment world with ease, speed and simplicity. OTE Group has other subsidiaries such as OTE SAT and OTE Globe and also presence in other countries through as it is depicted below:

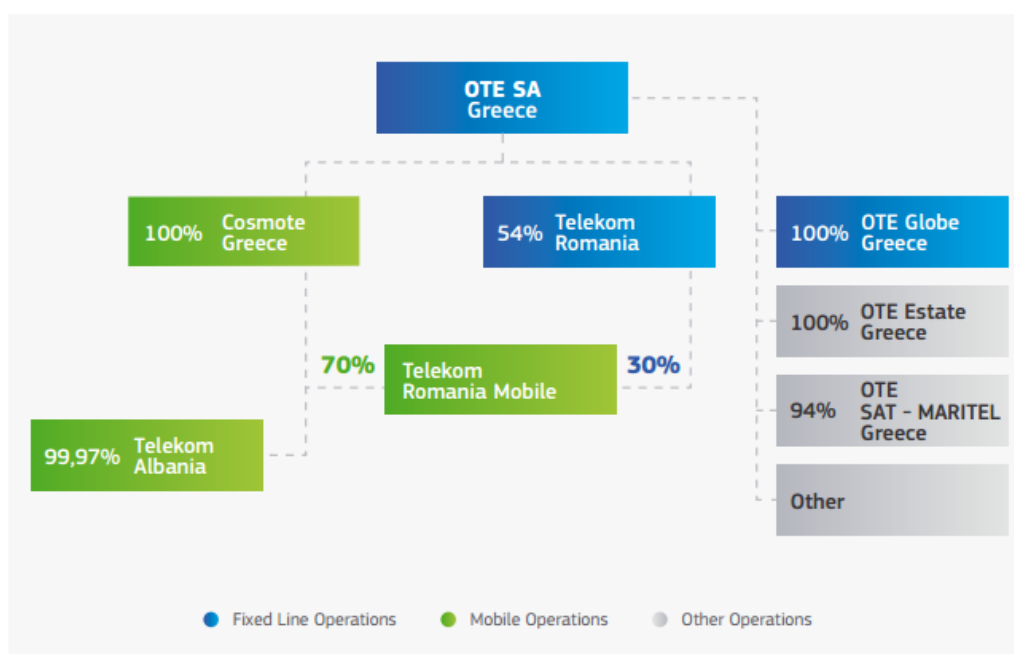


Figure 11: OTE Group of Companies

Products and Services offered by OTE Group¹

OTE operates in the fully liberated telecommunications' markets, providing telephony, Internet, services of telecommunications providers, as well as Satellite Communications. Having as main

¹ https://www.cosmote.gr/otegroupsustainability2017/downloads/report2017_eng.pdf#page=51

inspiration the daily life of its customers, OTE plans and offers innovative products and services, as well as integrated telecommunications solutions covering even the most specialized market needs. OTE is on the first line of technology development, having a leading position to the market of services broadband Internet (ADSL). A priority of strategic importance for the company is the constant upgrading of its networks in order to cover the continuously increased demand and the need for higher access speeds. In this frame, OTE also offers VDSL services, with connection speeds to the internet up to 50 Mbps.

The convergence of telecommunications, the trend for "house entertainment", as well as the important development of xDSL on recent years, lead OTE to the creation of services of digital subscription television. OTE TV offers more than 65 theme channels and the national channels available all over Greece via Satellite as well as via broadband connection.

For enterprise and company clients, OTE proposes innovative products and services of telephony, connectivity and data, as well as advanced solutions, which combine technologies of networking and informatics, for any modern enterprise regardless its size. For the alternative telecommunications providers, OTE, being the main provider of services of telecommunications infrastructure via OTEWholesale² and its subsidiary, OTEGlobe³, offers a total of high-tech products and high quality services.

In addition OTE Group offers integrated and innovative technology solutions to enhance business and sustainable development. Through products and services, customers enjoy the benefits of using broadband services to improve their operation, environmental performance and prosperity. Some examples of services offered are the following:

Business Cloud: Cloud services for businesses, in order to improve their operations and flexibility, and to reduce their operating costs. Such services are:

- COSMOTE Business Cloud Servers
- COSMOTE Business Email
- Specialized cloud applications: (e.g. Soft1 SmartWorks, Soft1 SmartPros, Soft1 SmartBiz),
- COSMOTE Video Conference

Information Security: Services for the increasing needs of businesses' security while they are using the Internet

- COSMOTE Business e-Secure
- Mobile Device Management
- COSMOTE Mobile Security NEW
- Anti DDos

Smart Cities: The "smart cities" portfolio includes solutions such as Smart Parking, Smart Traffic Management, Smart Street lighting, Smart Waste Management, Air Quality Monitoring, Smart Water Management and Electric Vehicle Charges.

Fleet Management: Fleet tracking and management, to ensure "green" and safe driving and thus to reduce operating costs, through the use of machine to-machine communication.

- Driving Performance
- COSMOTE e-Track
- e-Fuel Management

² <http://www.otewholesale.gr/HomePage/tabid/36/language/el-GR/Default.aspx>

³ <http://www.oteglobe.gr/en>

Solutions for Hospitals: Solutions specifically designed for the health sector and implementation of large and complex IT Integration projects

E-Energy: Solutions for better energy management consumption by businesses,

Development of Electronic Applications: Development and improvement of applications, digital self-care functionalities and on-line services, such as e-invoice, e-payment etc.

Infrastructure⁴

OTE provides reliable and qualitative communication to all people in Greece, even in the most remote and inaccessible areas of the country, utilizing more than 35.000 km of optical fibers, numerous satellite, underwater and terrestrial international links. Infrastructure is also continuously upgraded, following the technological developments. In the diagram below, Figure 12, the Urban High level Network Architecture is depicted.

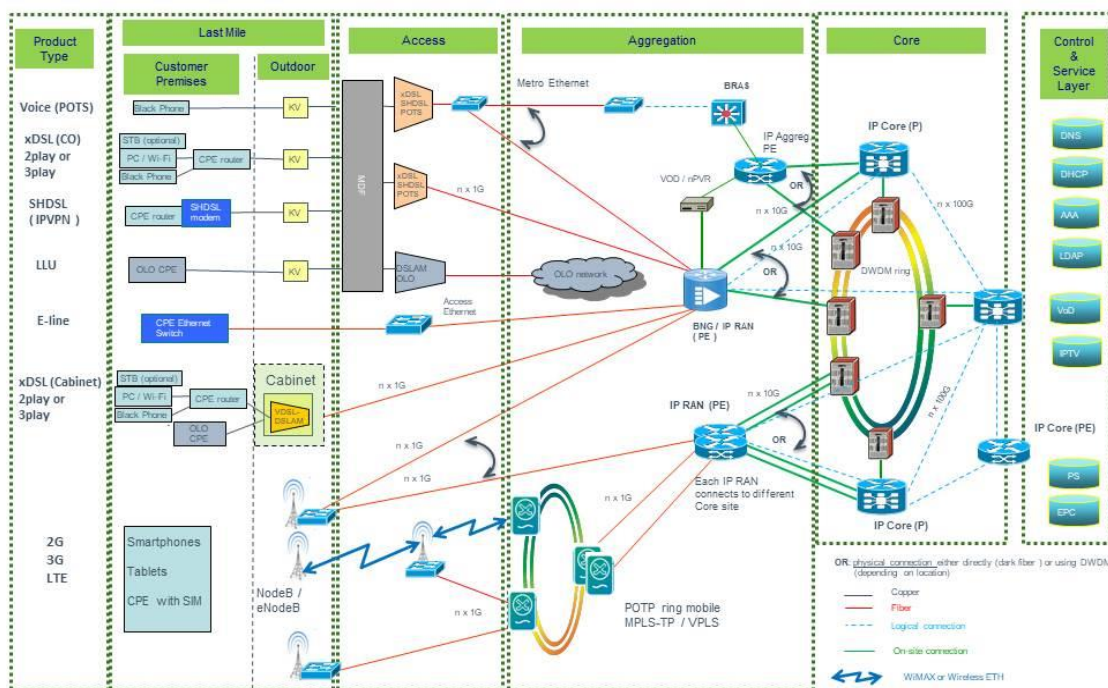


Figure 12: Urban High level Network Architecture

OTE's Network is configured in aggregation, access and core network. The core is routing traffic from cells sites (or points of presence) into the core network. It has higher speed to transfer large information sent from various terminal equipment. Backhaul parts as well as access parts can be via wired or wireless solutions. It should also be noted that mesh connectivity is used among many nodes in order to avoid congestion, provide load balancing and avoid single points of failure.

⁴ <https://www.cosmote.gr/fixed/corporate/company/who-we-are/network>

Control and Service Layer: Here are located all services provided by OTE. These services could be telephony services and IMS, users' authentication, address assignment, IPTV etc.

Core Network: Core network is the platform that serve all the services offered by OTE group and aims to connect all kinds of circuits from the access network to the aggregation and Core network (and vice versa). The Core network of OTE group includes Next-Generation Synchronous Digital Hierarchy (NG-SDH) rings, Metro Ethernet nodes and mobile links and Dense Wavelength Division Multiplexing (DWDM) optical rings. The IP/MPLS-based network consists of 7 (dual) core nodes (Koletti, NYMA, Ermou Thessaloniki, Patras, Larissa, Herakleion,). The core nodes at NYMA, Koletti & Ermou are also interconnected (in a resilient way) with our upstream provider (OTEGlobe) in order to provide global Internet connectivity.

100Gbps links have been introduced between core nodes, as well as between IP core & OTEGlobe. OTE's IP network is topologically very close to the TeraStream concept (only 2 IP nodes between customers and services, IPv6 support end to end) which the target architecture is for all NatCos in DT group. OTE is also in the process of consolidating the IP core networks of OTE & Cosmote, further enhancing the footprint of IP network and creating economies of scale.

OTE's IP core network supports dual stack operation (IPv6 protocol along with the former IPv4 protocol), as part of the preparations for future developments and services (internet of things, Machine2Machine etc), and will be the first network in the DT group to offer IPv4 as a service over IPv6 using the LW4o6 technology and NFV elements (and solving the problem with IPv4 addresses exhaustion. Regarding IPv6 penetration, OTE is in the top 20 providers worldwide.

In order to meet increased traffic demands of the access network, transport network extends and upgrades continuously by installing new nodes, upgrading capacities and addition of terrestrial and submarine fiber optic cables.

Aggregation Network: In this network there are more than 100 BNGs/BRASs that aggregate the broadband traffic and several other big routers dedicated to business services (SYZEFXIS, VPNs, LL etc). All BNGs/BRASs are connected to diverse core nodes with at least 2x10Gbps links. The core nodes themselves, are interconnected by Nx10Gbps links to ensure the maximum possible quality of service & reliability.

Transport network is part of aggregation and serves all the services offered by OTE group and aims to connect all kinds of circuits from the access network to the aggregation and Core network (and vice versa). The Transport network of OTE group includes Next-Generation Synchronous Digital Hierarchy (NG-SDH) rings and Metro Ethernet nodes,

New OTE Transmission Network, which is being developed is based on the MPLS-TP protocol and on the POTP platform (Packet Optical Transport Platform). This new platform is flexible enough to serve all the Packet-based broadband services with flexibility and expandability in the necessary bandwidth.

Access Network: The access network refers to the network segment that connects the subscriber to the Central Office (CO). It is based on copper cables which are gradually being replaced by optical fiber cables due to investment in NGA (Next Generation Access) network. Specifically, OTE deploys a modern NGA network based on Fiber to the Cabinet – FTTC architecture, which brings optical fiber cables and active VDSL2 equipment on outdoor cabinets and offers broadband access services of up to 50 Mbps bandwidth.

Basic Access Technologies

- Copper: Ethernet is the most commonly installed wired LAN (local area network) technology. Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires, xDSL POTS, ADSL, VDSL, ISDN, Metro Ethernet
- Wireless Transmission: Cellular (2G/3G/4G), WiFi (802.11x), WiMax (802.16)
- Optical Fiber: PON, SDH. Metro Ethernet

Last Mile network: Is the final connectivity leg between the telecommunication service provider and an individual customer. Here signals are carried via any kind of digital medium from the broad along the relatively short distance (hence, the "last mile") to and from the home or business. Last-mile technologies include:

- Plain old telephone systems (POTS)
- ISDN,
- Digital Subscriber Line (DSL) over existing telephone twisted pair lines
- cable and the cable modem for data,
- Wireless, Cellular
- optical fiber and its transmission technologies

Products: Voice (POTS), xDSL 2play or 3 play, Wholesale xDSL, 2G, 3G, LTE

In the table below a summary of OTE's networks and their elements is presented.

Domain	Network Elements
Access	Outdoor cabinets with xDSL DSLAM/MSAN (FttC). xDSL indoor DSLAM/MSAN Access Ethernet switches Mobile sites
Aggregation	NG-SDH nodes POTP nodes fixed & mobile BRAS routers BNG routers IP aggregation routers (PE) (fixed) IP RAN (PE) routers (
Core	DWDM nodes (both for PE to P and P to P) IP core (P) nodes fixed - mobile IP core (P) nodes mobile only (will be migrated to common core) IP core (PE) nodes mobile

Table 1: OTE Network Elements

Power supply:

Grid power supply for telecommunications enjoys a long tradition of reliability built into the public telephone network. But the new digital equipment requires extra protection in case of grid power interruptions and fluctuations.

The electronic equipment operates on direct current (DC) provided by batteries that can support the electronic equipment for several hours in the event of power failure. Being a constant voltage power source, batteries also isolate the electronics from electrical noise prevalent with alternating current (AC) power. Rectifiers that convert the incoming AC power into DC power recharge the batteries. DC power provides a simple, inherently reliable, and clean source of electricity.

As a primary power supply and especially in remote mobile nodes in the mountains besides grid power we use other sources of power such as oil generators, wind miles and solar panels.

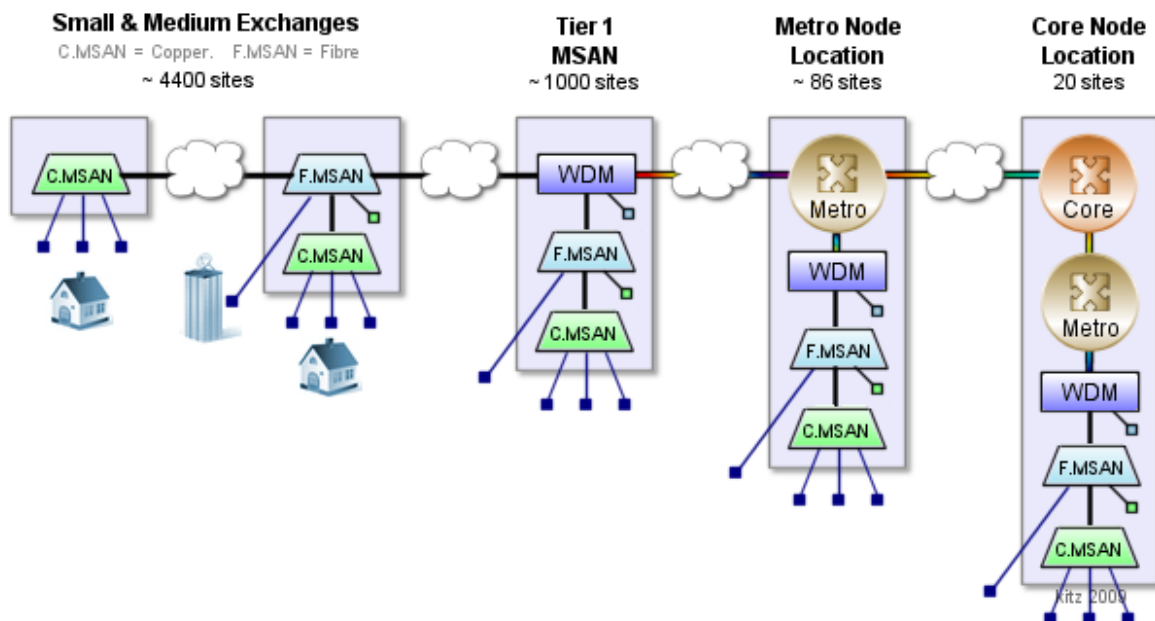
4.3.3. Network diagrams of the BTC infrastructure

All details provided in this subsection are publically available from the following site:

https://kitz.co.uk/adsl/BTwholesale_network.htm

BT's 21st century network is to replace the existing PSTN and ADSL Broadband equipment in the exchange as well as the core network with newer and more modern technologies. It will provide multi-services such as voice, video, content and data as well as higher speed broadband, all carried over an IP based network. This is an ongoing work and will take several years.

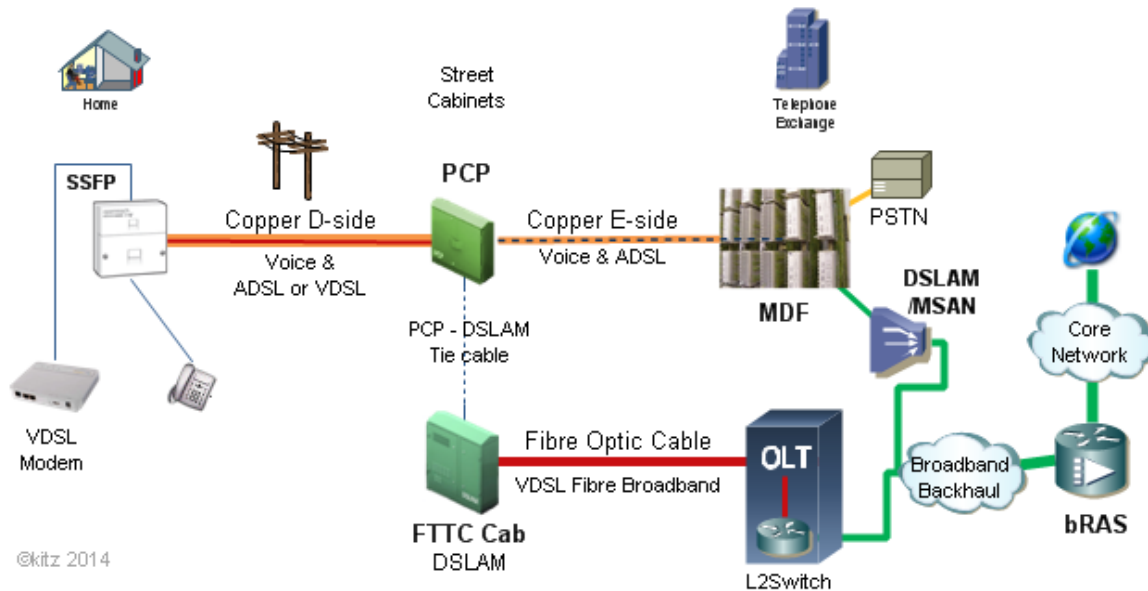
BT 21st Century Network



The MSAN (Multi Service Access Node) is the equipment in the exchange which is responsible for aggregating voice and data from customer and for routing this traffic on to the main backhaul.

- **C.MSANS** - terminate copper (telephone) cables from the home.
- **F.MSANS** - terminate fibre optic lines from business user premises.

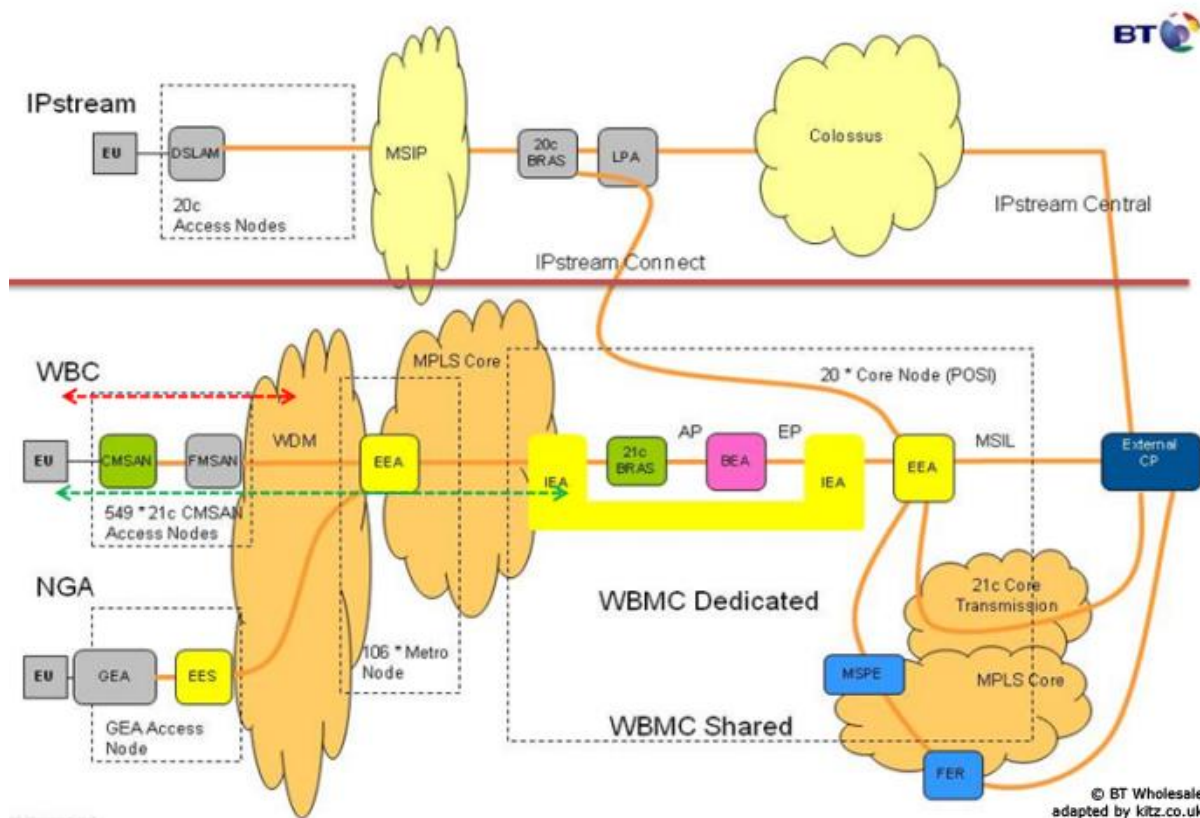
Fibre To The Cabinet (FTTC)



The BT Wholesale Converged Network below consists of

- IPStream/IPStream Connect
- WBC
- WBMC shared
- WBMC dedicated
- NGA

BT Wholesale Converged Network



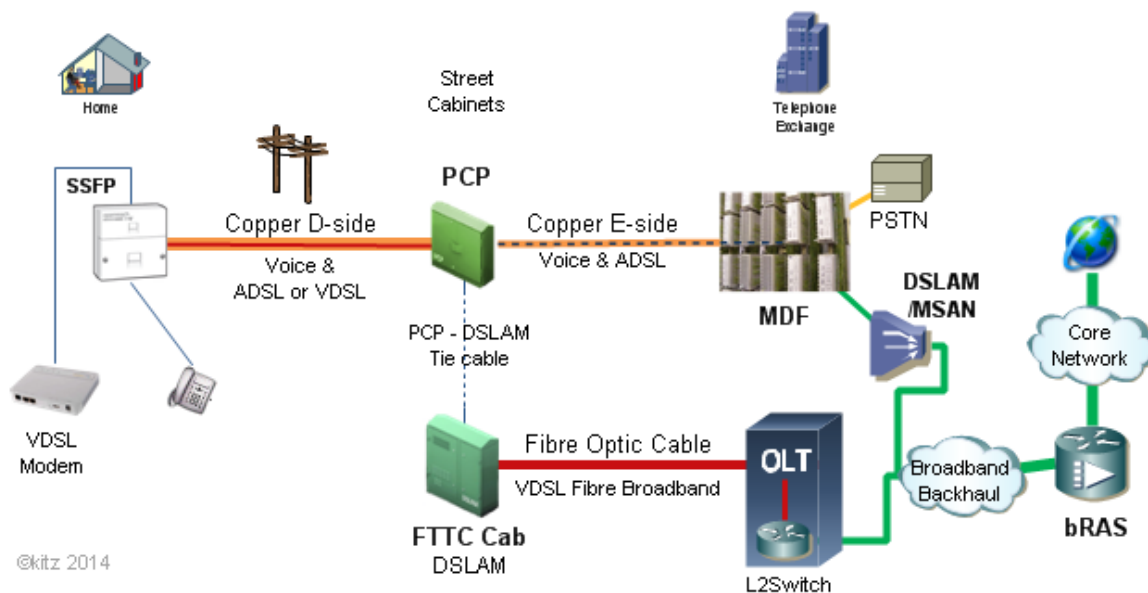
- **Access Node** - A local exchange containing one or more MSANs. For more info on MSANs see: [Inside the BT Telephone Exchange](#).
- **AP** - Aggregation Point. Where multiple end users are aggregated into a single path for connection to the CP. For more info on APs see: [What are Aggregation Points](#).
- **BBEA/BEA** Broadband Edge Aggregator.
- **BRAS** - Broadband Remote Access Server (BRAS or RAS) routes traffic to and from the digital subscriber line access multiplexors (DSLAM) on an ISP network. The BRAS manages the logical path from the consumers modem through to the IP core network. For more info see page: [BTw network RAS](#).
- **Colossus** - BT's 20CN UK core Internet backbone network mesh which runs on IP technology. For more info see page: [BTw network Colossus](#).

- **Core Node** - One of the 20 sites where WBC traffic is aggregated and handed over to the CPS.
For more info on Core Nodes see page: [21CN Core Nodes](#)
- **CP** - Allows CPs access to broadband end users - Carrier Provider.
- **DSLAM** - A Digital Subscriber Line Access Multiplexor (DSLAM pronounced dee-slam) allows telephone lines to make faster connections to the Internet. It is a network device, located in the telephony exchanges of the service providers, that connects multiple customer Digital Subscriber Lines (DSLs) to a high-speed Internet backbone line using multiplexing techniques.
For more info on DSLAMs see: [Inside the BT Telephone Exchange](#).
- **EEA** - Ethernet Edge Aggregator ([A 7750](#)).
- **EES** - Ethernet Edge Switch ([A 7750](#)).
- **EFM** - Ethernet in the First Mile. Ethernet over copper access.
- **EP** Extension Path. This is the connection from the AP at the WBC Interconnect Node to the CP.
For mor info see page : [What is an Extension Path](#)
- **EU** - End User. The customer or business that uses the service.
- **FER** - Front End Router.
- **GEA** - Generic Ethernet Access. Allows local loop equipment (eg Openreach) to be connected to fibre.
- **IEA** - Internet Edge Aggregator ([A 7750](#)).
- **IP Stream** - A method of delivering EU traffic over BTs network for presentation to the ISP using [Central Pipes](#). IPStream has been withdrawn as a product in 2014 replaced by [IPStream Connect](#).
For more information on IP Stream see page: [IPStream](#)
- **IPSC - IP Stream Connect** - A transitional product for delivery of EU traffic over BTs 21CN network for presentation to the ISP. Replaced [IPStream](#).
For more information on IPSC see page: [What is IPStream Connect \(IPSC\)?](#)
- **LPA** - Logical PoP Aggregator - A router that aggregates the traffic from BRASes at a 20CN broadband Point of Presence.
- **MCLAG** - Multi Chassis Link Aggregation Group
- **Metro Node** - The backhaul network from the Access Nodes terminates on the metro nodes.
For more information see page: [21CN Metro Nodes](#).
- **MPLS Core** - Multi Protocol Label Switching Core network. A high speed IP network, where packets are given a predefined route and pass straight through. Unlike a normal IP network where each packet is inspected and routed by each node in the network.
For more info see page: [21CN Core Nodes](#).

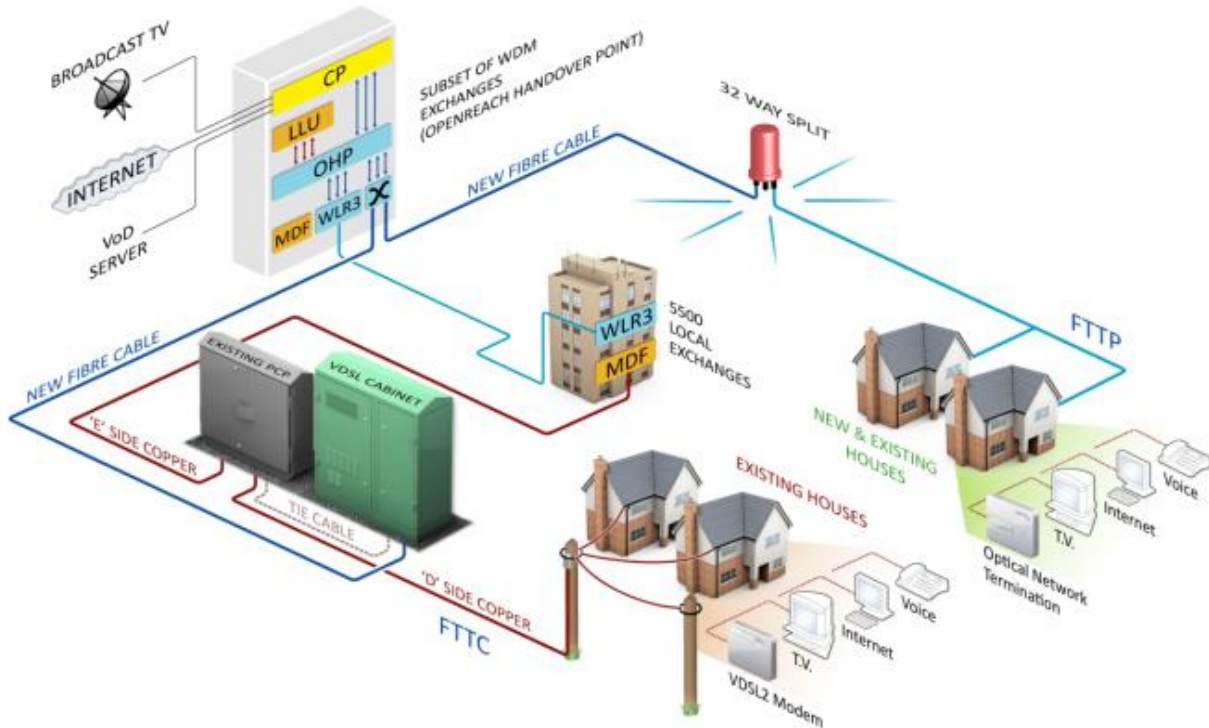
- **Fibre MSAN** - Fibre MSAN provides both direct access for Fibre fed customer services and aggregation/resilience protection to the Network. MSAN is essentially a next generation DSLAM and the edge of the 21CN backhaul.
For more info see page: [21CN Network Access FMSAN](#).
- **Copper MSAN** - Copper Multi Service Access Node equipment which provides all access for Copper Metallic fed services, PSTN Voice, DSL Broadband, Slow Speed Ethernet and converts the end user service to IP.
For more info see page: [21CN Network Access CMSAN](#).
- **MSE** - Multi Server Edge. See [MSE bRAS](#)
- **MSIL** - Multi service Interface Link is the Ethernet pipe connectivity between BTs and the CPs 21CN networks. MSIL provides for the needs of WBC, WBC (Converged) and NGN Call Conveyance.
For more info see page: [What is a MSIL](#).
- **MSIP** - Multi Service Intranet Platform. The name for BT's 20CN platform which carried ATM backhaul traffic.
For more info see page: [BTW Network MiSP](#)
- **Multiplexing** - Many of these network elements perform the same function of multiplexing many transmission pathways on to a single pathway such that a point is reached where a single physical connection can router connection into an ISPs network.
For more information see page: [DSLAM](#).
- **MSPE** - Multi Service Provider Edge. Takes 20CN BRAS capability closer to the end user. Less latency.
For more info see page: [MSE BRAS](#)
- **NGA** - Next Generation Architecture. Fibre based internet access such as [FTTC/FTTP](#) (Fibre to the cabinet/premises).
For more information see: [BT Openreach NGA Boundary](#).
- **WBC - Wholesale Broadband Connect**. A method of delivering EU traffic over the BT Wholesale network for presentation to the ISP. WBC requires the ISP to have a prescence at the core nodes for routing of traffic other than over the BTW core.
For more info see page: [Wholesale Broadband Connect](#).
- **WBMC (Dedicated) - Wholesale Broadband Managed Connect**. A method of delivering EU traffic over the BT Wholesale network for presentation to the ISP. BT Wholesale is responsible for not just backhaul routing but also routing over the core network. The ISP purchases their own [MSILs](#) at their chosen point(s) of prescence.
For more info see page: [WBMC - Dedicated](#).
- **WBMC (Shared) - Wholesale Broadband Managed Connect**. A method of delivering EU traffic over the BT Wholesale network for presentation to the ISP. BT Wholesale is responsible for not just backhaul routing but also routing over the core network. The ISP uses BTw [MSILs](#).
For more info see page: [WBMC - Shared](#).

- **WDM** - Wave Division Multiplexing. A method of combining multiple signals on to optical fibre. For more information see page: [Wave Division Multiplexing](#)
- **Alcatel 7750** Intrastate Ethernet Aggregation Switch (IP Multiplexor)

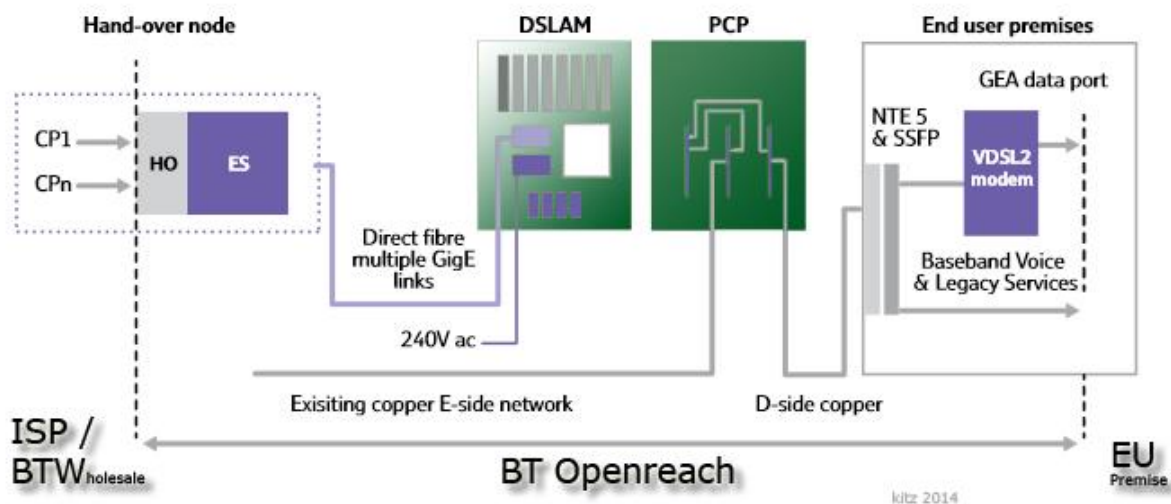
Fibre To The Cabinet (FTTC)



BT Openreach Fibre Network



FTTC Product NGA Boundary



5. IMPLEMENTATION OF TOOLS

Network simulation tools are planned to be provided for both the long-term and short-term control loop of the RESISTO platform. A state of the art overview on network simulations is given in Section 5.1. The partner RM3 plans to provide their network simulation tool CISIApro, which is introduced in Section 5.2. The partner EMI plans to adapt their more general simulation tool CEASAR to the special needs of communication infrastructures. They plan to use this simulation tool in particular for the long-term control loop and are currently revising it within the scope of WP3.

5.1. Network simulators

Simulation is commonly used as a tool to assess the behavior of a system in a controlled and simplified environment. In the field of networking, simulation is widely used for different purposes: to assess the impact of structural modifications, the effect of an attack, the interaction of protocols in a specific architecture, etc.

Nevertheless, the validity of the simulation results can be hindered by simplifying assumptions about the agents (i.e. devices, hosts...) behavior and other artefacts introduced by the framework. It is therefore critical to select simulators and models that are adequate in terms of complexity with respect to the context.

Beside simulation, network emulation can also be performed. In emulation, a virtualized network portion is connected to a real network, and the effect of the virtualized element is assessed. It is a step forward with respect to pure simulation. Most of modern network simulators can be used also as emulators (i.e. can relate to external network elements). In the following, simulators will be considered.

5.1.1. Key concepts

Network simulators can be characterized based on the method used to simulate events in the real world. The approach to simulation is usually defined based on how the flow of time is handled and how the events are generated. Time can be modelled either as a continuous or discrete variable. In a discrete-time simulation, the system is assumed to be in a stable-state except for instants where an event happens, therefore modifying the state of the system. The list of the events to be simulated can be stochastically generated or given as a simulation parameter. However, most of modern network simulators are based upon the discrete-time event approach.

A different approach is to categorize simulators based on the complexity of the scenarios that can be simulated. Simpler frameworks allow for faster prototyping while more complex simulators have the advantage of greater flexibility and customizability at the expense of a longer and more complicated setup.

A desirable feature in a simulator is the Graphical User Interface (GUI). While usually GUIs offer limited flexibility in customizing simulations, they can be used as a way of specifying the simulation topology at a coarse level.

In general, there is a great deal of overlap in the scope of application of most network simulator. Furthermore, most high-level simulators allow connection of virtual machines/devices to integrate natively available functions. Nevertheless, each simulator offers specialized functions that makes it more fitting to a specific context.

The complexity of the node behaviors can range from simple stochastic models of traffic handling (e.g., average time to service, average time in queue, average packet loss rate) to full stack emulation of an operating system. Notable examples include node models for heterogeneous type of networks (and connection standards) as well as complete emulation of network devices such as Cisco routers.

Finally, one of the most important features of a network simulator is the scalability. While the system requirements in itself are usually not a problem on modern computers, in order to simulate large topologies, it is fundamental that the resources footprint of simulating a simple node is as limited as possible.

5.1.2. Software packages

General network simulators

GNS3

GNS3 is a network simulator specialized in the emulation of network topologies, with a focus on layer 2 and above wired networks. GNS3 is specialized in topologies including completely virtualized professional devices (e.g. Cisco, Juniper) as well as using virtual machines as nodes. It is based on Dynamips, a no longer maintained solution for virtualizing IOS-based devices.

NS2/3

NS is one of the most well-known solution for network emulation, especially for research purposes. The older version (NS2) was written in C++ and OTcl. While it has been superseded by NS3, it is still used due to the large number of material (e.g. models, custom nodes) that are available. NS3 is written completely in C++ with Python bindings. Comparison studies [10], [11] show that NS3 appears to have the best overall performances in terms of speed and scalability between network simulators.

SDN simulation

SDN simulators are specialized on simulating a data plane that supports the OpenFlow protocol and other southbound API standards. Those are generally integrated with a software defined controller (e.g. POX, Floodlight) to simulate a complete SDN topology.

Mininet

Mininet is one of the first solution that was made available for the simulation of SDN networks. The topologies are specified in Python, and the behavior of the network nodes can be customized as well. One of the most important features of Mininet is its simplicity. Mininet is reported to be scalable, supporting topologies with a high number of nodes, albeit having potentially not consistent results in the data plane performances. As it is, Mininet is a useful tool for SDN simulation that are focused on the controller and its behavior.

Estinet

EstiNet [12] is a commercial solution for simulation of SDN networks. Unlike Mininet, Estinet is a more complete product, offering a simulation engine and better guarantee about the correctness of the results when investigating data-plane performances. Comparative studies show that, in general, Estinet offers more reliable results as well as better scalability [13] until topologies with more than a thousand nodes are simulated.

5.1.3. Network traffic models

To assess the performances of a given network element in a simulation, a realistic flow of network traffic is needed. For Internet traffic, a possible option is to use capture file (e.g., tcpdump traces) to replicate the traffic captured from a specific node. However, this approach has several limitations. Basically, to get reliable results a considerable amount of traffic must be available and stored. For this reason, a stochastic approach to the traffic generation is preferable. Two major trends can be distinguished: packet-based approaches, where the packets distribution generating packets is characterized, and flow-based approaches [14], where the traffic is characterized as flows of packets belonging to a common stream (e.g. a TCP session).

Packet-based traffic models

In the following, some of the most important family of probability models for packet-based traffic generation are introduced. A more complete coverage of the topic is available in [15] and [16].

Older models

The first model to be employed were the ones used to model telephonic traffic. A typical example is the Poisson traffic model, where the probability of a given event (e.g. packet departure from a node) is given by a Poisson distribution.

This type of model has not been very successful in modelling internet traffic. Furthermore, their main advantage, which was low complexity, has been made superfluous by modern computational capabilities.

Long-tailed models

Long-tailed model have been adopted given the observations of self-similarity in the distribution of real data. In general, the fact that many quantities in networking exhibit a long-tailed distribution (e.g. interarrival time for packets, file size distributions).

Example of long-tailed distributions are the Weibull and Pareto distribution

Autoregressive models

Autoregressive models are based on the principle that the next item in a series can be predicted by a combination (usually linear) of the previous n items in the series (where n is the order of the model). The coefficients are learned from data.

Flow-based traffic models

While long-tailed models can be characterized correctly the behavior of various quantities, there are usually more effective ways to characterize the network traffic at aggregate level. The term flow is used to describe aggregate of packets corresponding to specific sessions (e.g. the transfer of a particular file). Flow-based modelling has been proposed for various network traffic modelling tasks [17], [18], [19] Flow level is often modelled through Poisson processes, but self-similar behaviors are present at flow level as well [20].

5.2. Mixed Holistic Reductionist – CISIApro modelling approach

CISIApro (Critical Infrastructure Simulation by Interdependent Agents) [21] is an Agent-Based Simulation Software and Engine used in Critical Infrastructures (CI) Protection projects to model behaviors and characteristics of involved entities due to possible, complex, cascading effects. Such modeling software, in combination with the Mixed-Holistic-Reductionist (MHR) approach [22], is used

to address a coherent level of granularity to a given CI scenario. It was born with the aim to analyze failure propagation and performance degradation in systems composed of different, heterogeneous and interdependent infrastructures. Each component is defined as an agent. Each agent has the same structure based on few common quantities, representing the state or memory of the agent.

An **Agent-Based** approach adopts a bottom-up view considering the overall behavior of the system (of interconnected infrastructures) emerging from a consistent number of interacting agents each of which models one or more physical infrastructure components or services.

Functional **(inter)dependencies** in complex systems are, sometimes, very subtle and difficult to be described due to the presence of indirect relations and complex feedback paths. Modeling and simulation of interdependencies between critical infrastructures has become a considerable field of research with the aim to improve infrastructure support planning, maintenance and emergency decision-making. **Interdependencies** increase the vulnerability of the corresponding infrastructures as well as failures' propagation from one infrastructure to another with the consequence that the impact due to failures of infrastructure components and their severity can be exacerbated compared to failures confined to single infrastructures.

Complex systems and their interactions can be interpreted with different perspectives, multiple approaches and different levels of abstraction (granularity). MHR has the capability to combine **Holistic** and **Reductionist** approaches, in the same modelling technique, trying to maintain the benefits of both paradigms reaching an appreciable level of knowledge into a considered CI scenario. Transition between **Holistic** and **Reductionist** vision of a complex system does not occur only along the dimension (size), but also through different "point of view" with regard to the meanings of interdependencies and interactions, which exist between elements.

Reductionist approach tries to model complex systems into smallest and simplest pieces. With a reductionist perspective, each infrastructure is decomposed into a web of interconnected elementary entities and their behavior depends by the (mutual or not) interactions with the other reductionist elements.

Holistic methodology considers each infrastructure as reality with its own identity, functional properties and recognizable boundaries, which interacts with other similar entities according to reduced identifiable set of relationships. With such perspective it is easy to identify roles that each infrastructure plays in a specific context.

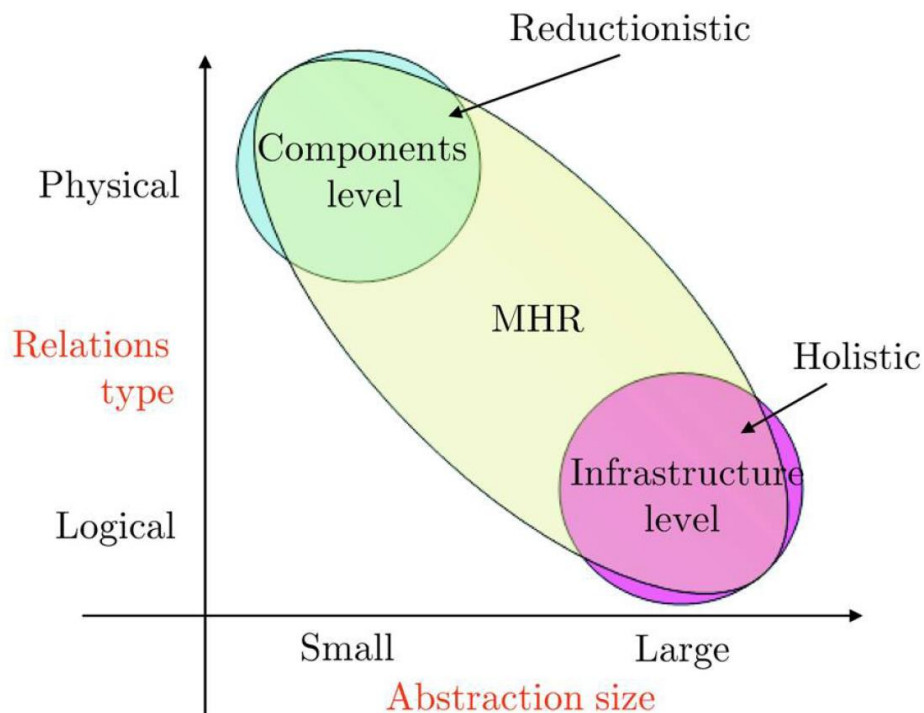


Figure 13 Dimensions in interdependent infrastructures modelling

The MHR takes the pros of each approach and tries to reduce disadvantages. Such methodology is cable of modelling interdependencies and Critical Infrastructures, respect to predefined levels of quality to customers or other facilities.

From this perspective, the best aspects of both approaches are maintained: the interdependencies among elementary components are modelled with the reductionist method, and the relations at high level are modelled through the holistic vision. MHR methodology contemplates infrastructure modelling at different hierarchical levels.

However, Holistic and Reductionist layers appears not sufficiently 'rich' to capture the CIs scenarios complexity and their interdependencies. To overcome this limit a further layer has been added, in the logical schema, to improve the model efficacy. The basic idea is to integrate three levels of abstractions, into a single simulator: holistic, reductionist and service. These intermediate entities are labelled as **Services** because their relevant characteristic is the function they perform and the *Quality of Service* (QoS) which they are able to provide.

Summarizing, MHR modelling permits to defining three different typologies of abstraction:

- An **Holistic Entity** [Figure 14] represents the infrastructure as a whole (or its general organizational divisions) in order to have a model that can take into account the global

dynamics between infrastructure (possibly one might think of representing behaviours related to policies, strategies, etc.).

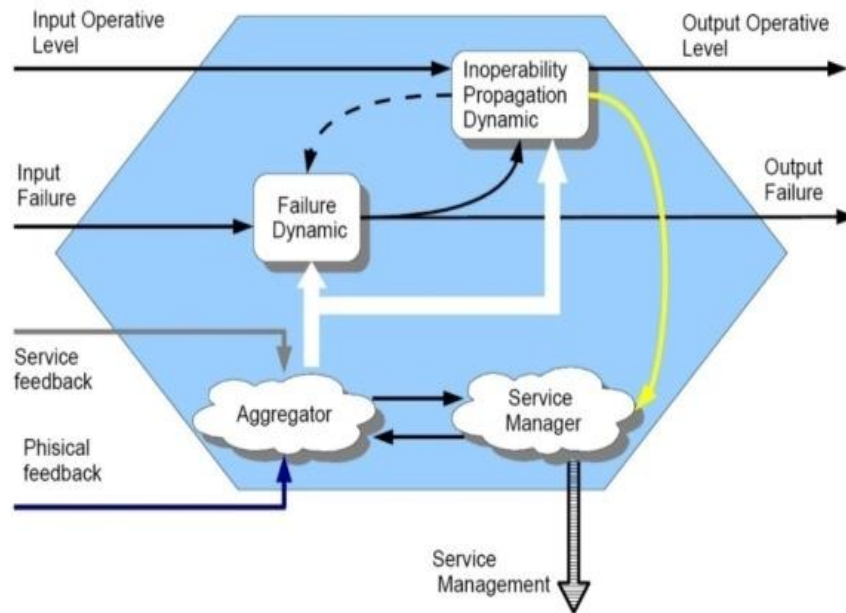


Figure 14 Holistic Block

- A **Service Entity** [Figure 15] represents a logical element, organizational or real, that provides an aggregate resource, for instance, could be express through a QoS (Quality of Service) level.

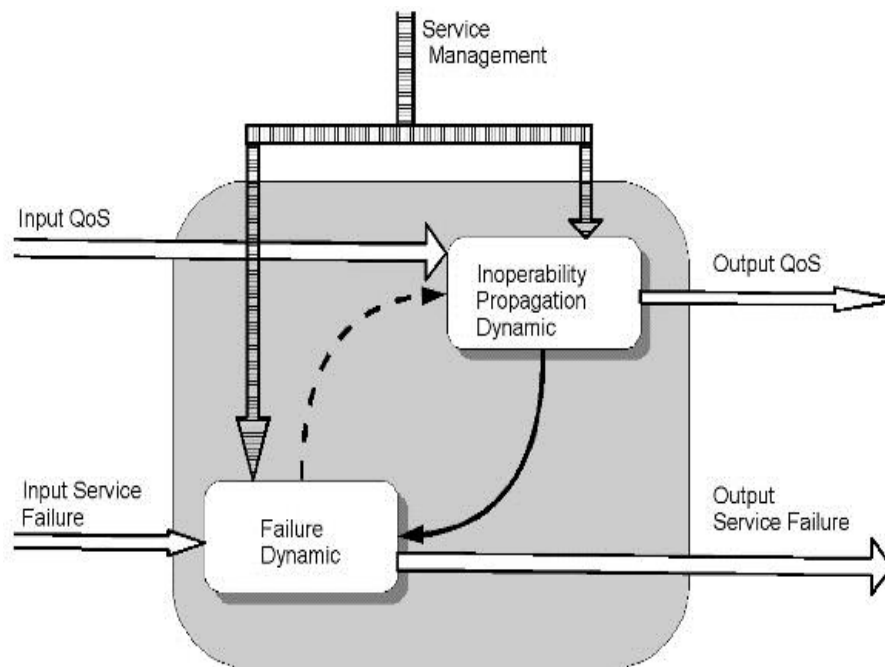


Figure 15 Service Block

- A **Reductionist Entity** [Figure 16] that represents, with the right degree of abstraction, all physical entities (also aggregated) of the infrastructure.

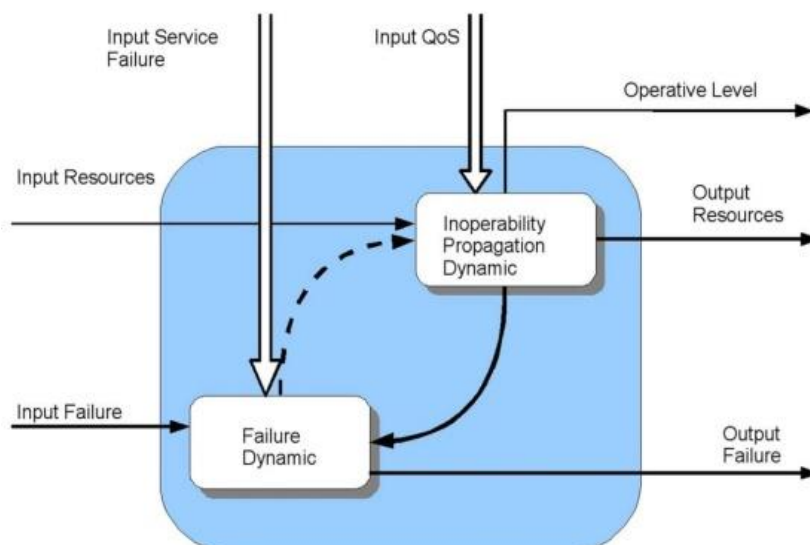


Figure 16 Reductionist Block

The actual state of the agent, in CISIApro, is summarized through the **Operational Level** concept [Figure 17]. The **Operational Level** can be defined as the ability of the agent to perform its required job; it is an internal measure of the potential production/service, if the operative level is 100% it does not mean that it is providing the maximum value but that it could, if necessary.

Agent inputs and outputs are necessary in order to perform interactions among agents. The Input/output can be:

1. Induced/propagated faults: faults propagated to the considered agent from its neighborhoods and from the considered agent to its neighborhood.
2. Input/output resources: amount of resources requested by/to other objects.

In CISIApro, the agent dynamic is described as an input/output model among the previously listed quantities. This description of agent's behavior is highly abstracted but it is enough rich to leave the experts to model the model dynamics in the most appropriate way.

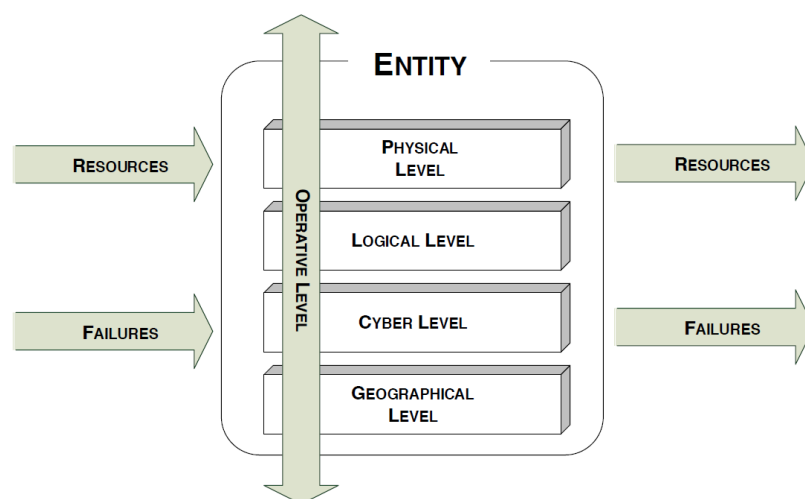


Figure 17 Generic entity representation

The relations among agents are based on their interdependencies, and they are described by incidence matrices. In fact, each matrix is able to spread a different type of interdependency, following the classical methodology among physical, geographical logic, and cyber connection [23]. Dependency and interdependency should be analyzed with respect to different dimensions. In particular, they catalogue dependencies into four, not mutually exclusive, classes:

- **Physical Dependency.** Two infrastructures are physically dependent if the operations of one infrastructure depends on the physical output of the other.
- **Geographical Dependency.** A geographic dependency occurs when elements of multiple infrastructures are in close spatial proximity. In this case, particular events, such as an

explosion or a fire in an element of an infrastructure may create a failure in one or more near infrastructures.

- **Cyber Dependency.** An infrastructure has cyber dependency if its state depends upon information transmitted through the ICT (Information and Communication Technology).
- **Logical Dependency.** Two infrastructures are logically dependent if their dependency is generated via control, regulatory or other mechanisms that cannot be considered physical, geographical or cyber.

At this point, we can imagine that all layers of the entity are crossed transversely by its **Operational Level** [see Figure 17]. In fact, the *Operational Level* represents the state of operability, its health and it is closely related to its capacity to provide or receive certain resources and thus the presence of certain faults. Usually, risk index is evaluated as a function of impact, threat and vulnerability:

$$Risk = Impact \times Threat \times Vulnerability$$

Typically, risk is, at least, a qualitative metrics, from the impact severity, the likelihood of occurrence or threat, and the vulnerability analysis. In CISIApro applications, the likelihood of occurrence is translated into the trust of the information. The operational level of each agent is associated to a risk level: the risk is the amount of harm due to specific events, such as a failure, and can be evaluated as:

$$Risk = 1 - Operative Level$$

where 1 is the maximum values of the operative level. A high value of operative level means a low risk. Therefore, the operational level represents a dynamic risk assessment considering the cascading effects of adverse events, i.e., natural disasters, failures or cyber-attacks.

6. SUMMARY AND CONCLUSIONS

The work presented in the report summarizes the current status of Task 2.3 at mid-interval. In order to fulfil the main goal of the task, providing a holistic socio-technical model of communication infrastructures, three main steps were identified:

1. A general review and assessment of modelling approaches.
2. The collection of necessary input to implement the models.
3. The implementation of approaches identified in step 1., based on input collected in step 2.

The assessment of modelling approaches was performed regarding the usability for RESISTO. Different modelling techniques, which were used historically and found in literature, were generally reviewed and brought into context of the risk and resilience management approach. In summary, conceptual models are needed for the context analysis and can provide a basis for setting up network models, which are needed for realistic network simulations. In addition, a graphical representation thereof is considered useful for a user friendly presentation of the network simulations.

Detailed information about telecommunication infrastructures is needed to realistically implement the network models. A general overview on LTE/4G and future network architectures is included in this report. The provision of specific network representations by the end users proved problematic due to confidentiality issues. Nevertheless, a collection of conceptual schemes and representations was gathered and is included. Furthermore, input from the operational partners is currently collected by other tasks and may contribute as additional source of information.

Finally, the technical implementation of the models and tools is addressed. This includes a comparison of available simulation software. A tool for network simulations by the partner RM3, which is already implemented and in use, is introduced.

The work, especially of steps 2. and 3. is ongoing. The next anticipated action points are discussed in the following subsection.

6.1. Next Steps

The collected information from the operational partners needs to be further evaluated:

1. Evaluation of the input provided by other tasks as introduced in Section 4.2:
 - a. Do we gain additional information from the interviews, e.g. additional information on modelling techniques used by the end users?
 - b. Can we incorporate information about the system components, provided by the tabular threat template?
2. Thorough inspection of the schemes provided in Section 4.3:
 - a. Are they usable by the partner in charge of model implementation, i.e. is additional information needed to understand and use them?
 - b. What are the differences between the infrastructures of different operators?
 - c. Is additional information needed that is not included in the current schemes?

The implementation of tools has partially started and needs to be refined:

3. Investigate further options and tools needed for the platform
 - a. Has RM3 all input needed for their simulation tool.
 - b. Has EMI all input needed for their simulation tool.
 - c. Are the end users requests and expectations of the platform covered? Are other model based tools needed?

7. REFERENCES

References

- [1] Häring I *et al* 2017 Towards a Generic Resilience Management, Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures, and Case Studies *Resilience and Risk (NATO Science for Peace and Security Series C: Environmental Security)* ed I Linkov and J M Palma-Oliveira (Dordrecht: Springer Netherlands) pp 21–80
- [2] Box GEP 1979 Robustness in the Strategy of Scientific Model Building *Robustness in Statistics* (Elsevier) pp 201–36
- [3] Ouyang M 2014 *RELIABILITY ENGINEERING & SYSTEM SAFETY* **121** 43–60
- [4] Chartrand G and Zhang P 2012 *A first course in graph theory (Dover books on mathematics)* (Mineola, N.Y.: Dover Publications)
- [5] Trudeau R J 2015 *Introduction to graph theory* ([s.l.]: PMA Publishing)
- [6] Barabási A-L and Pósfai M 2016 *Network science* (Cambridge, United Kingdom: Cambridge University Press)
- [7] Newman M E J 2015 *Networks: An introduction* 9th edn (Oxford: Oxford University Press)
- [8] Lee II E E, Mitchell J E and Wallace W A 2007 *IEEE Trans. Syst., Man, Cybern. C* **37** 1303–17
- [9] Wooldridge M J 2002 *Multi-agent systems: An introduction* (Chichester: Wiley)
- [10] Weingartner E, Vom Lehn H and Wehrle K 2009 - 2009 A Performance Comparison of Recent Network Simulators 2009 *IEEE International Conference on Communications ICC 2009 - 2009 IEEE International Conference on Communications (Dresden, Germany, 14.06.2009 - 18.06.2009)* (IEEE) pp 1–5
- [11] Patel R **2016**
- [12] Wang S-Y, Chou C-L and Yang C-M 2013 *IEEE Commun. Mag.* **51** 110–7
- [13] Wang S-Y 2014 - 2014 Comparison of SDN OpenFlow network simulator and emulators: EstiNet vs. Mininet 2014 *IEEE Symposium on Computers and Communications (ISCC) 2014 IEEE Symposium on Computers and Communication (ISCC) (Funchal, Madeira, Portugal, 23.06.2014 - 26.06.2014)* (IEEE) pp 1–6
- [14] Fred S B, Bonald T, Proutiere A, Régnié G and Roberts J W 2001 *SIGCOMM Comput. Commun. Rev.* **31** 111–22
- [15] B. Chandrasekaran *Survey on Network Traffic Models* https://www.cse.wustl.edu/~jain/cse567-06/traffic_models3.htm
- [16] Mohamed, Ahmed & Agamy, Adel 2011 *International Journal of Computer Networks*
- [17] Boussada M E H, Frikha M and Garcia J M 2015 - 2015 Flow level modelling of Internet traffic in Diffserv queuing 2015 *5th International Conference on Communications and Networking (COMNET) 2015 5th International Conference on Communications and Networking (COMNET) (Tunis, Tunisia, 04.11.2015 - 07.11.2015)* (IEEE) pp 1–7
- [18] Vargas-Munoz M J, Martinez-Pelaez R, Velarde-Alvarado P, Moreno-Garcia E, Torres-Roman D L and Ceballos-Mejia J J 2018 - 2018 Classification of network anomalies in flow level network traffic using Bayesian networks 2018 *International Conference on Electronics, Communications and Computers (CONIELECOMP) 2018 International Conference on Electronics, Communications and Computers (CONIELECOMP) (Cholula, 21.02.2018 - 23.02.2018)* (IEEE) pp 238–43
- [19] O. Lemeshko, A. M. Hailan and A. S. Ali 2010 225
- [20] Millán G and Lefranc G 2013 *Procedia Computer Science* **17** 420–5
- [21] Foglietta C, Palazzo C, Santini R and Panzieri S 2015 Assessing Cyber Risk Using the CISI Apro Simulator *Critical Infrastructure Protection IX (IFIP Advances in Information and Communication Technology)* ed M Rice and S Shenoit (Cham: Springer International Publishing) pp 315–31

- [22] Porcellinis S D, Panzieri S and Setola R 2009 *IJCIS* **5** 86
- [23] Rinaldi S M 2004 - 2004 Modeling and simulating critical infrastructures and their interdependencies *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the (Big Island, HI, USA, 08.01.2004 - 08.01.2004)* (IEEE) 8 pp