

RESISTO:

D2.5_TELECOMMUNICATION SYSTEM MODEL AND INTERFACES - FINAL



RESISTO

D2.5 – TELECOMMUNICATION SYSTEM MODEL AND INTERFACES - FINAL

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_D2.5_190524_01	Version:	1.0
Deliverable:	D2.5	Date:	24/05/2019
		Status:	APPROVED

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

Approval Status	
Prepared by:	Mirjam Fehling-Kaschek, Katja Faist (Fraunhofer)
Approved by: (WP Leader)	Zhan CUI (BTC)
Approved by: (Coordinator)	Bruno SACCOMANNO (LDO)
Advisory Board Validation (Advisory Board Coordinator)	NA
Security Approval (Security Advisory Board Leader)	Alberto BIANCHI (LDO)

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Mirjam Fehling-Kaschek, Jörg Finger, Katja Faist Natalie Miller	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	Contributor
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
0.8	29.03.2019	All	All	Document released
0.9	03.04.2019	All	All	Release for SAB Review
1.0	24.05.2019	All	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 results 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 the mid-version deliverable (D2.4). In this final version of the deliverable, a collection of testbeds constructed by the end-users is included. These testbeds are realistic environments for applying the built models later in the project. Finally, first details regarding the software implementations are presented.

CONTENTS

ABBREVIATIONS	10
1. INTRODUCTION [EMI]	13
2. RISK AND RESILIENCE MANAGEMENT [EMI]	14
3. ASSESSMENT OF MODELLING APPROACHES REGARDING THEIR USABILITY FOR RESISTO [EMI]	17
3.1. Conceptual models [EMI]	17
3.1.1. OSI model	18
3.1.2. SysML	19
3.2. Network/graph models [EMI]	20
3.2.1. Topological models	20
3.2.2. Flow based models	20
3.2.3. Multi Agent Systems	21
3.3. Geospatial representations [RM3]	21
4. ACQUISITION OF DETAILED MODEL SPECIFICATIONS	22
4.1. Network architectures [TEI]	22
4.1.1. 4G/LTE mobile networks	22
4.1.2. Future network architecture (Ericsson View)	24
4.2. Input collected via other tasks [EMI]	27
4.2.1. Information provided by guided interviews (Task 2.1)	27
4.2.2. Information provided by Excel template for threat list (Task 2.2)	27
4.2.3. Evaluation of Input	29
4.3. Testbed Description [ORO, OTE, BTC, TIM, ALB, RTV]	33
4.3.1. ORO Testbed	33
4.3.1. ORO Testbed	34
4.3.2. OTE Testbed	41
4.3.3. BTC Testbed	44
4.3.4. TIM Testbed	46
4.3.5. ALB Testbed	48
4.3.6. RTV Testbed	51
5. IMPLEMENTATION OF TOOLS	54
5.1. Network simulators [RM3]	54
5.1.1. Key concepts	54
5.1.2. Software packages	55
5.1.3. Network traffic models	56

5.2.	Mixed Holistic Reductionist – CISI Apro modelling approach [RM3]	56
6.	SUMMARY AND CONCLUSIONS [EMI]	63
7.	REFERENCES	64

ABBREVIATIONS

2G, 3G, 4G, 5G	Second, third and fourth generation of mobile phone systems
3GPP	3rd Generation Partnership Project
1G, 10G	1 Gbps, 10 Gbps
ACL	Access Control List
API	Application Programming Interface
B2B	Back-to-Back gateway
BIGIP	Web Application Firewall (F5 Networks)
BNG	Border Network Gateway
DAB	Digital Audio Broadcasting
DLP	Data Loss Prevention
DVB	Digital Video Broadcasting
eMMB	Enhanced Mobile Broadband
EoMPLS	Ethernet over MPLS
EU	European Union
FDD	Frequency Division Duplex
GNS3	Graphical Network Simulator
GUI	Graphical User Interface
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IOS	Internetwork Operating Systems (Cisco)
IoT	Internet of Things
IPS	Intrusion Prevention System
ISI	Inter System Interface

LDP	Label Distribution Protocol
LTE	Long Term Evolution (= 4G)
LTS	UBUNTU server specific named version
MME	Mobility Management Entity
mMTC	Massive Machine Type Communication
MPLS	Multiprotocol Label Switching
MTC	Machine Type Communication
NFV	Network Functions Virtualization
OAI	Open Application Interface
OFDM	Orthogonal Frequency-Division Multiplexing
OLT	Optical Line Termination
OS	Operating System
PC	Personal Computer
PE	Provider Edge
PGW	Packet Data Network Gateway
PoC	Proof of Concept
QAM	Quadrature amplitude modulation
QoS	Quality of Service
QPSK	Quadrature phase-shift keying
RAN	Radio Access Network
RRC	Radio Resource Controller
RRU	Remote Radio Unit
SDN	Software Defined Networking
SGW	Serving Gateway
SPGW	Serving Gateway/PDN Gateway
TCP	Transmission Control Protocol
TDD	Time Division Duplex
UE	User Equipment

URL	Uniform Resource Locator
URLLC	Ultra-Reliable and Low Latency Communications
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
WP	Work Package

1. INTRODUCTION [EMI]

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 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. All partners participating in this task were asked for missing modelling approaches or further input regarding the acceptance, especially in view of telecommunication networks. We received no request for evaluation of further approaches.

Section 4 gathers specific input for the setup and implementation of the telecommunication model. To gain relevant and tailored information, direct input as well as testbed descriptions 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.

2. RISK AND RESILIENCE MANAGEMENT [EMI]

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

The modelling of the communication infrastructures can serve as an input for several steps in the resilience management cycle, in particular Step 2 and Steps 6 to 9. The most prominent parts where system modelling 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**

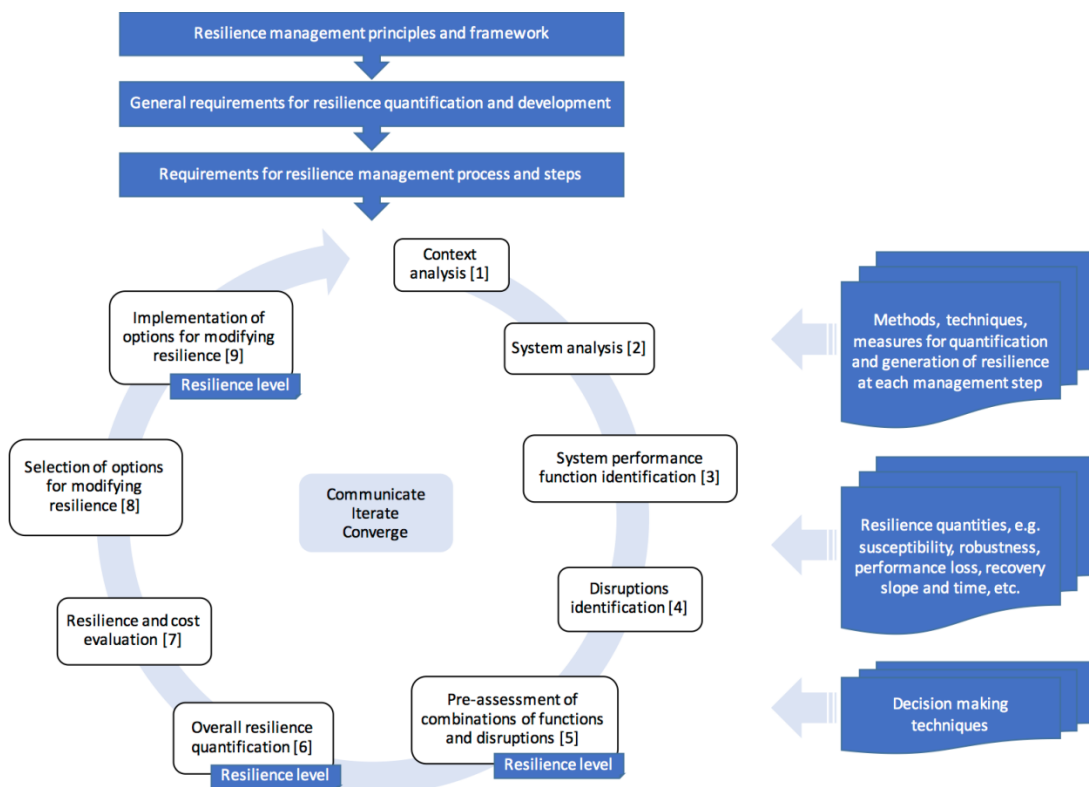


Figure 1: Generic resilience management process that consists of 9 steps and covers resilience quantification and development [1].

Figure 2 compares the resilience management process to the risk management steps as defined by ISO 31000 (2018). Both processes have the same structure each containing an assessment and a need for communication, consultation, monitoring, reviewing, recording and reporting. The risk management process contains only five steps: establishing the context and then identifying, analysing, evaluating and treating any risks. The resilience management process contains the same nine steps mentioned above, separating Steps 3 through 8 into a resilience assessment. Information within each process can be shared between the two.

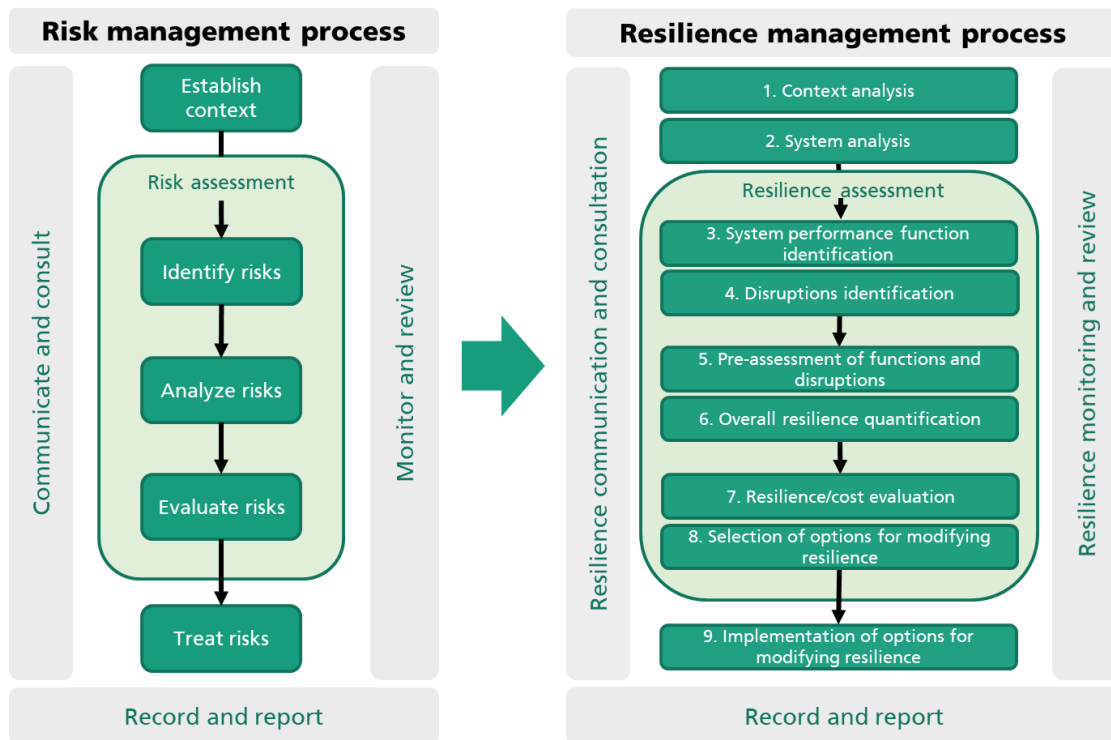


Figure 2: The resilience management process based off of ISO 31000 (2018).

3. ASSESSMENT OF MODELLING APPROACHES REGARDING THEIR USABILITY FOR RESISTO [EMI]

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 [EMI]

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 3 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.

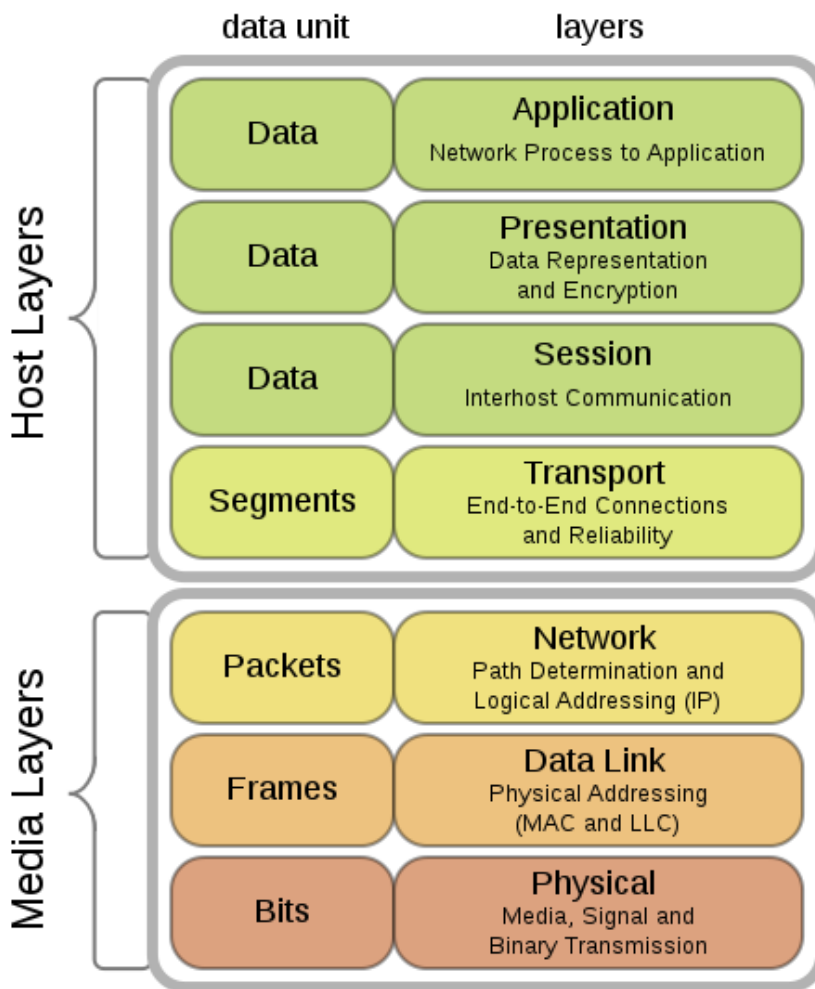


Figure 3: The seven layers defined in the OSI model
 (https://commons.wikimedia.org/wiki/File:OSI_Model_v1.svg - By Offnfopt [Public domain or CC0], from Wikimedia Commons)

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 behaviour 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 [EMI]

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 [RM3]

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 [TEI]

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. As seen in Figure 4, 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.

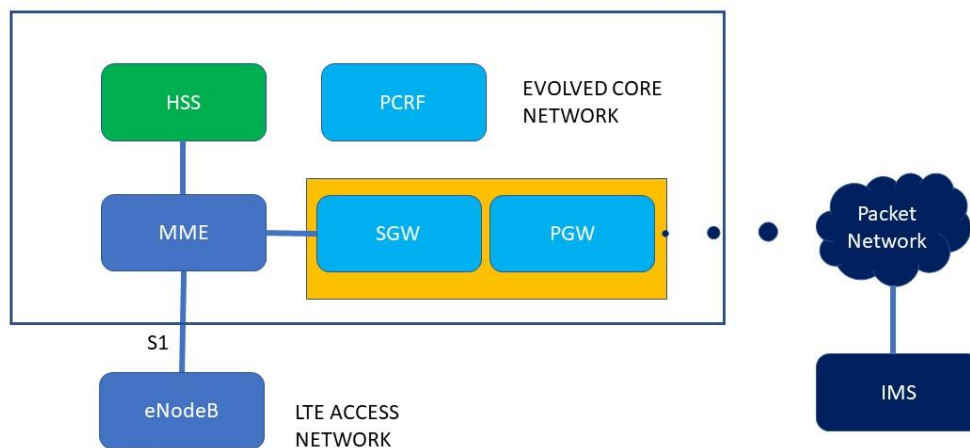


Figure 4: An example of a 4G architecture design.

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)

Figure 5 is an example of a global architecture for future networks. This architecture has vertical and horizontal domains that are described below.

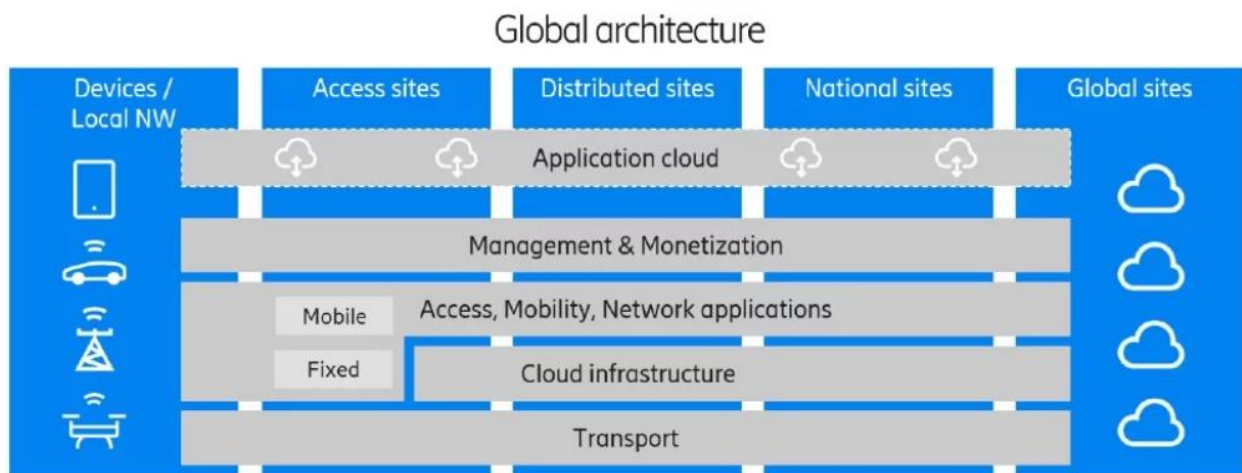


Figure 5: A global architecture design for future networks.

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, as seen in Figure 6, must be fulfilled by the future network architectures. These requirements can be grouped into:

- 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.

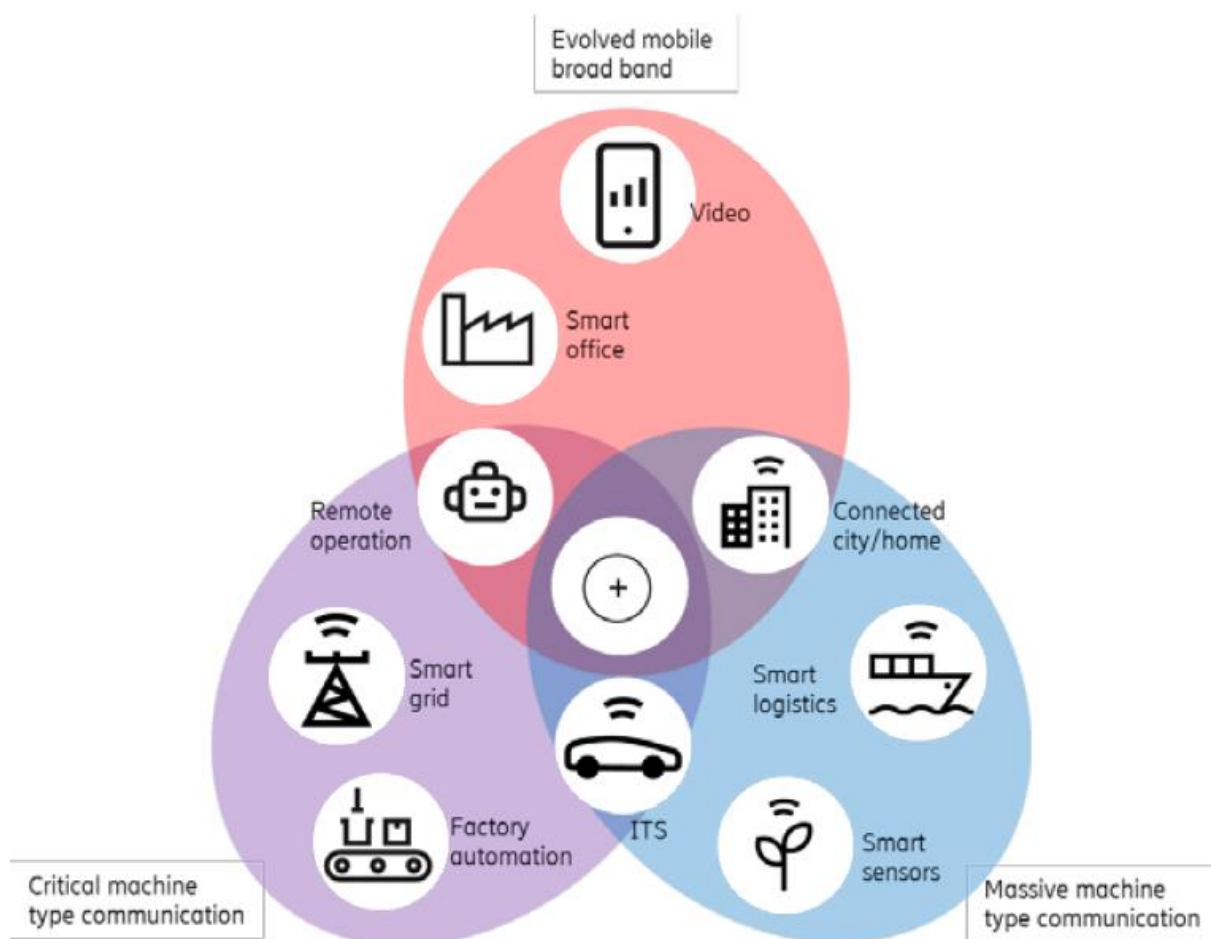


Figure 6: Future network requirements

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. An example of a 5G core architecture is seen in Figure 7.

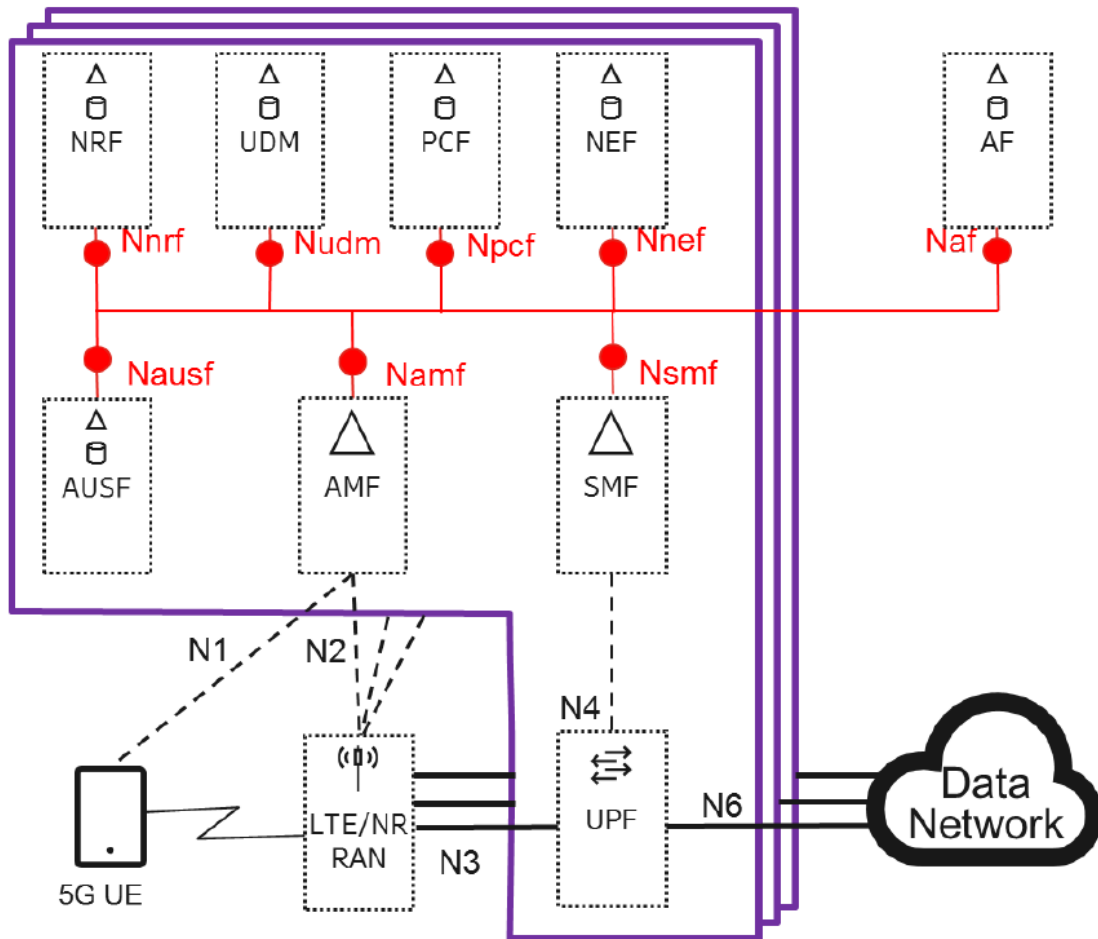


Figure 7: 5G core architecture

4.2. Input collected via other tasks [EMI]

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. A summary of the information collected in the interviews is given in D2.1.

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 8.

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

Figure 8: 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 reports for Task 2.2: *D2.2/D2.3 Cyber-physical threat/risk scenarios and pre-assessment*.

4.2.3. Evaluation of Input

In this section, the input provided by the Excel template (see section 4.2.2) is evaluated and shown. This input will be needed for feeding the simulation tools provided during the RESISTO project.

First, the system components are evaluated and second, the system functions. The system components are needed to support the network model for the computer simulation and to support the impact estimation for threats and mitigation options. An example for the gathered system components is shown in Figure 9. It shows different system components with their descriptions, corresponding subsystems, type, quantity, technical characteristics and possible interconnections to other system components. These interconnections are needed for providing a realistic system model with realistic dependencies between the different system components. Figure 10 shows the system components for each operator registered in the excel sheet. Figure 11 gives an overview on the assignment of system components to the subsystems. It shows that the system consists of many hardware components.

ID	Name	Description	Subsystem	Type	Quantity	Technical characteristics	Interconnections
SC1	Border Routers	Carrier Grade routers, provides resources access to subscribers	Core Network	Hardware Device	3	CISCO Carrier Grade Routers, 9000-Series	Workstations and Servers, Network Security Equipment, FO Infrastructure
SC2	FO Infrastructure	Fiber Optics Infrastructure	Optical Network	Interconnection	7548 km owned FO	Buried or aerial installation fiber optic cable. Transport technologies used are: DWDM or Gigabit Ethernet over fiber.	Border Routers, MSC, Radio Infrastructure
SC3	Mobile Switching Centers (MSC)	Primary service delivery nodes for GSM/CDMA, responsible for routing voice calls and SMS as well as other services	Core Network	Hardware Device	3 MSCS/7MGW	Ericsson MSCS: circuit-switched calling mobility management and GSM services to the mobile phones Ericsson MGW: conversion between different transmission and coding technique	FO Infrastructure, Border Routers
SC4	Radio Infrastructure (BTS, BSC, RNC, NodeB)	Provides radio connectivity for legacy (2G + 3G) and 4G services (voice and data)	Radio Network	Hardware Device	N/A		Border Routers, FO Infrastructure
SC5	Network Security Equipment (IPSs, FWs)	Deployed network security infrastructure including Firewalls, IPS, WAFs etc.	Core Network	Hardware Device	5: Mobile Services 2: Fixed Internet Services for Corporate customers	Fortinet Next-Gen Firewalls with UTM capabilities	Border Routers, Workstations and Servers, Applications
SC6	Workstations and Servers	All servers, internal and public - facing, all end-points in one of the Microsoft Security Domains	Internal Network	Hardware Device	N/A	Microsoft Windows PCs, Microsoft Windows Servers and various CentOS/RHEL Servers running on bare iron or in VMs	Border Routers, Network Security Equipment, Microsoft Security Domain
SC7	Microsoft Security Domain	All devices, users, policies and data in one of the Microsoft Windows Security Domains	Internal Network	Software Tool	x	MSAD + Windows Professional workstations	Network Security Equipment, Workstations and Servers, Border Routers
SC8	Business Applications	Applications such as SSO/Multi Authentication tool, Databases, Internal Webservers (Intranet), Billing Apps, Monitoring apps, VPN access etc.)	Applications	Software Tool	N/A	Various Business Apps based on technologies such as Databases, Database Connectors, Java, APIs etc.	Workstations and Servers, Microsoft Windows Security Domain, Border Routers
SC9	Equipment Shelters	Build structures that houses and provides weather and human-tampering protection to sensitive equipment	Radio Network	Built structure	N/A	Built structures that houses various equipment	Radio Infrastructure, FO Infrastructure
SC10	Mobile Core Network		Core Network	Hardware Device	11		FO Infrastructure, Radio Infrastructure

Figure 9: System components list gathered by the excel template

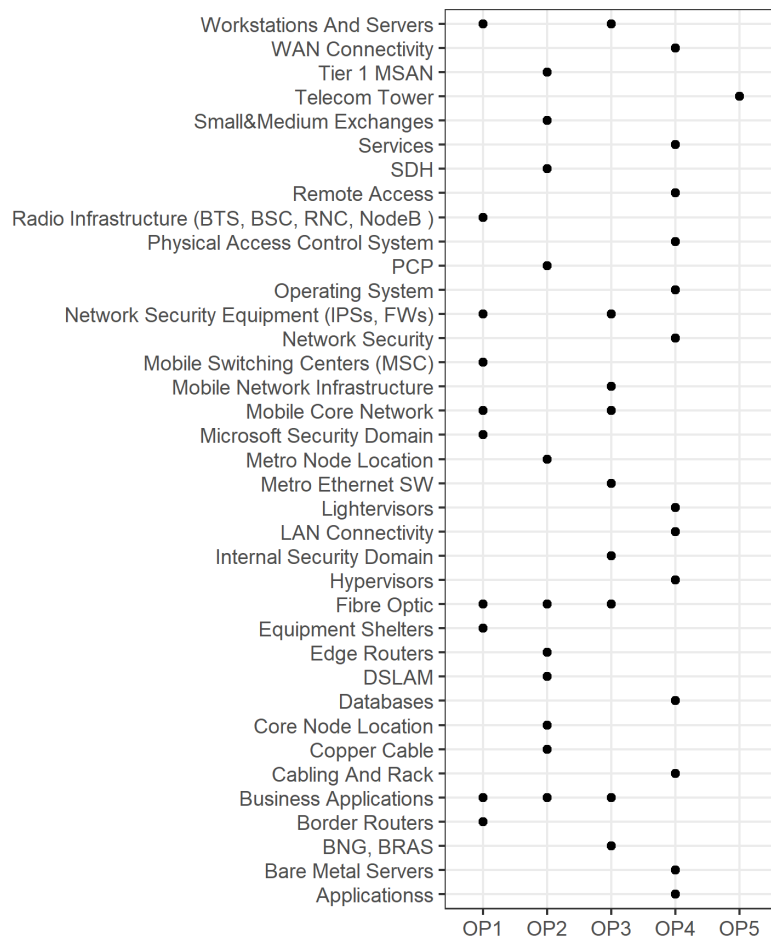


Figure 10: System components per operator.

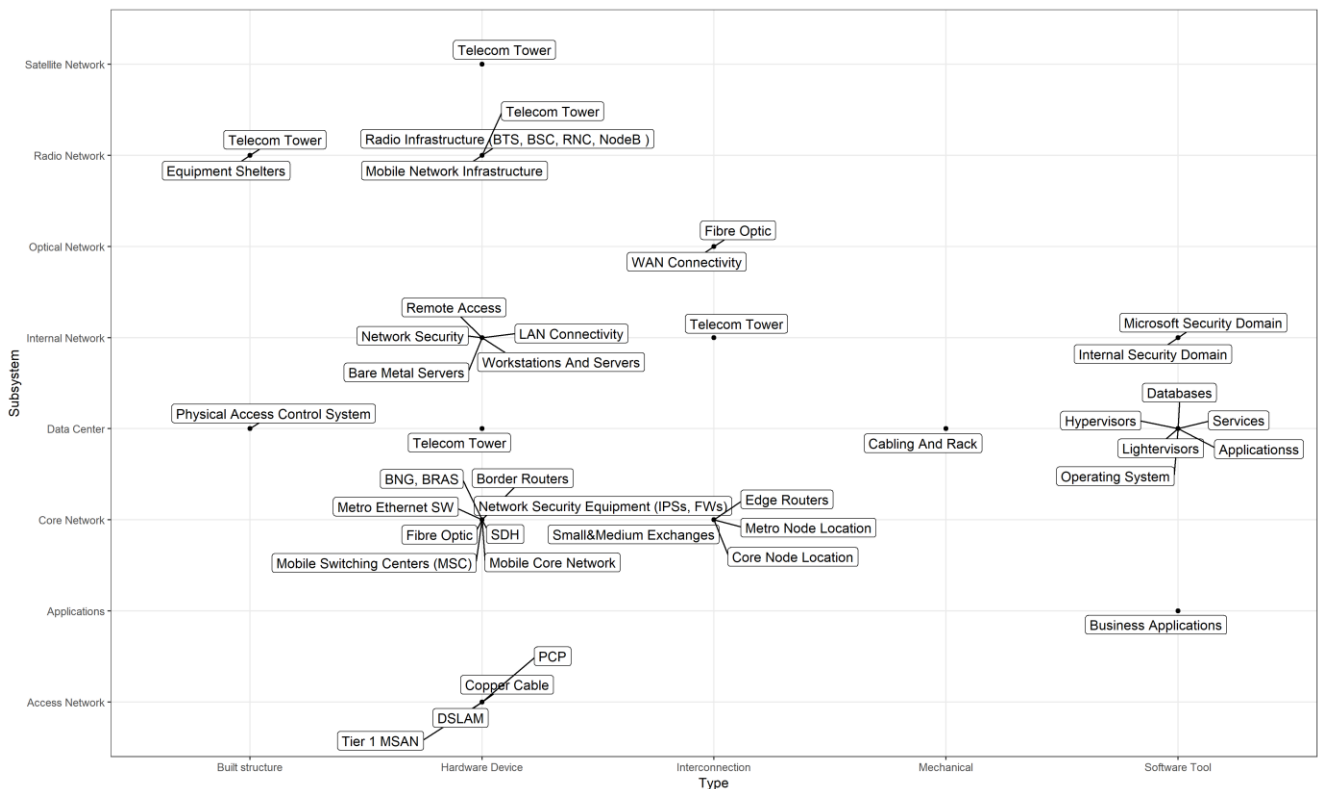


Figure 11: Assignment of system components to subsystems

The system functions are needed for resilience quantification. An example for the gathered system functions is shown in Figure 12. Different system functions with their descriptions, names, corresponding subsystems and performance quantifications are gathered. Beyond, the figure shows linked system components, i.e. which system components shown above are linked with the mentioned system function. Furthermore, system functions can also depend on other system functions, which is also represented by the designed excel sheet. This linkages will be used for modelling dependencies and delegate system failures. Furthermore, the resilience of the telecommunication system towards disruptive events can be evaluated. This part of the excel sheet covers the expected system behaviour and its assessment and contains quantitative and qualitative descriptions. The system behaviour is important for defining later in the project the key performance indicators (Task 3.4). Figure 13 shows the system functions registered in the excel template for each operator.

ID	Name	Description	Subsystem	Linked Components	Performance Quantification	Dependence of other SFs
SF1	Authentication and Authorization	Identify a person/technician and authorize the access	Data Center	SC1	open the door in less than a second	
SF2	L2 (Site-to-Site) connectivity	* establish a backend network to connect datacenters * provide redundant Internet access	Optical Network; Data Center	SC2	metrics: throughput, latency, round-trip delay, packetloss	SF4
SF3	L3 connectivity	provide connectivity for end user terminal, IoT devices, m2m, services and servers	Internal Network; Data Center	SC3; SC4	metrics: throughput, latency, round-trip delay, packetloss	SF2; SF4
SF4	L1 connectivity	* Physical connectivity between sites * Physical internal connectivity * Equipment assemble (inside rack)	Optical Network	SC4; SC3; SC2		
SF5	Remote Access and Extranets	* Provide access to external users * Extend connectivity by establishing site-to-site tunneling/circuits	Optical Network; Data Center; Applications; Internal Network	SC2; SC3; SC4; SC6		SF6; SF4; SF3; SF2
SF6	Network Security services	* network virtualization	Optical Network; Data Center; Internal Network	SC5; SC4; SC3; SC2		SF2; SF3; SF4
SF7	Cloud services	* automated bare metal server provision * automated virtual machines provision * automated container deployment * network virtualization * storage virtualization	Data Center; Internal Network	SC7; SC8; SC9; SC10	Monitoring services for: * vCPU and RAM usage, Disk IO, Network IO	SF6; SF4; SF3; SF2
SF8	Bearer network services	Name Resolution (DNS), IP address assignment (DHCP), User Control and Policy (DC), Directory Services (X.500)	Data Center; Internal Network	SC6; SC4; SC3	Metrics: * requests/sec	SF7; SF6; SF4; SF3; SF2
SF9	Database services	Database engine for data storage, manipulation and ETL	Data Center	SC11; SC9; SC8; SC7; SC6	Metrics: * requests/sec * % volume data grow	SF8; SF7; SF6; SF4; SF3; SF2
SF10	Applications	* Corporate Applications * OSS Applications * BSS Applications	Applications	SC12; SC11; SC10; SC9; SC8; SC7; SC6; SC4; SC3	Metrics: * requests/sec * % volume data grow	SF9; SF8; SF7; SF6; SF4; SF3; SF2

Figure 12: Example for system functions with their relevant values.

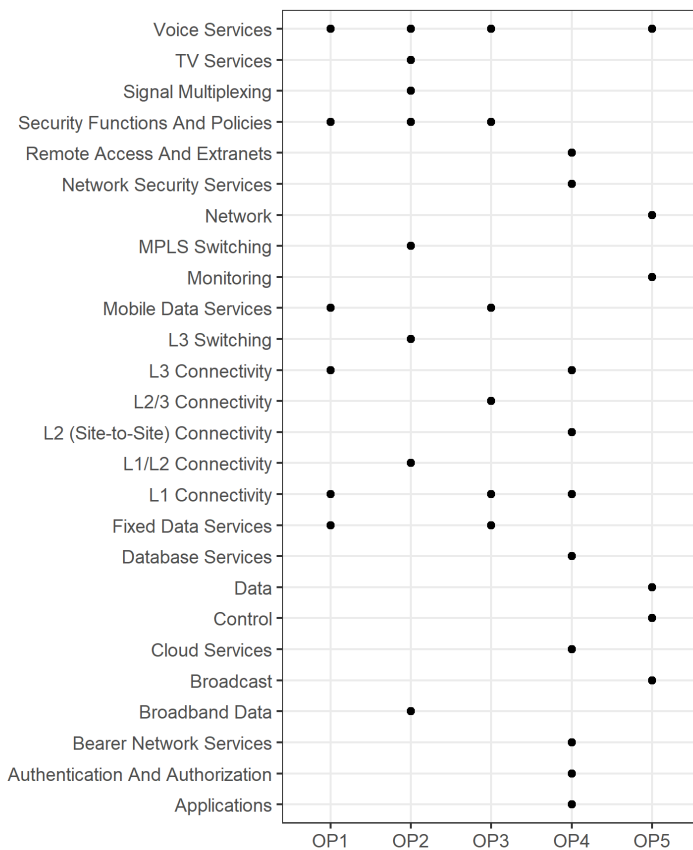


Figure 13: System functions registered in the excel file divided by operator.

Based on the gathered information, the model in the EMI simulation tool CaESAR can be extended and telecommunication networks can be integrated. CaESAR simulates networks and their dependencies as well as interdependencies for resilience analysis. For this simulation as first step the system components and the system functions described above are needed.

4.3. Testbed Description [ORO, OTE, BTC, TIM, ALB, RTV]

Testbeds can be used during the design phase of telecommunication networks as a way to complete testing and analysis on a smaller scale. The testbeds can be tested with a multitude of attacks including cyber, security and physical.

4.3.1. ORO Testbed

Testbeds can be used during the design phase of telecommunication networks as a way to complete testing and analysis on a smaller scale. The testbeds can be tested with a multitude of attacks including cyber, security and physical.

4.3.1. ORO Testbed

Orange Romania Use case is described in Figure 14 and all the test infrastructure components needed to cover the test scenarios and activities that will be detailed in D2.8 are described in this chapter.

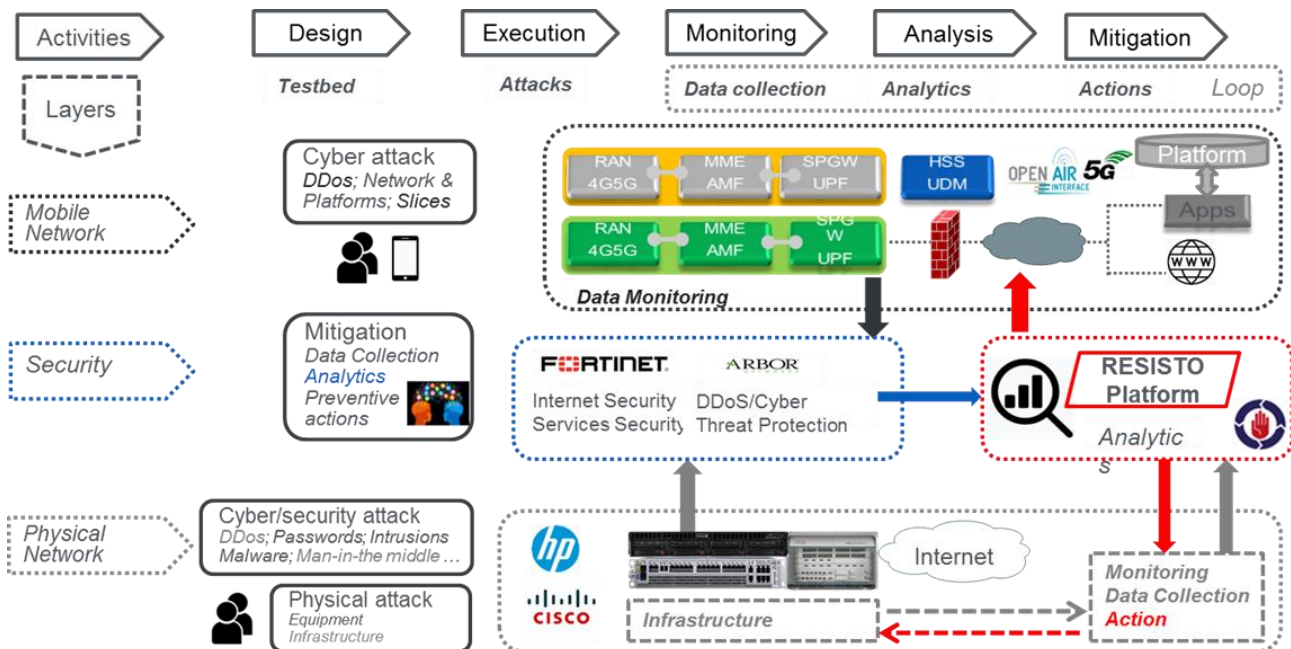


Figure 14: Orange Romania's use case general set up

Orange Romania's test bed is designed to include as many elements from the real network infrastructure as possible, thus replicating most of the core network functionalities and services.

The test infrastructure could be configured to obtain two variants of physical layouts in order to address all the test scenarios from ORO's use-case that are detailed in D2.8 deliverable

The test infrastructure contains various network elements, ranging from high speed backbone routers to mobile and B2B access routers and dedicated virtualized infrastructure, Openstack based and ETSI MANO orchestrated, supported by several capable compute nodes and shared storages. On the virtualized infrastructure, there are deployed specific mobile core network components and IoT platforms, in an initial phase 4G network elements and later the new and novel 5G CN. The deployed virtualized infrastructure will provide the possibility to connect several UEs and IoT devices to the network, enabling the possibilities to perform mobile networks attacks, DDoS through the network platforms inside the 5G slices.

The first physical layout, where all networking devices are interconnected via switches, is detailed in Figure 15. This figure describes a fully functional MPLS network. All the networking devices are aggregated using high speed links on the pair of Nexus switches – thus giving the testing engineers very high flexibility to deploy new designs in a very short amount of time, with no additional physical cabling – all with the usage of 802.1Q (VLAN) tagging.

The MPLS Layer contains PE routers from a wide range that are used to deliver backbone functionality (P Routers), mobile PE Router and B2B PE Routers. MPLS network will run LDP and IS-

IS as the underlay routing protocol and use various QOS mechanisms to emulate a real deployment. Services delivered across the MPLS network include MPLS Layer 3 VPNs, MPLS Layer 2 VPNs (both VPLS and EoMPLS). MPLS network will also include a pair of Route Reflectors for L3 and L2 VPNs autodiscovery.

MPLS Network will also integrate an OLT to simulate an attack/outage on the part of subscriber network.

The security fabric and datacenter layer is achieved using a few next-generation security equipment and application delivery controllers like:

- Fortinet FortiGate
 - o URL Filtering
 - o Centralised Antivirus
 - o IDS and IPS
 - o DLP
 - o E-mail filtering
 - o Layer 4 Firewall
- F5 BIGIP
 - o Web Application Firewall
 - o Enhanced application layer enrichment and protection

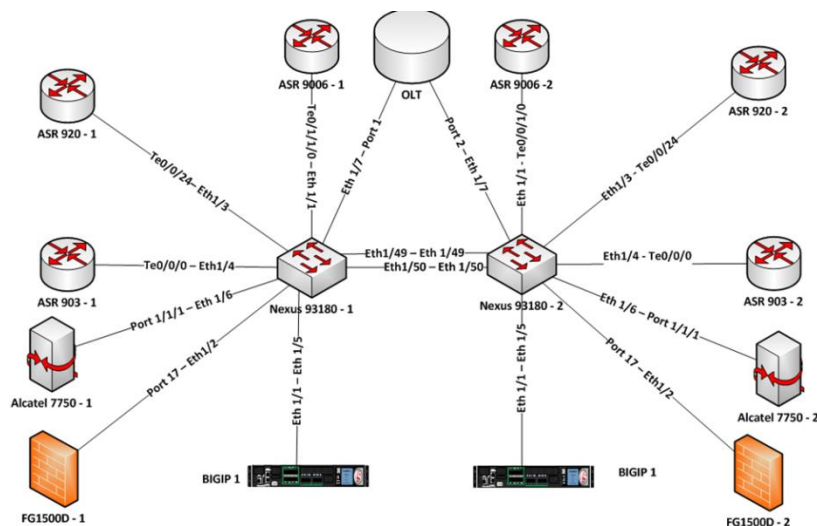


Figure 15: Physical layout of a MPLS network testbed with the elements connected with Nexus switches.

The following mapping can be used in order to link the described elements to the elements presented in Figure 15:

- The two Nexus switches are only used for physical – Layer 1 – connectivity. From a service provider perspective – you can view them as cables interconnecting the various equipments.
- The following elements (routers) will form a fully functional MPLS Network :
 - ASR9006

- ASR920
- ASR903
- Alcatel 7750
- Cisco 7600
- From an MPLS perspective the following mapping will be used :
 - ASR 9006 – Datacenter Gateway Routers / PE Routers + Route Reflectors
 - ASR 920 – Mobile Network Access Router / PE Router
 - ASR 903 – Mobile Network Distribution Router / PE Router
 - Cisco 7600 – Fixed B2B client distribution router / PE Router
 - Alcatel 7750 – Mainly P Backbone Routers
 - OLT – Non-MPLS Broadband client aggregation
 - F5BIGIPs – Non-MPLS application delivery controllers in the Datacenter
 - FG1500 Firewalls – Non-MPLS next generation firewalls in the Datacenter
- From a Datacenter Perspective – all the servers can run either VMWare vSphere or Openstack virtualization technologies .
- Services such as MPLS Layer 3 or Layer 2 VPNs can be delivered between/from any PE router described above.

Figure 16 is the second physical layout option. Access routers and border/core routers are directly interconnected, in order to assure the testing of Fiber-cut scenario, which is very often encountered in our production network and is included in the Hazards Excel Template. Moreover other physical security scenarios that imply damage of physical connections could be tested using this design, according to the final list and the details of test scenarios detailed in D2.8. The testbed also includes various servers which run VMWare and Openstack hypervisors for virtualized solutions and datacenter services emulation.

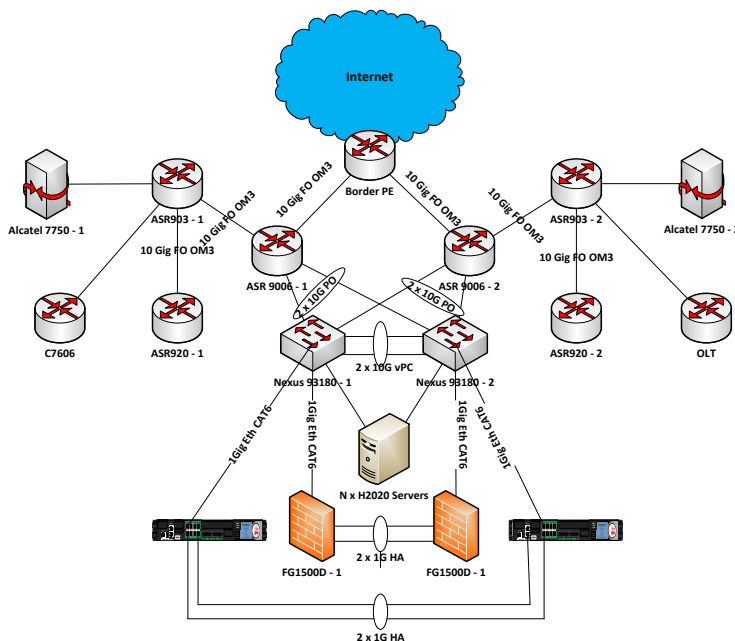


Figure 16: Another physical layout design for a testbed that is better for testing physical attacks

The purpose of the servers is also to deploy the necessary infrastructure components for Cockpit and Long-term/Short-term control Loop. Figure 17 shows the server set up while Figure 18 displays the overall logical design.

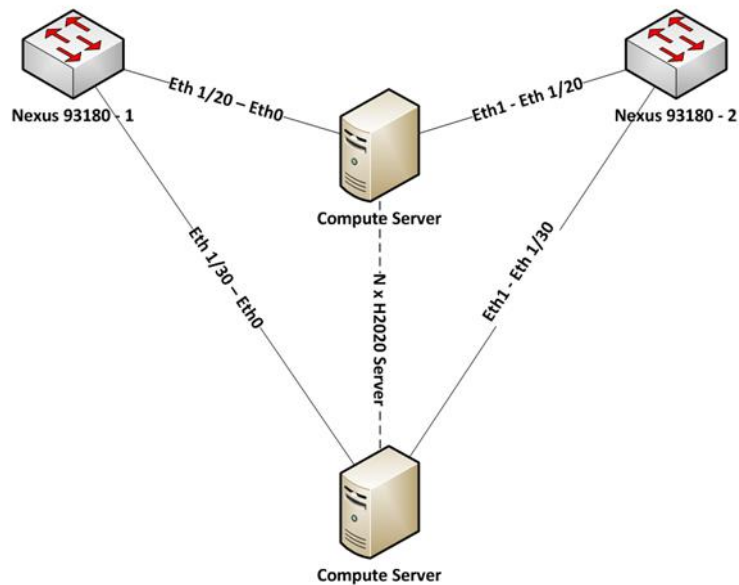


Figure 17: Server set up

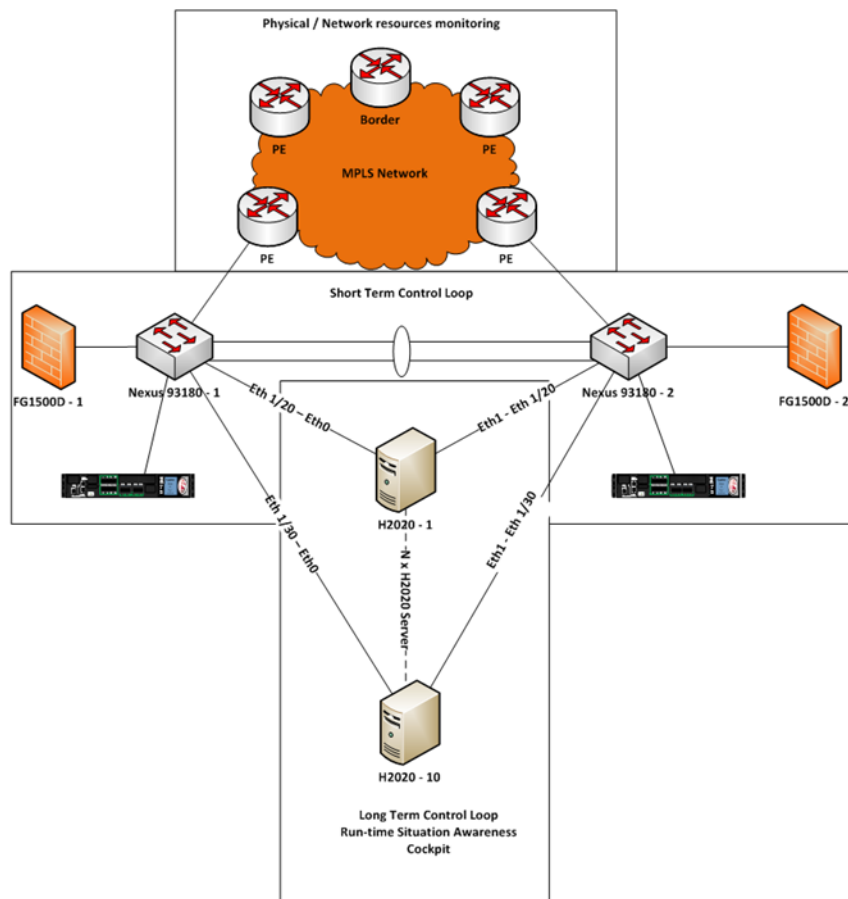


Figure 18: The overall logical design

Most RESISTO components (COCKPIT, some parts of SHORT TERM CONTROL LOOP, LONG TERM CONTROL LOOP) will be deployed in a virtualized environment over Openstack or VMWare – giving the test engineers the possibility to scale-out different components both vertically (grow a single VMs resources) and horizontally (deploy more instances of the same type of VM).

The test scenarios involving the Mobile Network, will be demonstrated in a test virtualized 4G/5G environment as depicted in Figure 19.

The test mobile infrastructure is comprising 4G virtualized components, the 5G ones being available in 2-3 months,. There will be used developed users simulations appsthat will also permit to simulate attacks on IoT infrastructure and core network via 4G/5G technologies.

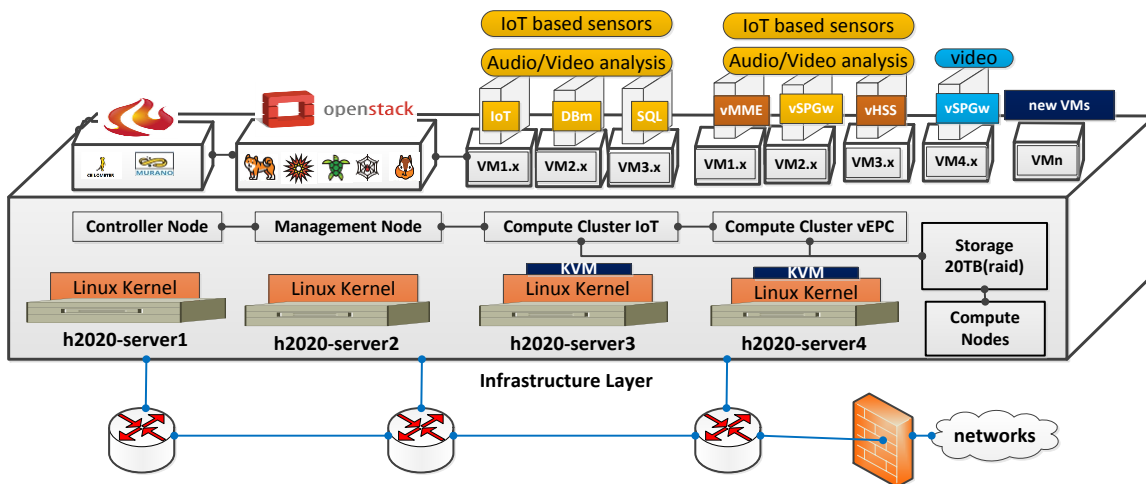


Figure 19: Testing infrastructure for the mobile network

The IoT sensors are dedicated IoT devices like IoT lighting poles for smart-lighting systems, IoT energy measurements devices and the audio/video devices are capable video-camera that have eMBB dedicated transport resources, communicating with analytics server in the MEC, through dedicated network slice, exposed to the network attacks.

The next figure provide a high level detailed design for the existing virtualized core network infrastructure, 4G vEPC and RAN network element, for the MME, HSS and SP-GW and the eNodeB configured through OAI software with the BBU on a physical linux machine and the RRU the USRP. All the virtualized network element components are instantiated, orchestrated and monitored through the Openstack deployments. Several virtualized networks will be deployed for each attack scenario, the networks being isolated one-of the other, through metrics collection capable software(Ceilometer and Prometheus), the data may be exposed to upper RESISTO analytics layers.

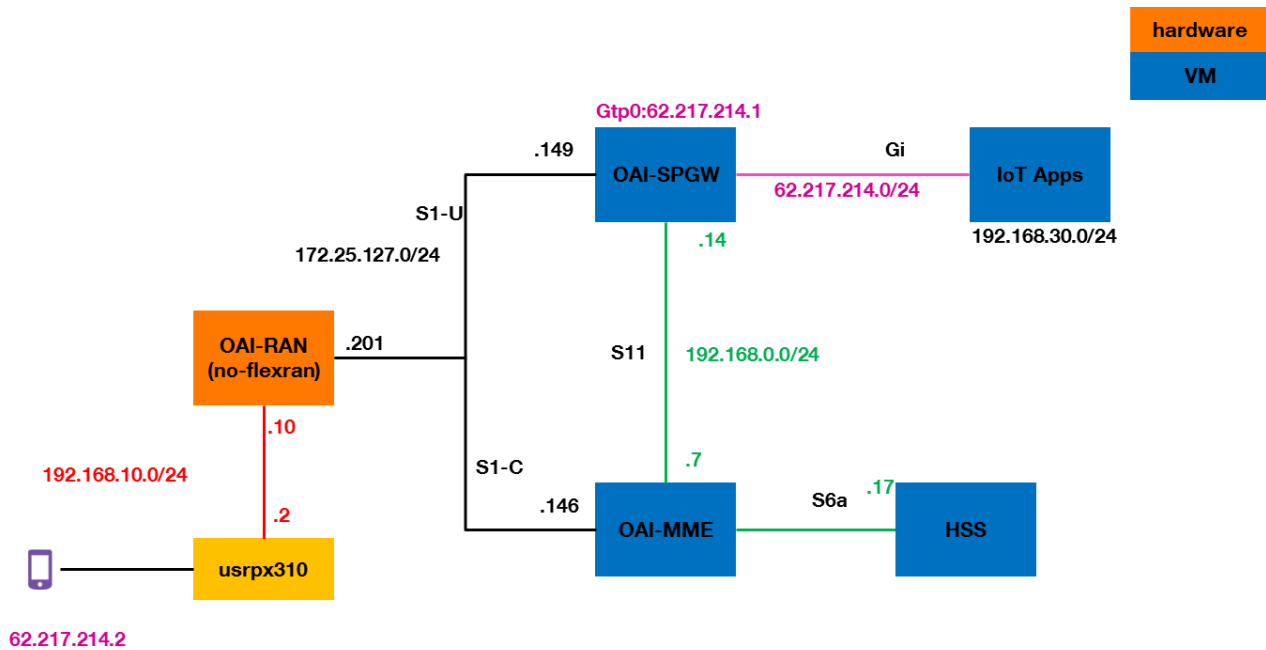


Figure 20: Physical configuration of OAI-RAN

Figure 21:Physical configuration of OAI RAN RRU

In the Hazards Excel Template provided by Orange, there are 10 System Components from the production network infrastructure that were identified and are providing system functions that could be affected by different hazards. From the 10 system components mentioned, the following are encountered or could be simulated in the testbed:

- SC1- Border Routers
- SC3- Mobile Switching Centers
- SC4- Radio Infrastructure
- SC5- Network Security Equipment
- SC6- Workstations and Servers

- SC9- Equipment Shelters (racks, testbed room)
- SC10- Mobile Core Network

Figure 22 shows the distribution of testbed devices in racks, also the equipment's connectivity to power supply is specified.

RACK 1					RACK 2					RACK 3				
U	PCB	Equipment type	PCB	PW (W)	U	PCB	Equipment type	PCB	PW (W)	U	PCB	Equipment type	PCB	PW (W)
				(C13)					(C13)					(C13)
42					42					42				
41		ODF (Optical Distribution Frame)			41		ODF (Optical Distribution Frame)			41		ODF (Optical Distribution Frame)		
40					40					40				
39		Patch Panel for copper Ethernet			39		Patch Panel for copper Ethernet			39		Patch Panel for copper Ethernet		
38					38					38				
37					37					37				
36					36					36				
35					35		LAB H2020 server1 - 1 HPE PROLIANT DL380 8th Generation		x	35		LAB FG 1500D-1	404	x
34					34		LAB H2020 server2 - 1 HPE PROLIANT DL380 8th Generation			34		LAB FG 1500D-2	404	
33					33		LAB H2020 server3 - 1 HPE PROLIANT DL380 8th Generation			33		LAB BIGIP-1	300	x
32					32		LAB H2020 server4 - 1 HPE PROLIANT DL380 8th Generation			32		LAB BIGIP-2	300	x
31					31					31				
30					30		LAB H2020 ssa - 1 HPE STOREEASY 1860			30				
29					29					29				
28					28					28				
27					27					27				
26					26					26				
25					25		LAB Nexus 93180-1		x	25		LAB Alcatel 7750 - 1	1.500	x
24					24		LAB Nexus 93180-2			24				
23					23					23		LAB Alcatel 7750 - 2	1500	
22					22					22				
21					21					21				
20					20					20				
19					19		LAB Mistral			19		Nexus 93180	500	
18					18		LAB LII Probe			18				
17					17					17				
16					16					16				
15					15					15				
14					14		LAB Server 5		x	14		LAB OLT	1.000	
13					13		LAB Server 6			13				
12					12					12				
11					11					11				
10					10					10				
9					9					9				
8					8					8				
7					7					7				
6					6					6				
5					5					5				
4					4					4				
3					3					3				
2					2					2				
1					1					1				

Figure 22: The distribution of testbed devices in racks

4.3.2. OTE Testbed

OTE's core lab infrastructure (depicted in Figure 23) for the needs of RESISTO pilot will be interconnected with OTE's openstack cloud.(Figure 24)

Core lab's interfaces are mainly 10G and 1G both fiber and copper. There is a traffic generator which is Spirent test Center and has direct/physical connection to other components with cable (fiber for data and copper for management)

All metro Ethernet Switches (distributors) are Huawei connected with Layer 2 and L3 VPN connections to distant sites while locally are connected cable (both fiber and copper). All BNG Routers are CISCO and are considered core network. They have connections to other components with cable (fiber and copper) and indirect connections to other components located in other sites through Layer 2 and L3 VPN connections.

Regarding security they lab has firewalls enabled through ACLs (Access Control Lists)

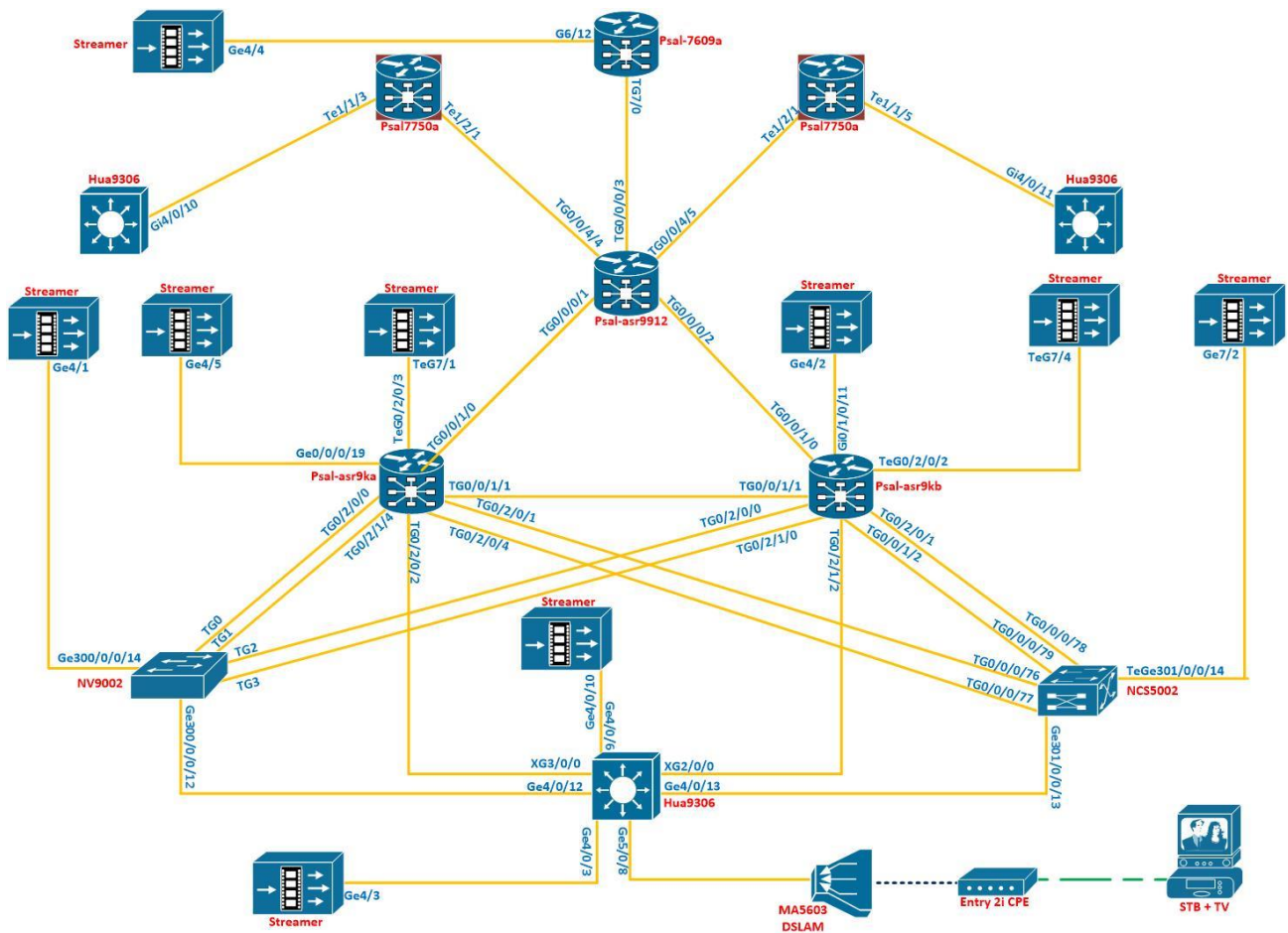


Figure 23: Core Lab Description

The second “part” of this testbed is the openstack testbed an indicative architecture of which is presented as follows.

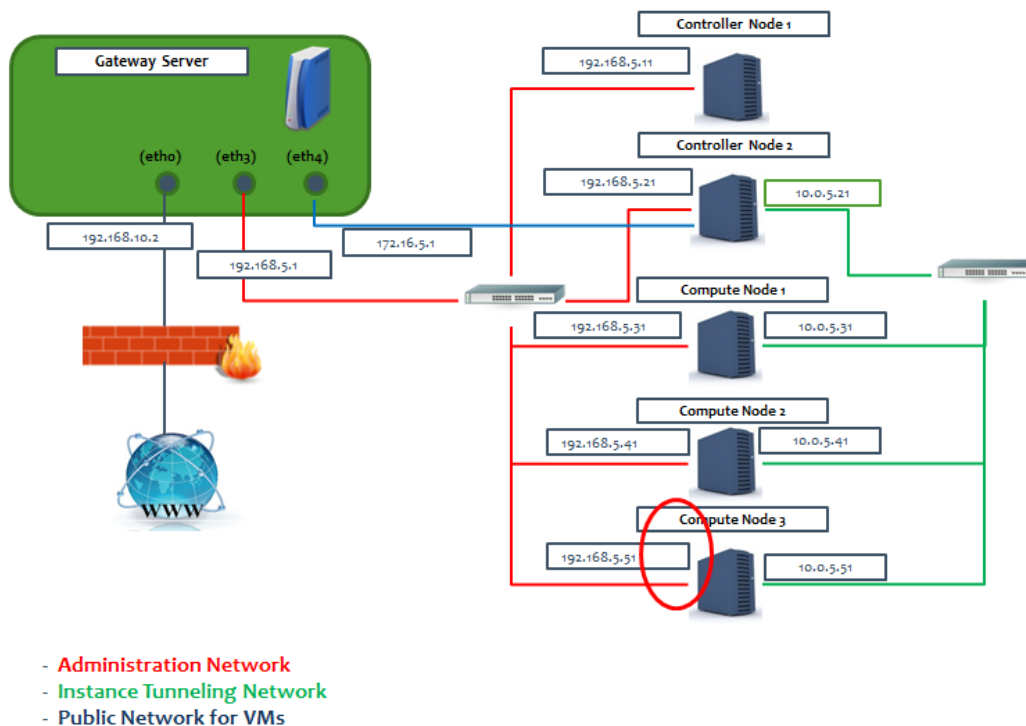


Figure 24: Generic architecture of OTE's Openstack testbed

The Openstack testbed OS is Ubuntu Server 16.04 LTS, while the current Openstack version is Queens; it can be upgraded based on project's specific requirements. Ubuntu Server 16.04 LTS, as one of the most active providing Long Term Support and ensuring that any issues that come up within the next five years will be dealt with. The testbed can be utilized for new technologies experimentation, either for PoC (Proof of Concept) or for field trials.

The testbed is composed of by gateways, various controllers and compute nodes (interconnected via switches/routers which can be formulated in any required architecture. The testbed generic architecture/layout is depicted in (see Figure 24).

The whole setup is behind a Cisco PIX 515 firewall, which provides NAT services. Additionally, a VPN server has been set up on the Gateway, which provides access to the Openstack hosts and the running VMs.

The testbed can be expanded to cover depending on the needs of projects either research or internal ones, depending on the given requirements. It can be expanded by adding "any" number of servers/services e.g. media, secure file/storage, monitoring. At this point it should be noted that openstack integrates well with Openflow, allowing the creation for complex architectures including both cloud, SDN and NFV technologies.

In Table 1, the Openstack hardware equipment is presented.

Table 1: Openstack hardware equipment

	System	#CPUs
Gateway	T310 PowerEdge	4
Controller 1	Optiplex 9020	4
Controller 2	T310 PowerEdge	4
Compute 1	Optiplex 9020	4
Compute 2	Optiplex 9020	4
Compute (x2)	HP ML350T09 SFF	44/88
Controller (x2)	Lenovo M900	2/4
storage	HPE proLiantDL380 Gen9	8/16

4.3.3. BTC Testbed

The UK testbed is provided by 5G-VINNI as part of the H2020 ICT-17 programme, can be seen in Figure 25. 5G-VINNI is an E2E 5G facility that can be used to first demonstrate the practical implementation of infrastructure to support the key 5G KPIs, and then to allow vertical industries to test and validate specific applications that are dependent upon those KPIs. The 5G-VINNI facility is composed of several geographic sites including a UK facility located at BT's Adastral Park research centre. The facility provides a full 5G system, implementing 3.5GHz NR and 26/28 GHz mmWave systems.

The transport network between Radio Access Network (RAN) and Core connect using the fibre network across the Adastral Park site and will utilise the on-site layer 3 switching network. Cell Site Routers are deployed at each of the RAN sites for all instances of 3.5GHz NR and mmWave installations. For 3.5GHz NR, the Cell Site Routers will connect with the 5G baseband and LTE baseband units which will be co-located with antenna units. Provider Edge Routers will connect the transport links with the Adastral Park data centre containing the 5G Core and 3.5GHz NR gNodeBs and mmWave gNodeBs.

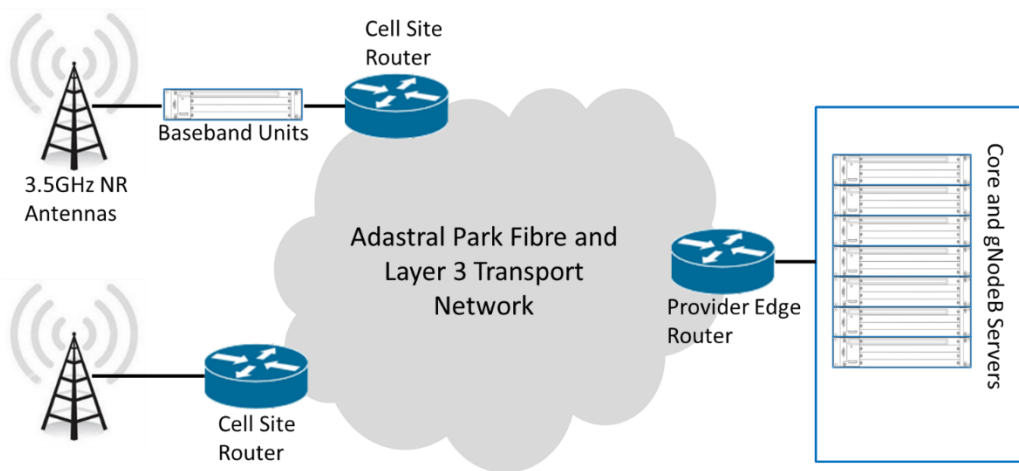


Figure 25: Testbed design for the transport network

The UK facility will be configured to demonstrate interworking with other 5G-VINNI locations, including a Norway facility operated by Telenor. 5G-VINNI is not only intended to be simply a group of interconnected test facility sites, as it is underpinned by principles that will allow for highly dynamic and flexible network architectures, service deployment and testing, that will create new technical and commercial service deployment models. These drive inter-facility interconnection to enable virtualized functions from the network and service layer to be called upon from any facility, with complete location agnosticism – a truly cloud-based network instantiation that has no functional boundaries, implemented across multiple facility sites.

In terms of 5G use cases, the UK facility will support all three basic service types - eMBB, URLLC and mMTC, provided to customer applications as a Network Slice as a Service (NSaaS). In addition, the UK facility will offer NSaaS based on a customised slice. The UK facility will also allow customers to bring their own VNFs and will be granted access to control and manage them. Likewise, it will offer an integration capability for customers to use their own infrastructure (e.g. additional gNodeBs), including the ability to manage and control this infrastructure, as well as the end-to-end slice. In addition, the UK facility will offer a service orchestration capability which will a) orchestrate the overall UK facility, b) support the ability to cross-orchestrate services between the UK and other 5G-VINNI facilities, c) provide an on-boarding capability for 5G applications, based upon a defined service description, offering service against an agreed SLA.

On top of 5G testbed, IoT platform will be deployed. Figure 26 shows IoT devices to Data Hub connectivity options. The data hub will include device information, IoT device traffic data, security and SLA data, and application specific data. It also provides various data analytic services.

The IoT platform also includes application enablement which enables customers to readily create applications that interface with the devices. This is achieved by abstracting the underlying complexity of the device into accessible APIs.

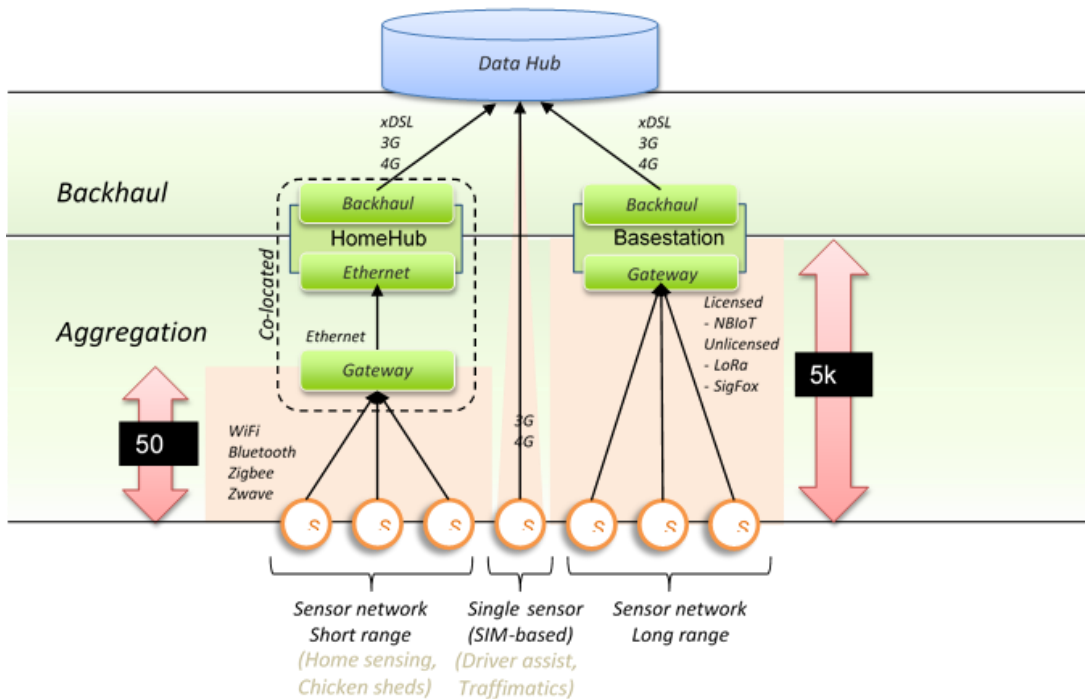


Figure 26: IoT devices to Data Hub connectivity options

The management of the device is equally as important as the telemetry and actuation. It must be possible to remotely manage the device through its complete life-cycle: deploy, monitor, manage (inventory), service, updates and decommission. These are all covered by the following four facets of device management:

- **Provisioning & Authentication** – the ability to allow devices to securely connect in the first instance and thereafter. Ideally this will rely on certificates. To support mass market devices it must allow new devices to autonomously connect and receive security credentials.
- **Configuration & Control** – the ability to control the remote device (e.g. soft reset, hard (factory) reset, firmware reload) and the configuration of the device (e.g. input/output ports enabled/disabled)
- **Monitoring & Diagnostics** – routine device level telemetry reporting its health (signal strength, battery level, etc.) as well as the ability to access audit logs and, possibly, remotely login to investigate issues.
- **Software Update & Maintenance** – the ability to manage all software configurable items on the device (firmware, operating system, application). It must be possible to schedule updates so as not to adversely impact the device when in use.

4.3.4. TIM Testbed

This testbed is a combination of a primary site and a second system at a remote system, and is defined as a hyper converged system. A visual of this design is seen in Figure 27. A hyper converged system is a platform that combines compute, storage and networking in a single system. This typically

implies hypervisor for virtualization of servers, software defined storage and virtual networking.

Each of the systems has a number of nodes that forms a local cluster for redundancy of the services. Each node in the cluster runs a hypervisor where all the virtual machines will be running. The sites are connected to each other that allows for replication of the virtual machines of the architecture.

Testbed

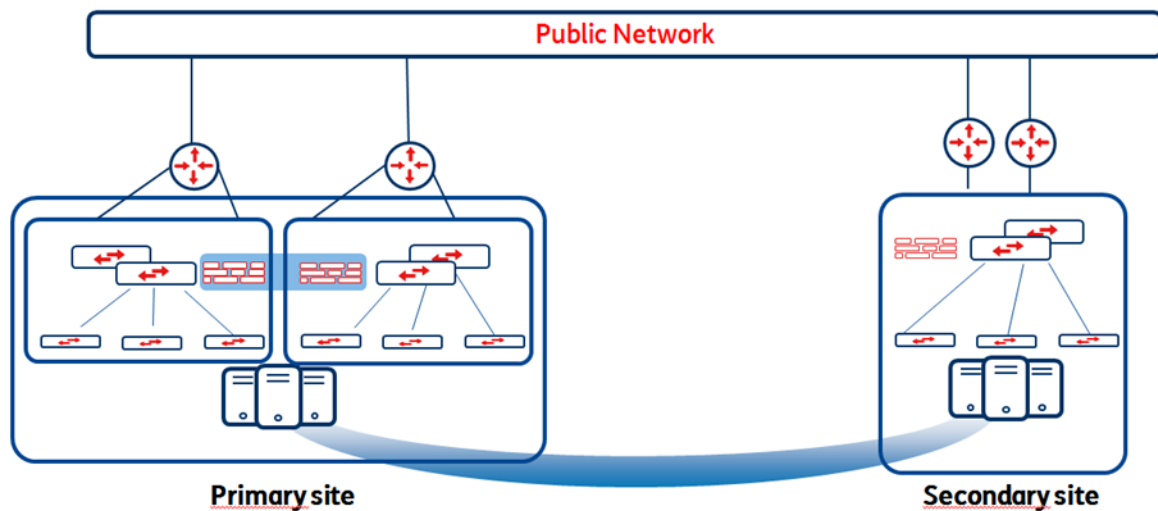


Figure 27: The testbed design with division between the primary and secondary sites

There are two main encryption methods for the data of the test beds as seen in Figure 28. The data at rest encryption focuses on the physical, virtual and cloud data. Within the virtual data encryption, the virtual disks are protected with encryption, pre-boot authentication, protection against theft or copy. The protection can be configured in local systems and also on remote sites and in public cloud. The files and shares on the systems will also be encrypted.

Additionally, the data on the storage of the cloud system will be encrypted and the security of the keys will be managed by an external key manager connected to the hypervisors as seen in Figure 29. The key manager will be deployed in virtual appliances on both sites for redundancy purposes. The solutions have different connectors to enable different encryption solutions based on different scenarios to be tested.

All of the sensitive data including the virtual machines disks will be protected against unauthorized use. The communication between the sites will use data in motion encryption to secure the transfer of sensitive data across external networks.



Figure 28: The different data encryption methods for the testbeds

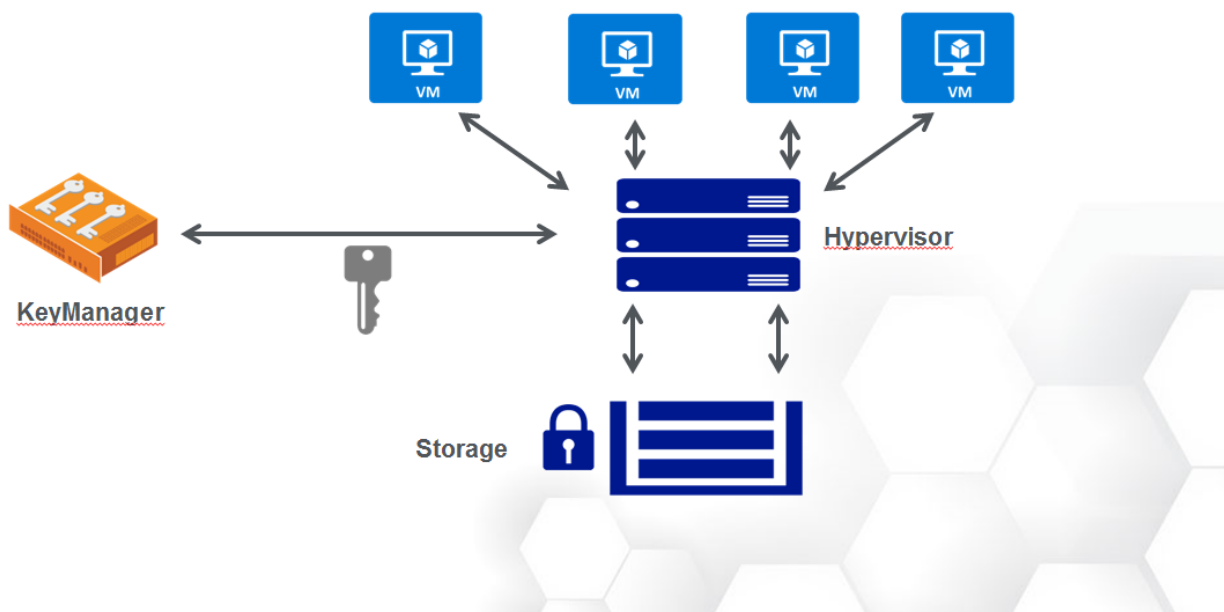


Figure 29: The set up for the data in the cloud encryption

4.3.5. ALB Testbed

Altice Labs' testbed is a facility for 5G experimentation and research, located in Aveiro, Portugal. The infrastructure is being deployed under the auspices of the H2020 ICT-17 project 5G-VINNI [10].

As illustrated in Figure 30 the 5G infrastructure can be divided in five different segments:

- Core DC
- IP/MPLS & Internet
- Central Office/ Edge Points of Presence (PoP)

- Mobile x-haul
- 5G RAN/cell site

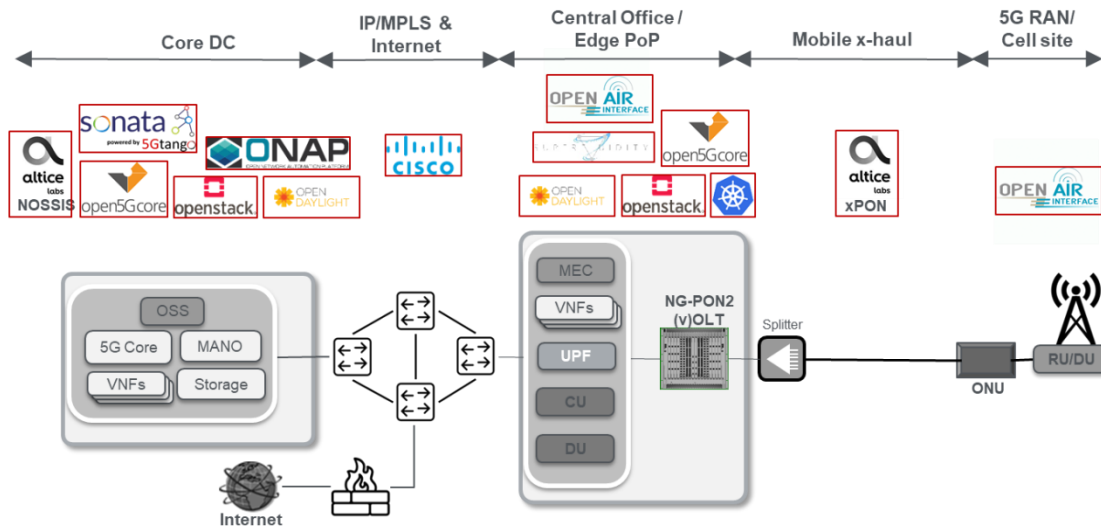


Figure 30: Altice Labs 5G testbed infrastructure and main technological components

From a physical perspective, the infrastructure will be hosted in two sites - Altice Labs and Institute of Telecommunications (IT) [12], both located in Aveiro. Figure 31 illustrates the physical location of the edge, core, MANO and OSS components of the site. Both Altice Labs and IT-Aveiro will host edge PoP. Altice Labs will host the 5G core, as well as the Management & Orchestration (MANO) and Operations Support Systems (OSS) components. IT -Aveiro will host a second instance of the 5G core, if required for specific scenarios or to address specific use case requirements (e.g. multi-domain, redundancy, resource migration).

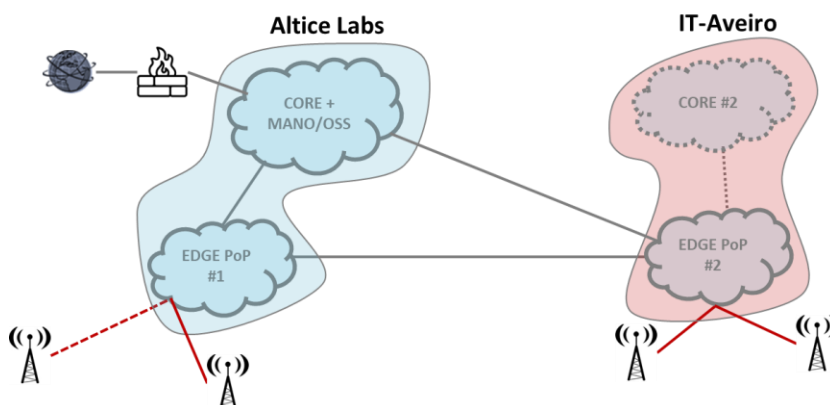


Figure 31: Physical topology of Altice Labs 5G testbed infrastructure

A brief description of each of these segments is provided below.

Radio Access Network

The radio access network's starting site is based on OpenAirInterface (OAI) [13] and leverages on the local 4G-based infrastructure supporting related research activities in Altice Labs. Currently supporting 4G radio, the OAI roadmap includes the support of 5G in the near future. OAI is designed to be agnostic to the hardware radio frequency (RF) platforms. It can be interfaced with 3rd party Software-Defined Radio (SDR) RF platforms without significant effort. The lab hardware components can be seen in Figure 32.

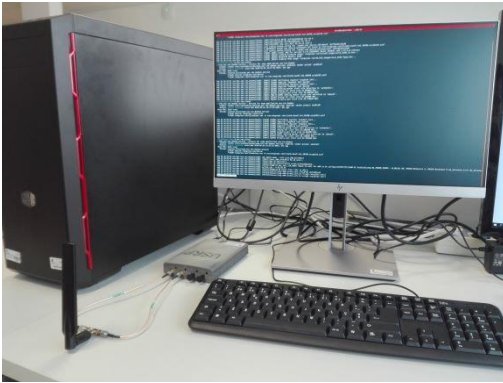


Figure 32: OAI lab hardware components (eNB, USRP, antenna)

Edge PoPs

Two edge PoPs will be setup, located at the premises of Altice Labs and IT-Aveiro. The Edge PoPs will typically host edge computing resources, virtualized network functions, virtualized C-RAN resources and selected 5G core components.

5G Core

The 5G Core component of the Portugal Facility-site will be based on Fraunhofer FOKUS Open5GCore toolkit [14] and will be hosted at the premises of Altice Labs. The target for Facility release 1 will be the deployment of the 5G Core compliant with 3GPP release 15, integrated with 5G NR and support for 5G interfaces (e.g. N1, N2, N3, N4) and the fundamental 5G core network components (e.g. AMF, SMF, UPF).

NFV Infrastructure

The ALB site can offer the following infrastructure resources:

- an OpenStack Virtual Infrastructure Manager (VIM) [15] running on one Controller Node and two Compute Nodes, appropriate to act as the Core site;
- an OpenStack VIM running on a single machine, aka 'all-in-one' configuration, appropriate to act as an Edge PoP. A second Edge PoP is available at 'IT Aveiro';
- a Kubernetes VIM [16] running on five bare metal blade servers, two master nodes and three worker nodes;
- one Opendaylight SDN Controller running on a dedicated bare metal blade server.

The generic ALB's NFVI can be used by any MANO framework if the connectivity is established, and the right credentials are provided. The NFV Orchestrator part of the MANO, based on SONATA as described in the following section, contains built-in plugins to connect to an OpenStack and Kubernetes VIM. Considering its modular architecture, other plugins can be developed to add other VIM types.

The NFV infrastructure at IT premises is based on Intel Xeon / Intel Core i7 cores, currently a total of 120 cores, running OpenStack Newton w/ KVM; 2x OpenFlow 1.4 Pica8 switches and OvS 2.4+ network nodes.

Management and Orchestration

The Management and Orchestration (MANO) will be provided by SONATA open source platform [17]. SONATA was initially developed by the H2020 5G-PPP Phase 1 project with the same name and is currently under development in a Phase 2 project, 5GTANGO [18] This tool compares very well with other well-known open source, such as ONAP or OSM in terms of supported features.

Service Orchestration

The Service Orchestration function will be performed using the ONAP open source tool. ONAP will perform functionalities such as:

- Receive customer service orders and trigger the execution of specific processes, sequencing activities for the creation, modification and removal of a service (the RESISTO platform should be seen as a customer in this context);
- Manage the lifecycle of network slices, enabling the design, creation, modification and removal of slices on top of a cloud infrastructure, ensuring the proper customer isolation;
- Expose service orchestration capabilities to BSSs by using an API;
- Use NFV Orchestration (NFVO) APIs to manage the lifecycle of NFV artifacts (VNFs and Network Services), as a way to build end-to-end network slices.

4.3.6. RTV Testbed

The two different testbeds, one for maritime and one for future networks are used for different use cases and scenarios. The maritime testbed focuses on maritime rural sites when a cyber-physical attack occurs. The aim of the tests is to have continued maritime communications even with the attacks. Figure 33 shows the Polarys infrastructure that was used a starting point for the physical probes. Propagation or cascading effects can be analysed with this system once the Leonardo and NOC platforms are connected. The testbed can be split into district, regional and central office areas. Small cells and macro cells are connected to the street cabinets which are then aggregated into the network in the district area. After the district region and the aggregation occurs, everything is sent to the data center in the regional area and then continues on the cloud and private data centers at the central office.

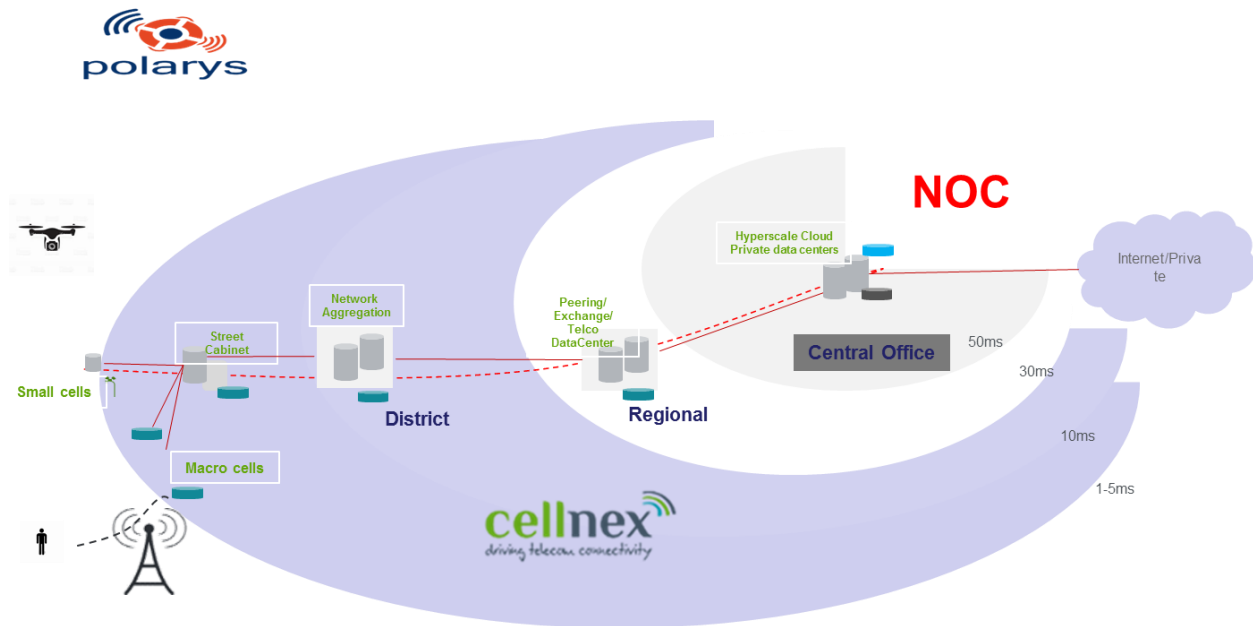


Figure 33: Polarys infrastructure used for maritime testbeds

Within the future network testbeds mobile future networks are tested against cyber-attacks with the aim that these 5G sites will continue to provide private communications and services. As seen in Figure 34, the AI MARS infrastructure is used as a starting point for attack simulations and cyber probe set up. The test bed has many EPCs that flow to and from the Internet. Then the MNO network connects and more EPCs are introduced. Testing can include local breakout and slicing with this testbed design.

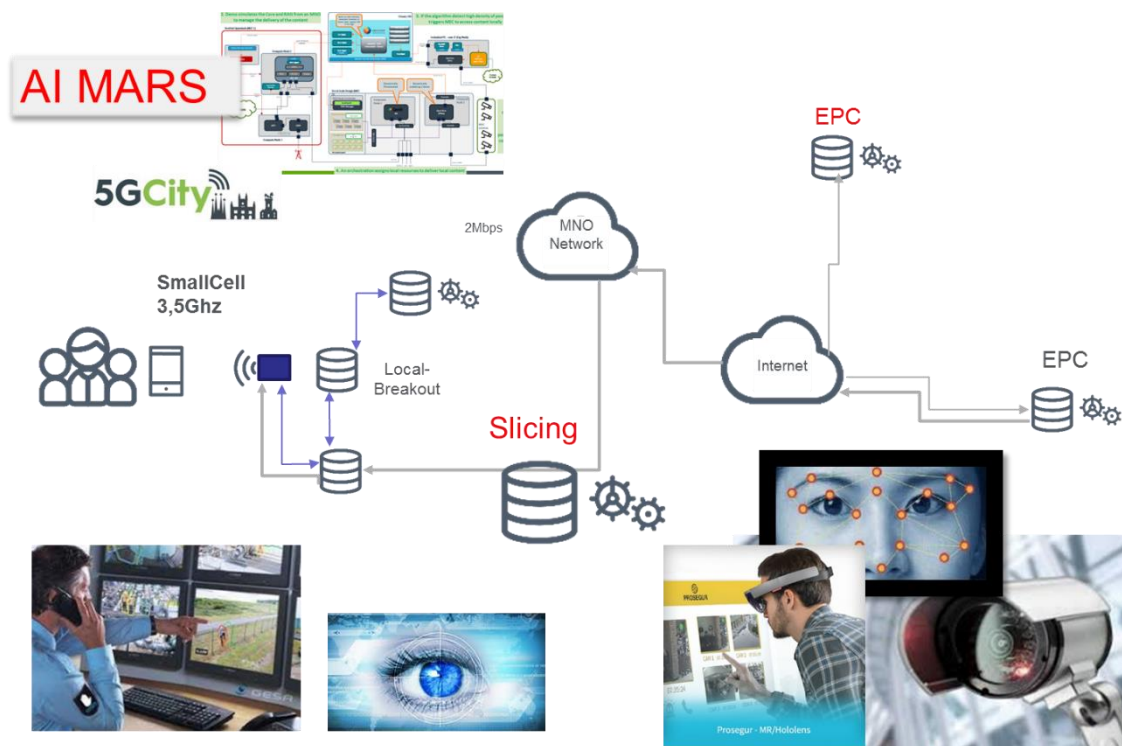


Figure 34: Future network testbed set up

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 (see D3.5 of Task 3.3).

5.1. Network simulators [RM3]

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 behaviours 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 [19], [20] 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 behaviour 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 behaviour.

Estinet

EstiNet [21] 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 [22] 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 [23], 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 [24] and [25].

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 behaviour 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 [26], [27], [28] Flow level is often modelled through Poisson processes, but self-similar behaviours are present at flow level as well [29].

5.2. Mixed Holistic Reductionist – CISIApro modelling approach [RM3]

CISIApro (Critical Infrastructure Simulation by Interdependent Agents) [30] is an Agent-Based Simulation Software and Engine used in Critical Infrastructures (CI) Protection projects to model behaviours and characteristics of involved entities due to possible, complex, cascading effects. Such

modeling software, in combination with the Mixed-Holistic-Reductionist (MHR) approach [31], is used to address a coherent level of granularity to a given CI scenario. It was born with the aim to analyse 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 behaviour 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 behaviour 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.

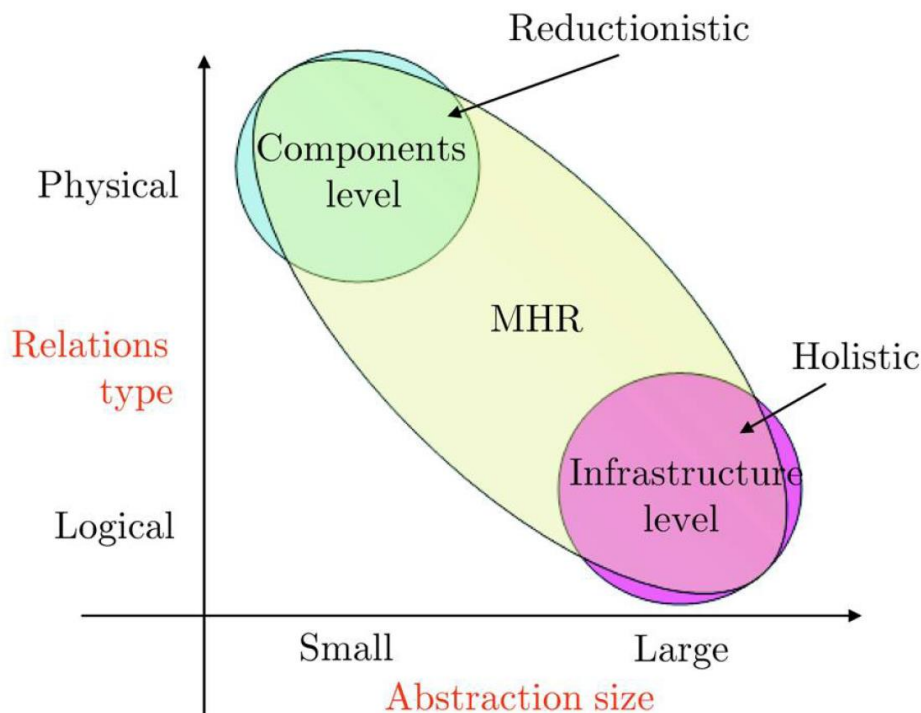


Figure 35: Dimensions in interdependent infrastructures modelling

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 36) 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.).

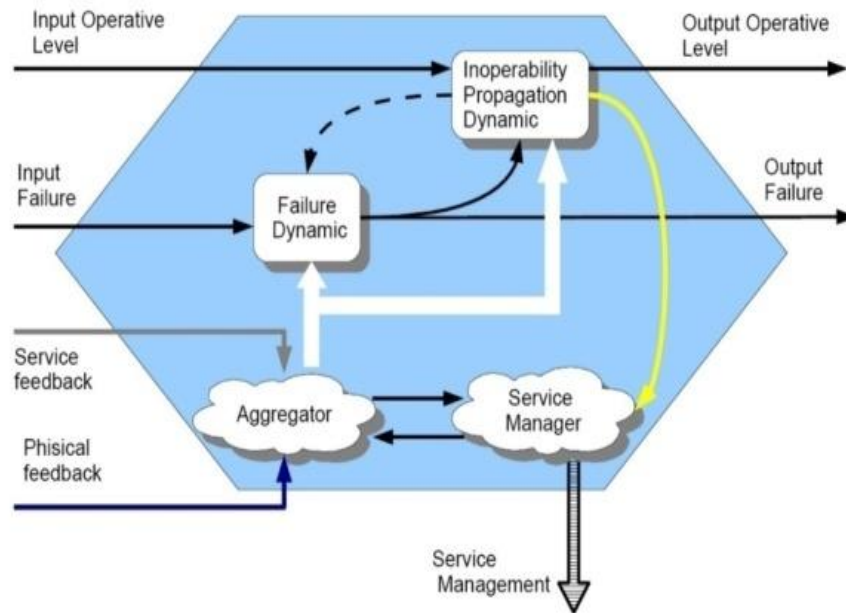


Figure 36: Holistic Block

- A **Service Entity** [Figure 37] represents a logical element, organizational or real, that provides an aggregate resource, for instance, could be express through a QoS (Quality of Service) level.

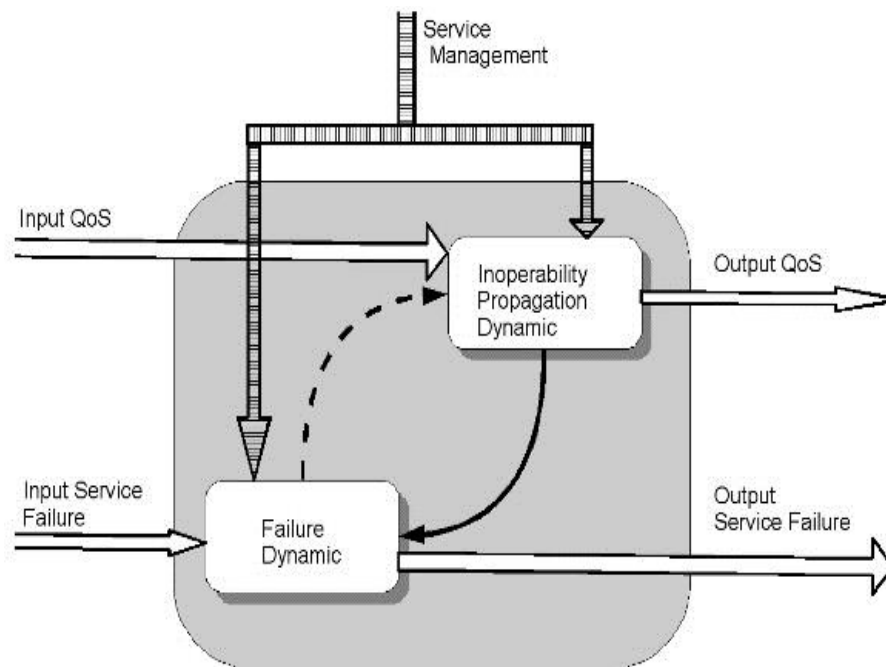


Figure 37: Service Block

- A **Reductionist Entity** [Figure 38] that represents, with the right degree of abstraction, all physical entities (also aggregated) of the infrastructure.

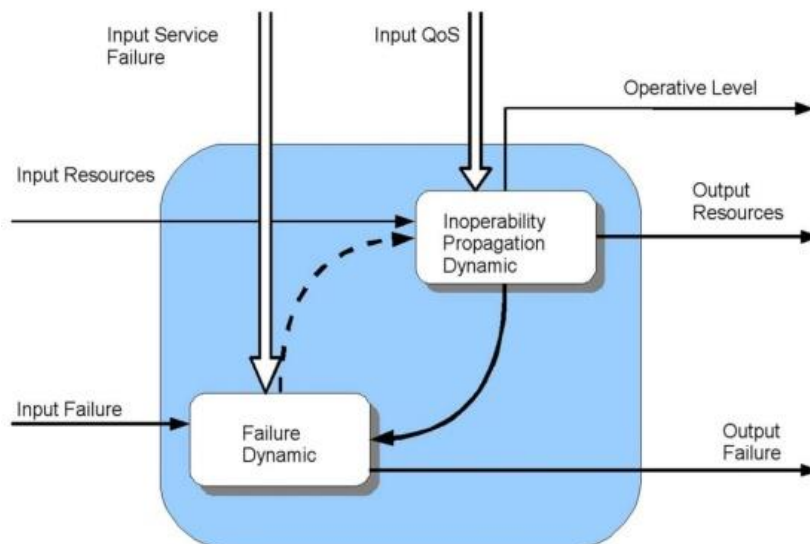


Figure 38: Reductionist Block

The actual state of the agent, in CISIApro, is summarised through the **Operational Level** concept [Figure 39]. 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 neighbourhoods and from the considered agent to its neighbourhood.
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 behaviour is highly abstracted but it is enough rich to leave the experts to model the model dynamics in the most appropriate way.

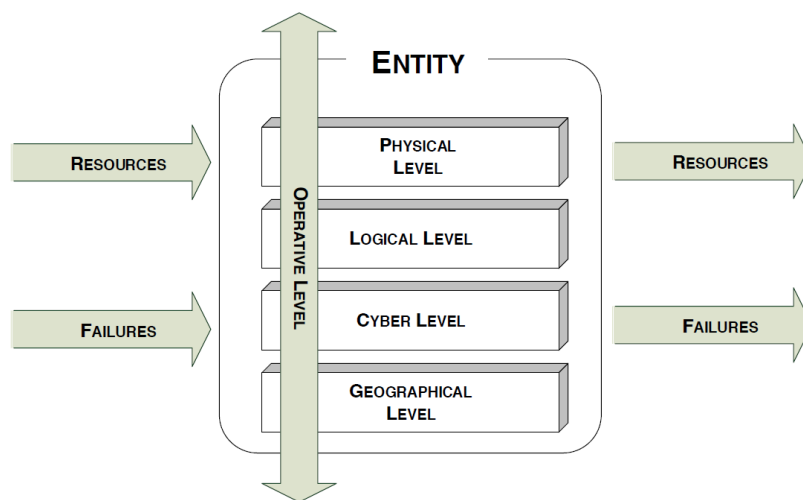


Figure 39 Generic entity representation

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 [32]. Dependency and interdependency should be analysed 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 39]. 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 [EMI]

The work presented in the report summarizes the result of Task 2.3. 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 in the mid-report (D2.4). In this report, some testbeds for the simulations were drafted in cooperation with the end-users. Furthermore, input from the operational partners is currently collected by other tasks and may contribute as additional source of information. Based on the drafted testbeds and the gathered information, realistic models and test scenarios can be provided in further tasks of the project, e.g. for tool refinements.

Finally, the technical implementation of the models and tools is addressed. This includes a comparison of available simulation software. The modelling approaches were selected with a view on scientific and operator acceptance. Later in the project, the assessed modelling approaches will be used as base for model building in the software implementation. A tool for network simulations by the partner RM3, which is already implemented and in use, is introduced.

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] 5G Verticals Innovation Infrastructure: H2020 5G-VINNI Project <https://www.5g-vinni.eu>
- [11] Finger J, Faist K, Hasenstein S and Leismann T 2017 *Transforming Cities* **2** 58–60
- [12] Instituto de Telecomunicações <https://www.it.pt/>
- [13] OpenAirInterface, 5G software alliance for democratising wireless innovation <https://www.openairinterface.org>
- [14] Open5GCore – The Next Mobile Core Network Testbed Platform <https://www.open5gcore.org>
- [15] OpenStack <https://www.openstack.org/>
- [16] Kubernetes Production-Grade Container Orchestration <https://kubernetes.io/>
- [17] SONATA <https://sonata-nfv.github.io/>
- [18] 5GTANGO 5G Development and Validation Platform for Global Industry-Specific Network Services and Apps <https://5gtango.eu/>
- [19] 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
- [20] Patel R **2016**
- [21] Wang S-Y, Chou C-L and Yang C-M 2013 *IEEE Commun. Mag.* **51** 110–7
- [22] 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
- [23] Fred S B, Bonald T, Proutiere A, Régnié G and Roberts J W 2001 *SIGCOMM Comput. Commun. Rev.* **31** 111–22
- [24] B. Chandrasekaran *Survey on Network Traffic Models* https://www.cse.wustl.edu/~jain/cse567-06/traffic_models3.htm
- [25] Mohamed, Ahmed & Agamy, Adel 2011 *International Journal of Computer Networks*
- [26] 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
- [27] 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
- [28] O. Lemeshko, A. M. Hailan and A. S. Ali 2010 225
- [29] Millán G and Lefranc G 2013 *Procedia Computer Science* **17** 420–5
- [30] Foglietta C, Palazzo C, Santini R and Panzieri S 2015 Assessing Cyber Risk Using the CISIApro Simulator *Critical Infrastructure Protection IX (IFIP Advances in Information and Communication Technology)* ed M Rice and S Sheno (Cham: Springer International Publishing) pp 315–31
- [31] Porcellinis S D, Panzieri S and Setola R 2009 *IJCIS* **5** 86
- [32] 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