

RESISTO: D4.4_COMPLETE PROPAGATION ANALYSIS



RESISTO

D4.4 – COMPLETE PROPAGATION ANALYSIS

Document Manager:	Stefano Panzieri	ORG: RM3	Editor
--------------------------	------------------	----------	--------

Project Title:	RESilience enhancement and risk control platform for communication infraSTructure Operators
Project Acronym:	RESISTO
Contract Number:	786409
Project Coordinator:	LEONARDO
WP Leader:	Giuseppe Celozzi (TEI)

Document ID N°:	RESISTO_D4.4_200525_01	Version:	1.0
Deliverable:	D4.4	Date:	25/05/2020
		Status:	APPROVED

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

Approval Status	
Prepared by:	Stefano Panzieri (RM3) Elena Bernardini (RM3) Chiara Foglietta (RM3)
Approved by: (WP Leader)	Giuseppe Celozzi
Approved by: (Coordinator)	Bruno Saccomanno
Advisory Board Validation (Advisory Board Coordinator)	N.A.
Security Approval (Security Advisory Board Leader)	Paolo DI MICHELE (LDO)

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Maria Belesioti Evangelos Sfakianakis	OTE	Senior Researchers, Electrical Engineers, Telecommunication Experts
Giuseppe Celozzi, Cosimo Zotti, Giuseppe Amato	TEI	Telecommunications Experts, Senior Researchers
Annarita Di Lallo, Alberto Neri	LDO	Senior Researchers, Defence and Security Specialists
Michael Skitsas, Nikolaos Koutras	ADI	Senior Researchers, Electrical Engineers, Defence and Security Specialists
Moisés Valeo, Jose Sanchez, Javier Valera	INT	Senior Researchers, Electrical Engineers, Defence and Security Specialists
Marco Mancini Luca Lionetti Marco Mella	TIM	Telecommunications Experts, Senior Researchers
Manuel Canete Luis Moreno	RTV	Telecommunications Experts, Senior Researchers
Sandro Mari Maura Gambassi	CER	Cybersecurity experts Senior Researchers

DISTRIBUTION LIST

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

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
0.1	5.07.2019	All	All	Table of contents and draft sections
0.5	8.11.2019	All	All	Updated Table of contents and draft sections
0.7	18.11.2019	All	All	Additions and partners contributions
0.8	16.01.2020	All	All	Interim release for review
0.9	07.05.2020	All	All	Final Release for SAB assessment
1.0	25.05.2020	All	All	Final version

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 2 – Genova – 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

Private businesses and government agencies are dependent on telephone and internet services provided by telecommunications networks to carry out daily operations and the increasing digitalization of telecommunication infrastructure makes it a field for cyber-attacks, which is further enabled through the distributed, combined and legacy nature of the telecommunication Cis. The move towards the 5G standard, that is further increasing virtualization and abstraction from physical layers, causes these networks have a larger number of alternative routings as well as a larger amount of redundancies and back-up options to carry ever-increasing amount of data that is transported through the telecommunication infrastructure consumer services (e.g. video communication, navigation, M2M communication) and private and business cloud services (e.g. software on demand, storage on demand, etc.). To assess the exposure to the risks and impacts to which these systems are subject, Deliverable D4.4 aims to model unified scenarios of interdependent service-oriented infrastructures.

CISI Apro 2.0, an agent-based simulator, models these interconnected infrastructures in order to evaluate the consequences that adverse events, such as failures, cyber-attacks, and natural disasters, and restoring actions, have on these systems.

CONTENTS

ABBREVIATIONS.....	14
1. INTRODUCTION – PURPOSE OF THE DOCUMENT	17
2. A FRAMEWORK FOR RISK PREDICTION	18
2.1. Critical Infrastructure Resiliency and Interdependency.....	18
2.2. The Concepts of Risk and Resilience.....	22
2.3. Modelling Interdependencies with MHR approach.....	25
2.4. Risk Prediction related KPIs from D3.7 (RM3)	29
3. REQUIREMENTS.....	31
3.1. Functional Requirements	32
3.1.1. Input data.....	33
3.1.2. System Reports and Other Outputs.....	34
3.1.3. Functional Requirements related to 5G.....	34
3.2. Non-Functional Requirements	35
3.2.1. Design Requirements.....	35
3.2.2. Interface Requirements	35
4. A TOOL FOR IMPACT ASSESSMENT: CISIAPRO 2.0	37
4.1. CISIApro 2.0 – Dynamic Risk Analysis Tool	37
4.2. Layers & Resources Module.....	40
4.3. Entity Maker Module	41
4.4. Modeler Module	42
4.5. State Variables Module	43
4.6. Link States Module.....	44
4.7. CISIAmat – the CISIApro 2.0 on-line engine	45
5. UNIFIED REFERENCE SCENARIOS	48
5.1. Unified Scenarios	48
5.2. General Telecommunication architecture for Unified Scenarios.....	49
5.3. End users modelling	51
5.3.1. Hospital	51
5.3.2. Smart Factory.....	56
5.3.3. Aveiro Port	58
5.3.4. Maritime Environment.....	58
5.4. Emergency Warning Communications (EWC) and the RESISTO PLATFORM.....	59
5.5. CISIApro implementation of all unified reference scenarios.....	60

5.5.1.	Entity Types used in the unified scenarios.....	60
5.5.2.	Description of State Variables.....	103
5.5.3.	Description of Input-Output Resources.....	105
6.	USE CASE 1-2: CORE NETWORK FAILURE CAUSED BY PHYSICAL & CYBER-ATTACKS OR NATURAL DISASTERS TO TELECOMMUNICATION SITES (OTE TESTBED)	108
6.1.	Unified Reference Scenario 1.....	108
6.2.	Sub Scenarios for Use Case 1 and Impacts on the Unified Scenario	110
6.3.	Sub Scenarios for Use Case 2 and Impacts on the Unified Scenario	112
6.4.	Threats and Impacts on CISIApro	115
6.5.	CISIApro implementation	117
6.5.1.	Description of CISIApro model.....	117
6.5.2.	Model design: entities for Unified Scenario 1.....	119
6.5.3.	Model design: services associated to entities	122
7.	USE CASE 6: CYBER AND PHYSICAL PROTECTION OF NETWORK AND NETWORK ELEMENTS MECHANISMS USED BY CRITICAL SERVICES THAT IMPACT USERS (ORO TESTBED)	123
7.1.	Unified Reference Scenario 2.....	123
7.2.	Threats and Impacts on CISIApro	126
7.3.	Sub Use Cases and Impacts on the Unified Scenario	127
7.4.	CISIApro implementation	128
7.4.1.	Description of CISIApro model.....	128
7.4.2.	Model design: entities for Unified Scenario 2.....	129
7.4.3.	Model design: services associated to entities	132
8.	USE CASE 9: 5G NETWORK RESPONSE TO A SECURITY BREACH (ALB TESTBED)	133
8.1.	Unified Reference Scenario 3.....	133
8.2.	Threats and Impacts on CISIApro	136
8.3.	Impacts on the Unified Scenario	136
8.4.	CISIApro implementation	137
8.4.1.	Description of CISIApro model.....	137
8.4.2.	Model design: entities for Unified Scenario 3.....	138
8.4.3.	Model design: services associated to entities	140
9.	USE CASE 4: DISRUPTION OF MAJOR SPORTING EVENT BY COMBINED PHYSICAL & CYBER-ATTACK BY TERRORIST ORGANIZATION (BTC TESTBED).....	141
9.1.	Unified Reference Scenario 4.....	141
9.2.	Threats and Impacts on CISIApro	143
9.3.	Impacts on the Unified Scenario	144
9.4.	CISIApro implementation	146
9.4.1.	Description of CISIApro model.....	146
9.4.2.	Model design: entities for Unified Scenario 4.....	147

9.4.3. Model design: services associated to entities	150
10. USE CASE 5.1: PROTECTION OF CLOUD STORAGE SERVICES HEALTHCARE SYSTEM (TIM TESTBED)	152
10.1. Unified Reference Scenario 5	152
10.2. Threats and Impacts on CISIApro	155
10.3. Impacts on the Unified Scenario	156
10.4. CISIApro implementation	157
10.4.1. Description of CISIApro model	157
10.4.2. Model design: entities for Unified Scenario 5	158
10.4.3. Model design: services associated to entities	163
11. USE CASE 5.2: PROTECTION OF CLOUD STORAGE SERVICES – 5G SMART MANUFACTURING (TIM TESTBED)	165
11.1. Unified Reference Scenario 6	165
11.2. Threats and Impacts on CISIApro Services	168
11.3. Impacts on the Unified Scenario	168
11.4. CISIApro implementation	169
11.4.1. Description of CISIApro model	169
11.4.2. Model design: entities for Unified Scenario 6	170
11.4.3. Model design: services associated to entities	174
12. USE CASE 7: MARITIME SAFETY AND EMERGENCY CASE (RTV TESTBED)	175
12.1. Unified Reference Scenario 7	175
12.2. Threats and Impacts on CISIApro	178
12.3. Impact on the Unified Scenario	178
12.4. CISIApro implementation	179
12.4.1. Description of CISIApro model	179
12.4.2. Model design: entities for Unified Scenario 7	180
12.4.3. Model design: services associated to entities	183
13. SUMMARY AND CONCLUSIONS	185
14. REFERENCES	186

LIST OF FIGURES

Figure 1 – Example of interdependencies among critical infrastructures from [6]	19
Figure 2 – Representation of resilience profile from [6].	21
Figure 3 - Resilience cycle phases	23
Figure 4 – Risk and resilience management from [10], where PMI is Protective Measurement Index, RMI is Resilience Measurement Index and CMI is Consequences Measurement Index	24

Figure 5 – Holistic component in MHR approach	27
Figure 6 – Service component in MHR approach.....	28
Figure 7 – Reductionist component in MHR approach	29
Figure 8 – Risk Predictor Architecture	38
Figure 9 – CISIApro SQL data structure.	39
Figure 10 – CISIApro SQL output data structure.	39
Figure 11 – CISIApro user interface.....	40
Figure 12 – CISIApro Module: Layers & Resources.	41
Figure 13 – CISIApro Module: Entity Maker.....	42
Figure 14 – CISIApro Module: Modeler.	43
Figure 15 – CISIApro Module: State Variables.....	44
Figure 16 – CISIApro Module: Link State.	45
Figure 17 – URANIUM platform civil protection panel.	46
Figure 18 – ATENA Platform.....	47
Figure 19 General Telecom architecture for Unified Scenario	50
Figure 20 Model of hospital ward.....	51
Figure 21 Plan of hospital ward	52
Figure 22 Smart Factory	56
Figure 23 Factory deployment using pico 4G/5G base stations (green) and with on-premises breakout possibility	57
Figure 24 Aveiro Port	58
Figure 25 Maritime Environment	58
Figure 26 Emergency Warning Communications (EWC)	59
Figure 27 Unified Scenario 1: Use Case 1-2 – OTE Testbed	108
Figure 28 RESISTO slice Core Lab Description	109
Figure 29 Unified Reference Scenario 1 CISIApro Model top view.....	117
Figure 30 Scenario used for Use Case 1 and 2	118
Figure 31 Scenario in CISIApro	118
Figure 32 Unified Scenario 2: Use Case 6 – ORO Testbed.....	123
Figure 33 ORO Testbed	124
Figure 34 Unified Scenario 2 CISIApro Model top view	128
Figure 35 End Users in Unified Scenario 2	129
Figure 36 Unified Scenario 3: Use Case 9 – ALB Testbed	133
Figure 37 ALB Testbed.....	134
Figure 38 Unified Scenario 3 CISIApro Model top view	137
Figure 39 Aveiro Sea Port in CISIApro.....	138
Figure 40 Unified Scenario 4: Use Case 4 – BTC Testbed	141
Figure 41 BTC Testbed.....	142
Figure 42 Unified Scenario 4 CISIApro Model top view	146
Figure 43 End-devices in Unified Scenario 4	147
Figure 44 Unified Scenario 5: Use Case 5.1 – TIM Testbed.....	152
Figure 45 Tim Cloud storage critical infrastructure Healthcare Scenario	153
Figure 46 Unified Scenario 5 CISIApro Model top view	157
Figure 47 Hospital Ward CISIAPro Model	158
Figure 48 Unified Scenario 6: Use Case 5.2 – TIM Testbed.....	165

Figure 49 Critical infrastructure Smart Manufacturing Scenario	166
Figure 50 Unified Scenario 6 CISIApro Model top view	169
Figure 51 Smart Factory in CISIApro Model	170
Figure 52 Unified Scenario 7: Use Case 7 – RTV Testbed	175
Figure 53 Topology of Emergency service provision.....	176
Figure 54: Use case 7 Topology of Maritime Use Cases.....	176
Figure 55 Unified Scenario 7 CISIApro Model top view	179
Figure 56 Maritime Environment in CISIApro Model	180

LIST OF TABLES

Table 1 KPIs from D3.7 RISK Predictor related	30
Table 2 Functional Requirements	32
Table 3 Input Data.....	33
Table 4 System Reports and Other Outputs.....	34
Table 5 Functional Requirements related to 5G	34
Table 6 Design Requirements	35
Table 7 Interface Requirements	35
Table 8 Unified Reference Scenarios.....	48
Table 9 Entities and Variables for Building.....	53
Table 10 Entities and Variables for Electrical system	53
Table 11 Entities and Variables for Water system.....	54
Table 12 Entities and Variables for Air Conditioning system	55
Table 13 Entity Type	60
Table 14 CISIApro State Variables	103
Table 15 Input-Output Resources	105
Table 16 TLC Network Elements for Reference Scenario 1	109
Table 17 Sub Scenarios for Use Case 1	111
Table 18 Impacts on the Unified Scenario 1 for Use Case 1	111
Table 19 Sub Scenarios for Use Case 2	112
Table 20 Impacts on the Unified Scenario 1 for Use Case 2	113
Table 21 Cyber and Physical security events for the Unified Scenario 1	115
Table 22 Entities for Unified Scenario 1	119
Table 23 Services for Unified Scenario 1	122
Table 24 TLC Network Elements for Reference Scenario 2	125
Table 25 Cyber and Physical security events for the Unified Scenario 2	126
Table 26 Sub Use Cases for Use Case 6	127
Table 27 Impacts on the Unified Scenario 2	127
Table 28 Entities for Unified Scenario 2	129
Table 29 Services for Use Case 6	132
Table 30 TLC Network Elements for Reference Scenario 3	135
Table 31 Cyber and Physical security events for the Unified Scenario 3	136
Table 32 Impacts on the Unified Scenario 3	136

Table 33 Entities for Unified Scenario 3	138
Table 34 Services for Use Case 9	140
Table 35 TLC Network Elements for Reference Scenario 4	143
Table 36 Cyber and Physical security events for the Unified Scenario 4	143
Table 37 Impacts on the Unified Scenario 4	144
Table 38 Entities for Unified Scenario 4	147
Table 39 Services for Use Case 4	150
Table 40 TLC Network Elements for Reference Unified Scenario 5	154
Table 41 Cyber and Physical security events for the Unified Scenario 5	155
Table 42 Impacts on the Unified Scenario 5	156
Table 43 Entities for Unified Scenario 5	158
Table 44 Services for Use Case 5.1	163
Table 45 TLC Network Elements for Reference Scenario 6	167
Table 46 Cyber and Physical security events for the Unified Scenario 6	168
Table 47 Impacts on the Unified Scenario 6	168
Table 48 Entities for Unified Scenario 6	170
Table 49 Services for Use Case 5.2	174
Table 50 TLC Network Elements for Reference Scenario 7	177
Table 51 Cyber and Physical security events for the Unified Scenario 7	178
Table 52 Impact on the Unified Scenario 7	178
Table 53 Entities for Unified Scenario 7	180
Table 54 Services for Use Case 7	183

ABBREVIATIONS

2G, 3G, 4G	Second, third and fourth generation of mobile phone systems
ACLs	Access Control Lists
API	Application Programming Interface
APN	Access Point Name
ASIC	Application Specific Integrated Circuit
AV	Antivirus detection
B2B	Back-to-Back gateway
BNG	Broadband Network Gateway
CCA	Critical Communication Application
CCS	Critical Communications System
CCTV	Closed Circuit TV
CDN	Content Delivery Network
CI	Critical infrastructure
CPS	Cyber-Physical Systems
CPU	Central Processing Unit
DHS	Department of Homeland Security
DMO	Direct Mode Operations
ETSI	European Telecommunications Standard Institute
EU	European Union
FW	Firewall
GGSN	Gateway GPRS Support Node
GSM	Global System for Mobile communications
GSSI	Group Short Subscriber Identity
HW	HardWare
HTTP	HyperText Transfer Protocol
ICT	Information and Communication Technology

IDS	Intrusion detection systems
IGMP	Internet Group Management Protocol
IIM	Input-output Inoperability Model
IoT	Internet of Things
IPS	Intrusion prevention systems
IPTV	Internet Protocol Television
ISI	Inter System Interface
ISSI	Individual Short Subscriber Identity
ISITEP	Inter System Interfaces for TETRA-TETRAPOL Networks
ITSI	Individual TETRA subscriber Identity
KPIs	Key Performance Indicators
LTCL	Long Term Control Loop
LTE	Long Term Evolution (= 4G)
MCEER	Multidisciplinary Center for Earthquake Engineering Research
MHR	Mixed Holistic Reductionistic
MNO	Mobile Network Operator
NaaS	Network as a Service
NFV	Network Functions Virtualization
NOC	Network Operations Center
NSSP	Network Slice Subnet Provider
OTT	Over-the-Top
PC	Personal Computer
PPDR	Public Protection and Disaster Relief
PSIM-C	Physical Security Management Center
PTT	Push To Talk
QoS	Quality of Service
RTU	Remote Terminal Unit

SDN	Software Defined Networking
SDS	Software Defined Security
SOC	Security Operation Center
SP	Service Provider
SW	SoftWare
TCCE	TETRA and Critical Communications Evolution
TEA2	TETRA Encryption Algorithm #2
TETRA	TErrestrial Trunked RAdio
TG	Talk Group
TMO	Trunked Mode Operations
UE	User Equipment
UAV	Unmanned Aerial Vehicle
VM	Virtual machine
VPN	Virtual Private Network
WP	Work Package

1. INTRODUCTION – PURPOSE OF THE DOCUMENT

The development of 5G technology is completely revolutionizing the world of telecommunications. The fifth-generation networks will influence, not only on the performances offered to users, but above all on those sectors which, taking advantage of future connections, will be able to offer increasingly innovative services.

The ability to take advantage of network requirements such as high transmission speeds, reduced latency times and reliable connections between a large number of devices, allow to realize the paradigm of the connected society and the pervasive digitization of the activities.

In view of the advantages that the 5G network offers, however, we must consider the many challenges that this new communication standard requires to face.

In this regard, the rapid spread of ICT (Information and Communications Technology) and the resulting digital revolution have made the importance of telecommunications networks grow more and more in comparison with all the other Critical Infrastructures, both that today their operation depends almost totally on their functioning.

The establishment of these interdependencies undoubtedly makes the various systems most vulnerable to a series of threats. This implies that certain types of accidental failures or focused attacks can simultaneously compromise the ability of several Critical Infrastructures to offer their services.

The purpose of this deliverable is therefore to describe unified scenarios able to simulate the risk scenario explained in each specific use case described in Deliverable 2.8 and to assess the exposure to risks and the impact that possible threats would have on the same systems at stake.

The structure of the present Deliverable D4.4 is as follows:

Chapter 2 illustrates the concepts of critical infrastructures and interdependencies existing between them. In particular, this chapter describes in detail the resilience of critical infrastructures and presents the Mixed Holistic-Reductionist (MHR) approach.

Chapter 3 presents the functional and non-functional requirements of the RESISTO architecture indicating which are the requirements that can be supported in their fulfilment by Risk Predictor.

Chapter 4 is dedicated to the tool used to assess the risk to which a system could be subject: CISIApro 2.0 models interconnected infrastructures to assess the consequences of adverse events, such as failures, cyber-attacks, natural disasters, and restoring actions.

In Chapter 5 the unified scenarios are defined, describing in detail the architecture of the telecommunications network and the end user models as the Hospital, the Smart Factory, the Aveiro Port and the Maritime Environment. This Chapter moreover shows the entity types, the state variables and the input/output resources that have been defined to model the different telecommunications network components of each unified scenario.

Chapters from 6 to 12 present the models created in CISIApro 2.0 to simulate the different use cases described in Deliverable 2.8.

2. A FRAMEWORK FOR RISK PREDICTION

This chapter describes the main concepts related to the impact analysis within the RESISTO project. Critical Infrastructures (or Essential Services, following the European law) concept has changed during the last 20 years: Critical Infrastructures are large and geographically extended systems that are a fundamental part of our lives. Critical infrastructures are tightly connected to the concept of interdependency. In fact, those systems are not isolated, but they are interconnected one to another in, sometimes, unpredictable ways.

Other two concepts are well described along the RESISTO project: risk and resilience. Risk is usually related to a possible metric for understanding the consequences of adverse events; resilience is the ability to decreasing the effects of adverse events. In this document, the two concepts are exploited for understanding the consequences of adverse events (such as natural disasters, cyber-attacks or faults) and the consequences of restoration or mitigation actions.

One of the key components of the RESISTO architecture is the Risk Predictor. The Risk Predictor can assess the consequences of different events on the considered infrastructures: for example, the Risk Predictor evaluates the domino effect of a DoS attack on the physical infrastructure and on its services. The events are also the restoration actions performed after a fault or a cyber-attack.

The modelling approach exploited in the Risk Predictor module is based on the Mixed Holistic Reductionist approach, where each infrastructure is divided into components (reductionist layer), services (service layer) and holistic nodes (holistic layer). This approach is then applied using an agent-based simulator, called CISIApro 2.0. This simulator can represent the consequences of adverse and positive events on an interdependent scenario.

2.1. Critical Infrastructure Resiliency and Interdependency

The concept of critical infrastructure is evolving. In the 1980s, critical infrastructures were connected to aging public works: National Council on Public Works Improvement in 1988 focused on infrastructure in the public sector, such as highways, roads, bridges, airports, public transit, water supply facilities, wastewater treatment facilities, and solid-waste and hazardous-waste services. In the 1990s, as a result of increased international terrorism, infrastructure was redefined in terms of national security. After 9/11, the number of “critical” infrastructure sectors and key assets listed in the National Infrastructure Protection Plan [1] was expanded to 17: it includes agriculture and food systems, the defence-industrial base, energy systems, public health and health care facilities, national monuments and icons, banking and finance systems, drinking water systems, chemical facilities, commercial facilities, dams, emergency services, nuclear power systems, information technology systems, telecommunications systems, postal and shipping services, transportation systems, and government facilities. In Europe, the concept of critical infrastructures is defined under the name “essential services” [4].

Changing the definition of critical infrastructures has led to more flexibility and adaptability. On the other hand, the complexity of an already complex field is increased, causing more confusion and more ambiguity. Therefore, some researchers defined the concept of “lifeline system”, [5] to evaluate

the performance of large, geographically distributed networks during crisis caused by adverse events, such as natural events or cyber-attacks. Lifelines are grouped into six principal systems: electric power, gas and liquid fuels, telecommunications, transportation, waste disposal, and water supply. Those systems are tightly linked with the economic well-being, security, and safety of our lives. Thinking about critical infrastructure through the subset of lifelines helps clarify features that are common to essential support systems and provides insights into the engineering challenges to improving the performance of large networks.

Lifeline systems are interdependent, primarily by virtue of physical proximity and operational interaction. In crowded areas, cables and pipes are placed one near the others, causing an increased risk due to proximity. Damage to one infrastructural component, such as a cast-iron water main, can rapidly cascade into damage to surrounding components, such as electric and telecommunications cables and gas mains, with system-wide consequences.

Lifeline systems all influence each other. Electric power networks, for example, provide energy for pumping stations, storage facilities, and equipment control for transmission and distribution systems for oil and natural gas. Oil provides fuel and lubricants for generators, and natural gas provides energy for generating stations, compressors, and storage, all of which are necessary for the operation of electric power networks. This reciprocity can be found among all lifeline systems.

In Figure 1, some of the interdependencies among seven infrastructures are depicted. In particular, telecommunications need water for cooling, power and fuel for feeding, and gas for heating. Telecommunications are mandatory for SCADA (Supervisory Control and Data Acquisition) networks that are the communication infrastructures of the other lifeline systems.

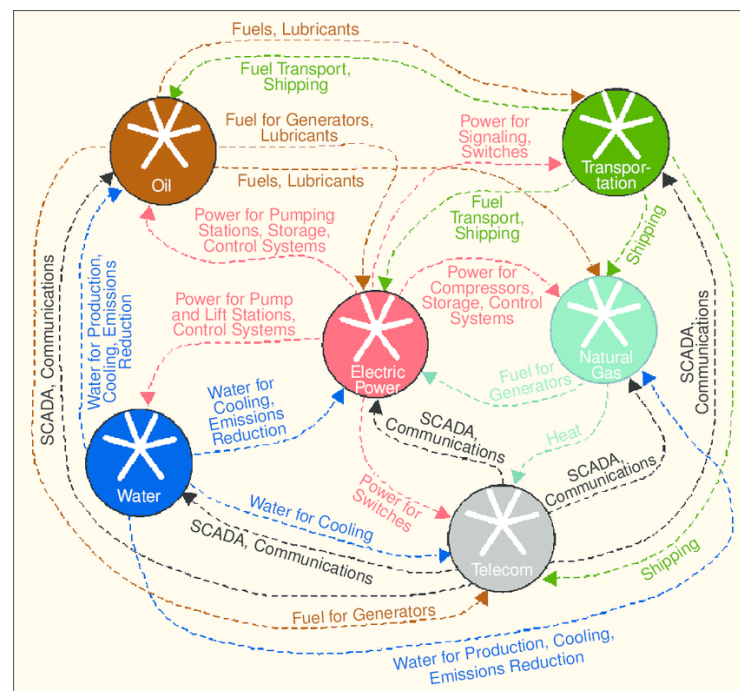


Figure 1 – Example of interdependencies among critical infrastructures from [6]

Resilience is defined in Webster's Unabridged Dictionary as "the ability to bounce or spring back into shape, position, etc., after being pressed or stretched." Definitions vary slightly, but they all link the concept of resilience to recovery after physical stress.

Since Hurricane Katrina, there has been a notable shift in emphasis from protecting critical infrastructure to ensuring that communities are resilient. When translating new ideas or concepts that connote a particular quality, such as resilience, into policy and implementation in the real world, we must remain mindful of the human dimensions of communities, which cannot be easily adapted or convolved into concepts based on the recovery of physical entities.

In addition, the concept of resilience, like the concept of critical infrastructure, is evolving. In its current form, the resilience of a community is an overarching attribute that reflects the degree of community preparedness and the ability to respond to and recover from a disaster. Because lifelines are intimately linked to the economic well-being, security, and social fabric of a community, the initial strength and rapid recovery of lifelines are closely related to community resilience.

Debate is likely to continue about the concept of resilience, and refinements and elaborations of the term are to be expected. Engineers and social scientists at the Multidisciplinary Center for Earthquake Engineering Research (MCEER) have proposed a framework for defining resilience. [7] According to [8], resilience for both physical and social systems can be conceptualized as having four infrastructural qualities:

- **Robustness:** the inherent strength or resistance in a system to withstand external demands without degradation or loss of functionality.
- **Redundancy:** system properties that allow for alternate options, choices, and substitutions under stress.
- **Resourcefulness:** the capacity to mobilize needed resources and services in emergencies.
- **Rapidity:** the speed with which disruption can be overcome and safety, services, and financial stability restored.

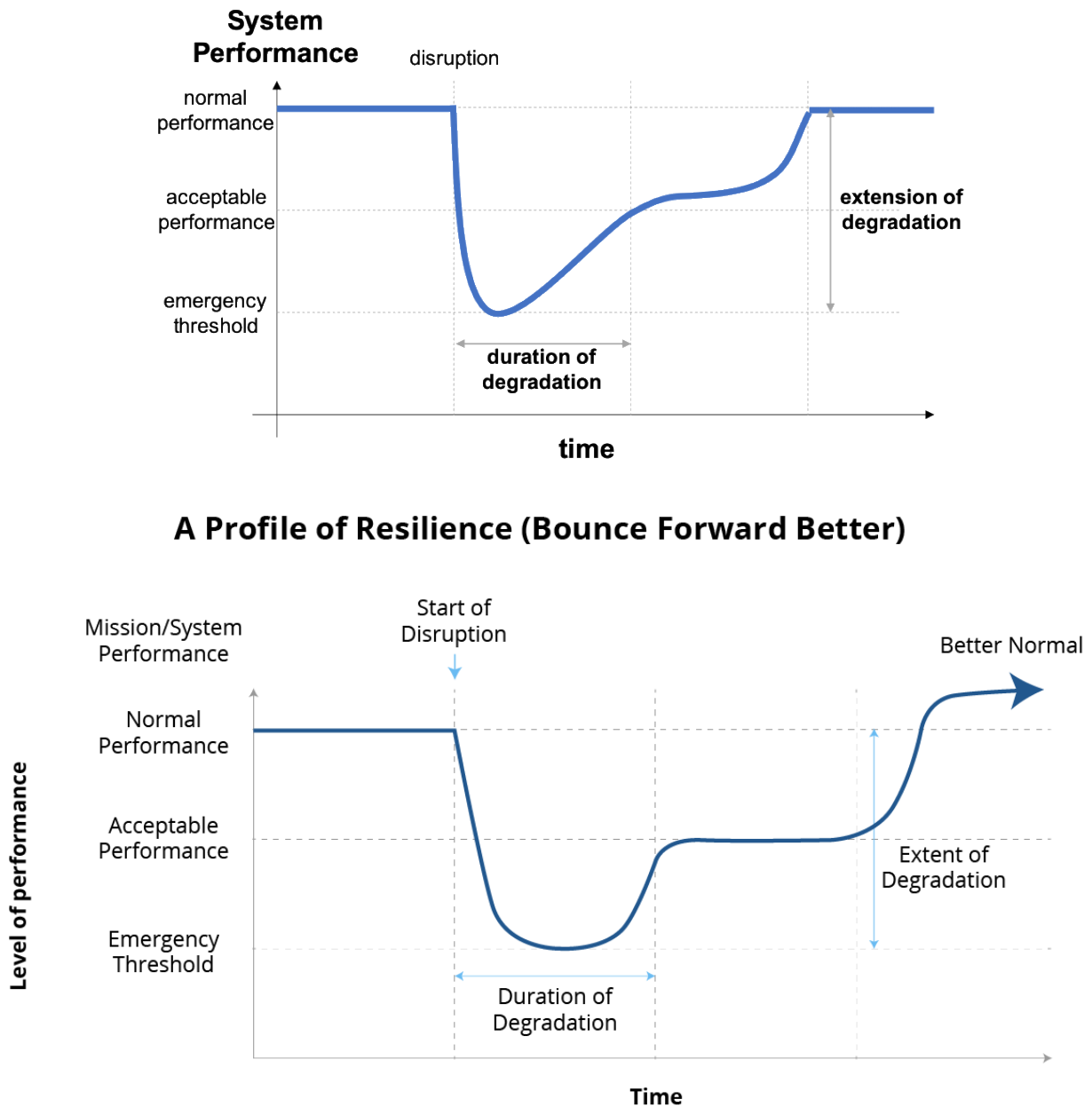


Figure 2 – Representation of resilience profile from [6].

As illustrated in Figure 2, an infrastructural performance, $Q(t)$, can be visualized as a percentage that changes with time. For buildings, $Q(t)$ may be the percentage of structural or functional integrity. For lifelines, $Q(t)$ may be the percentage of customers with water or electric power. Prior to a natural hazard, severe accident, terrorist act, or a general disruption, $Q(t)$ is at 100 percent; in picture is defined as normal performance. If the system is fully resilient, it remains at 100 percent. Total loss of service results in 0 percent $Q(t)$. If system disturbance occurs at time t_0 , in response to an earthquake or hurricane, for example, damage to the infrastructure may reduce the quality to less than 100 percent, the emergency threshold. Level of service, as reflected by the robustness of the system, is a function of the probability and consequences of damage. Robustness is restored over

time; at time t_1 , the system is returned to its original capacity. We called “duration of degradation” the time for the system to bounce back to an acceptable performance.

For a community, loss of resilience, R , can be measured as the expected loss in quality (probability of failure) over the time to recovery, $t_1 - t_0$. Thus, mathematically, R is defined as:

$$R = \int_{t_0}^{t_1} (1 - Q(t)) dt$$

The resilience factor, R , is a simple measure for quantifying resilience. Additional mathematical developments of this concept addressing the probabilistic and multidimensional aspects of resilience are explained elsewhere [7].

The resilience framework also addresses the technical, organizational, social, and economic dimensions of infrastructure. Each intersection of the matrix in Table 1 has examples of technical, organizational, social, and economic activities that support the qualities of a resilient community. Robustness, for example, is considered in terms of technical dimensions, such as building codes and retrofitting procedures. Robustness is linked organizationally to emergency personnel and operations planning, and socially through the preparedness and vulnerability of different neighbourhoods. Robustness is further related to the economic diversification in a given community or group of communities.

A more detailed analysis of the concept of resilience can be found in [14].

2.2. The Concepts of Risk and Resilience

The concepts of risk and resilience are similar and usually they are tight connected: improving the resilience of the system means decreasing risk. Risk is usually organised in terms of preparedness, mitigation measures, response capabilities, and recovery mechanisms; the traditional components of resilience are anticipation, absorption, adaptation and recovery.

The resilience of critical infrastructures is enhanced by owner and operators that perform specific operations: withstanding to specific threats, minimizing or mitigating potential impacts, returning to normal operations if some degradations occur. A resilience methodology requires to:

1. Increase preparedness for an incident,
2. Implement redundancy to mitigate the effects of an incident
3. Enhance emergency action and business continuity planning and implementation for response and recovery procedures.

In Figure 3, the resilience cycle is presented in five different steps: prepare, prevent, protect, response and recover. When considering interdependencies among critical infrastructures, the resilience cycle must consider the consequences of interdependencies. The RESISTO platform is an innovative solution for communication CIs for improving situation awareness and enhancing

resilience. The Risk Predictor runs in a fast control loop and it can help the operators in the recovery phase, knowing which the possible consequences of actual adverse events. The Risk Predictor aim is to assess the consequences of adverse events on critical infrastructures in terms of components, services and holistic view.



Figure 3 - Resilience cycle phases

The Department of Homeland Security (DHS) defines risk as “the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences”. [9] Risk is thus traditionally defined as a function of three elements: the threats to which an asset is susceptible, the vulnerabilities of the asset to the threat, and the consequences potentially generated by the degradation of the asset.

Threat is a “natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property”. [9] Sometimes the term hazard, which can be defined as a “natural or man-made source or cause of harm or difficulty” [9], is used instead of threat. However, a “hazard differs from a threat in that a threat is directed at an entity, asset, system, network, or geographic area, while a hazard is not directed”. [9] Vulnerability is a “physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard”. [9]. Consequences are the “effects of an event, incident, or occurrence”. [9]

If risk is a function of threats and hazards, vulnerabilities, and consequences, the challenge is to define where and how resilience fits into the determination of risk. In this deliverable, we consider the resilience as strictly depending from the definition of risk: the resilience is a function of the risk when time is explicitly considered.

Risk management can be defined as the “process of identifying, analysing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost”. [9]

Risk management involves knowing the threats and hazards that could potentially impact a given facility, the impacts on the facility due to its vulnerabilities, and the consequences that might result. Based on these characteristics, it is possible to develop specific indicators and metrics to assess the risk to an organization.

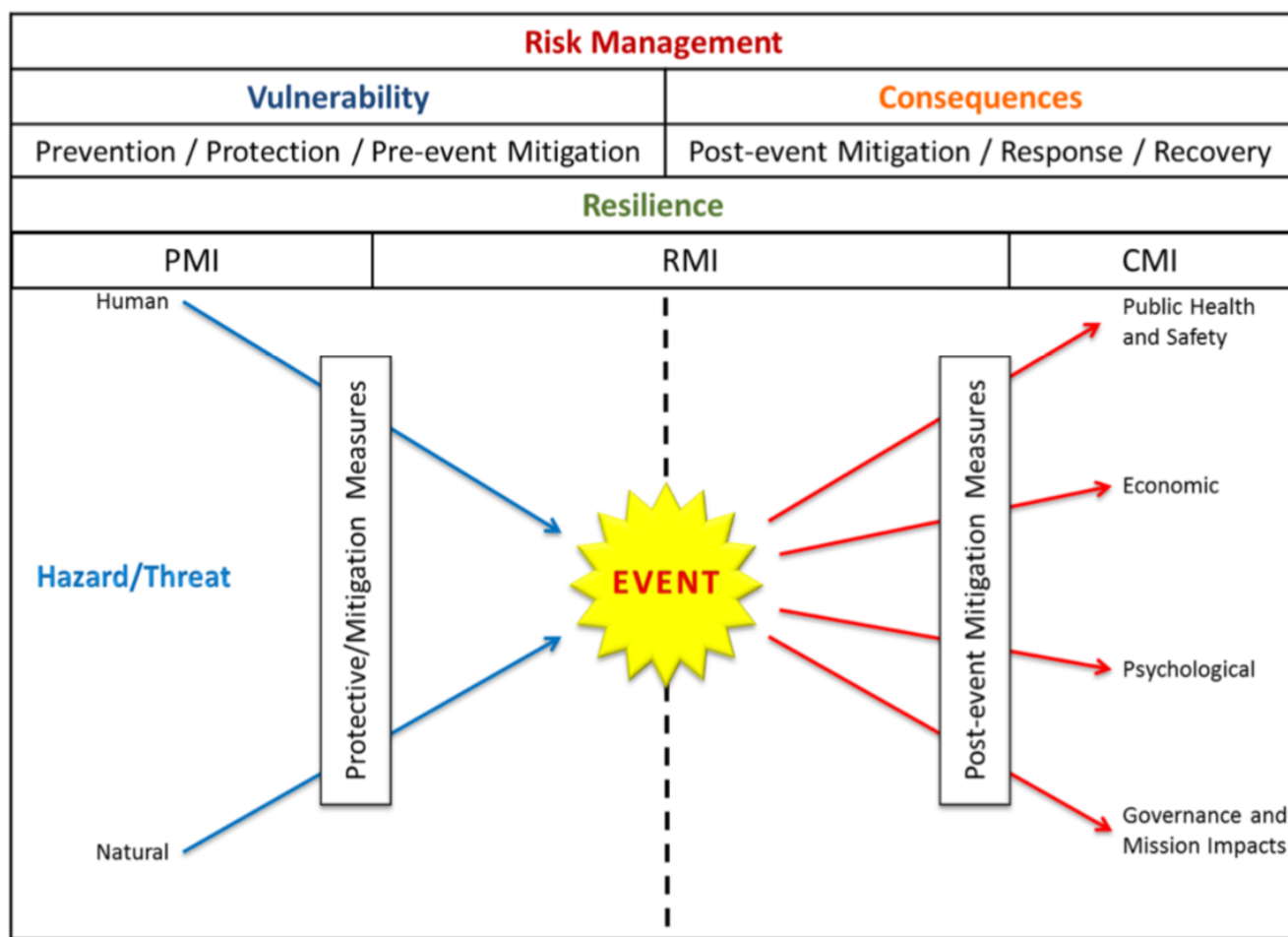


Figure 4 – Risk and resilience management from [10], where PMI is Protective Measurement Index, RMI is Resilience Measurement Index and CMI is Consequences Measurement Index

The risk management bowtie is represented in Figure 4, where threats, vulnerability, consequences and resilience fit together in a risk management process. Considering a threat or hazard (man-made or natural), the vulnerability and resilience of an organization will impact the potential consequences of an event. The interaction between the elements of risk is complex and made more so when one considers the transfer of risk between assets in the case of a threat by an intelligent adversary.

2.3. Modelling Interdependencies with MHR approach

During decision process, the available information is related to actual threats and fault on the infrastructure. The operator, based on his experience and his knowledge of the system, can also make decisions on the consequences of the actual adverse events. Modelling activities, and specifically a simulator for assessing which are the domino effect of an event or an action, can help in improving the situation awareness and in reducing risk while improving resilience.

In literature, there are three main methodologies for the modelling approaches of critical infrastructure modelling: agent-based simulation, input-output analysis and network modelling. In literature it is possible to find heterogenous and/or unclassified approaches [12].

The agent-based simulations consider each infrastructure as complex adaptive systems, composed of agents representing single aspects in the infrastructure itself. Different agents can be modelled at different degrees of abstraction based on the proposed level of resolution modelling. The main advantage of agent-based simulation is the ability to arise synergistic behaviours when agents are starting to interact together [6].

The second approach is based on the Input-Output economic analysis introduced by Leontief in the early 1930s, but then adapted to modelling infrastructures. Haimes and Jiang developed the linear input-output inoperability model (IIM) to study the effect of interdependencies on the inoperability of interconnected networked systems. [11] For example, we consider a two-system model. When failure of subsystem 1 leads to subsystem 2 to be 80% inoperable, and a failure of subsystem 2 makes subsystem 1 to be 20% inoperable, the effect of functionality loss due to an external perturbation can be calculated by solving the Leontief equations. The main advantage of the IIM and its improvements is related to the simplicity and flexibility of the proposed approach. Usually, IIM is limited to the economic costs of interdependencies.

In the last years, researchers explored new approaches for modelling infrastructure interdependencies. The most promising approach is based on graph and network theory. In this approach, infrastructures are represented using abstract graphs made of nodes and arcs, standing for links between components in the infrastructures. The main advantage is to exploit closed form expressions and numerical simulations to characterise their topology, performance and uncertainty.

In this document, we propose an already applied approach, for helping during the modelling phase. The Mixed Holistic Reductionist (MHR) [13] approach was created to exploit the advantages of both methods: holistic and reductionist. The main aim of MHR approach is to give a possible guideline to properly model critical infrastructures and their interdependencies.

In holistic modelling, infrastructures are seen as singular entities with defined boundaries and functional properties, generating a global and overall analysis. Seeing an infrastructure as a single element aims at identifying and characterising the different infrastructures and their geographical level. At this level, the amount of data needed for modelling activities is very low and can be found in public databases. For example, in Figure 1 we can describe interdependencies among different infrastructures, such as telecommunication and electrical grid.

On the other hand, reductionist model emphasizes the need to fully understand the roles and the behaviour of individual components to truly understand the overall infrastructure. The reductionist approach drills down to each component in terms of inputs and outputs. At this level of abstraction is easy to find dependencies between equipment and single components, such as routers and firewall in telecommunication or breaker and generators in electrical grids.

Different levels of analysis are required in modelled systems and their boundaries are lost in the event of complex case studies. With the MHR model, relationships between infrastructures could be seen at different levels through either a top-down or bottom-up approach. The other main advantage is to model infrastructures at different level of abstraction considering the amount of available data.

The connection point between the two levels of abstraction, i.e. holistic and reductionist approaches, is the quality of service (in the following, abbreviated as “service”) evaluation which is a key element for operators. This layer describes functional relationships between components and infrastructure at different levels of granularity. In MHR, services to customers and to other interconnected infrastructures are explicitly considered as a middle layer between holistic and reductionist agents.

The MHR allows us to reach the right level of detail with minimal data and collected information. Some important considerations can be summarised in the following:

- Each infrastructure is modelled starting from the identification of components and their interactions;
- Each layer is defined with an appropriate level of abstraction based on information coming from end-users, stakeholders and open documents;
- Each component (we called it entity or agent) must be described in a way to decouple it from other components: the behaviour of the component must depend on the valued explicitly exchanged with the other components;

MHR approach allows to define three different typologies of entities:

- Holistic entities;
- Service entities
- Reductionist entities.

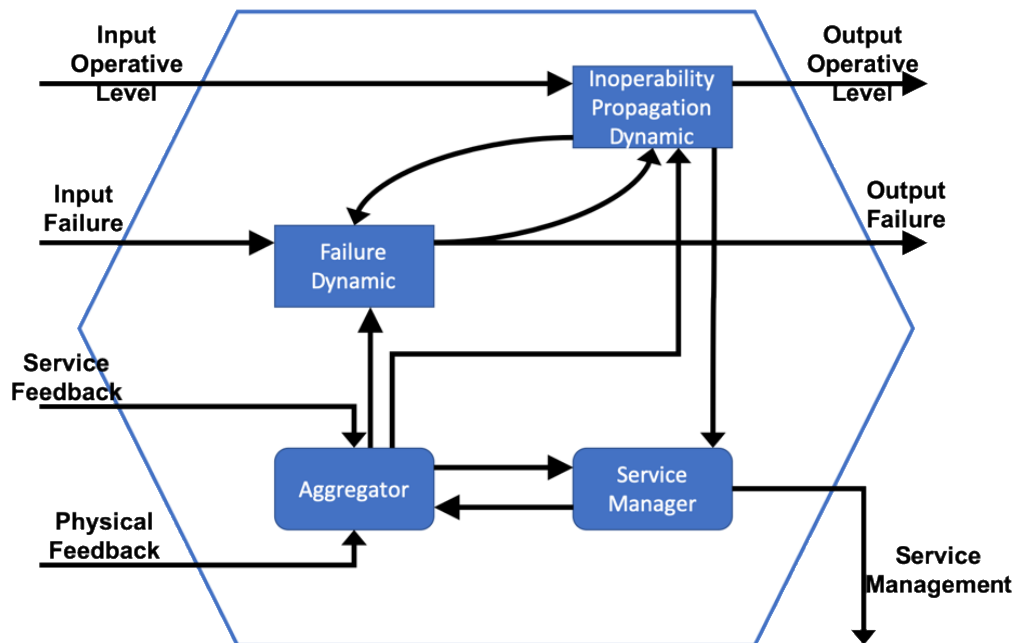


Figure 5 – Holistic component in MHR approach

An Holistic Entity (Figure 5) represents the infrastructure as a whole (or its general organizational divisions) in order to have a model that can consider the global dynamics between infrastructure possibly one might think of representing behaviours related to policies, strategies, etc..

A Service Entity represents a logical or organizational element, that provides an aggregate resource as the remote control: the remote control generally refers to a solution that provides supervision, by means of software and data collection. Data can be collected through telecommunication network or field equipment in case of a geographically distributed infrastructure. In Figure 6, a service component is depicted considering the classical model of an agent in CISIApro 2.0. Some examples of service are:

- the ability to supply customers
- the ability to produce resources
- the ability to change topology
- the status of some specific and important components

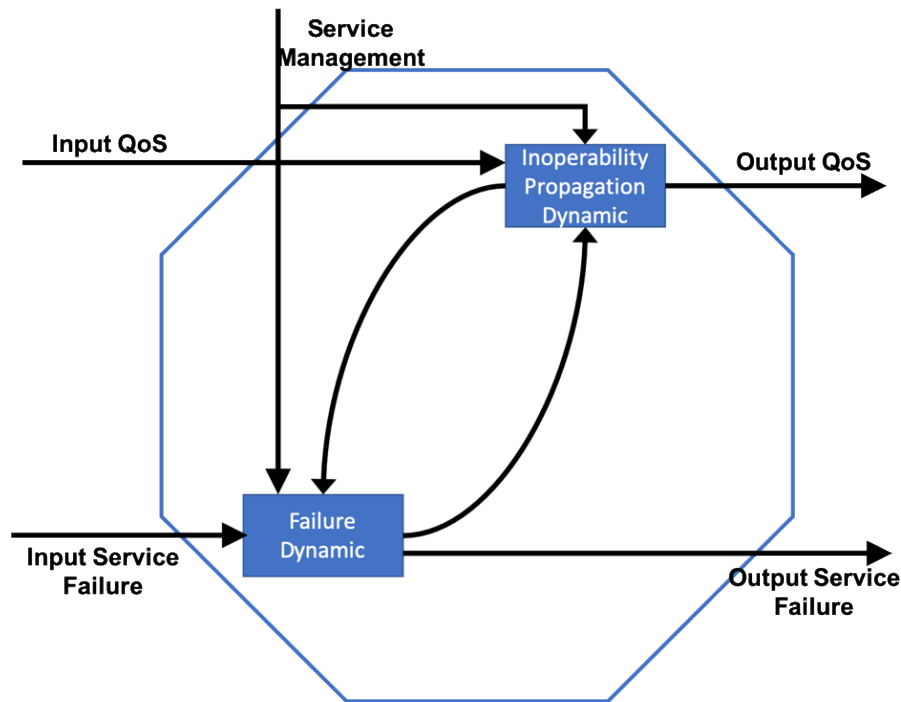


Figure 6 – Service component in MHR approach

Finally, with a Reductionist Entity, we can represent, with the right degree of abstraction, all physical or aggregated entities of the overall system. In Figure 7, the representation of a reductionist component is depicted. The picture does not explicitly consider a cyber threat: this malicious event can be represented in the same way as an input failure with a suitable “cyber dynamic”.

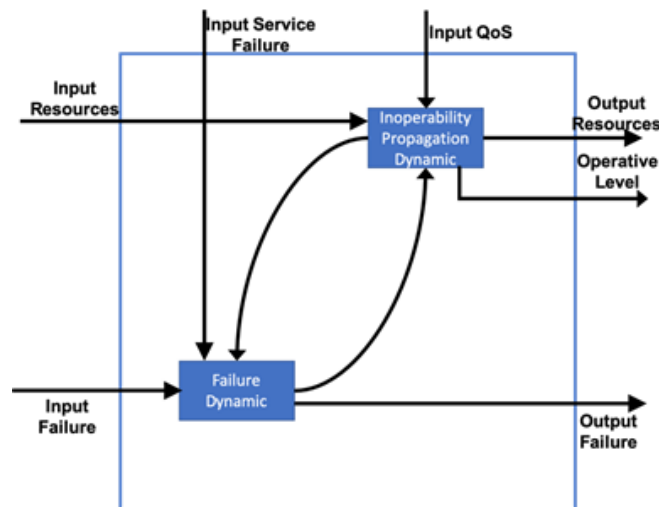


Figure 7 – Reductionist component in MHR approach

The MHR approach allow the developer to represent a complex scenario into components that have different functionalities. The layers allow to model a complex scenario, made of several interconnected infrastructures, with different abstraction levels: an infrastructure can be modelled in all its features (reductionist, service and holistic layers) , another can be modelled using only the holistic layer, without any kind of problem apart from the granularity and the precision of the results.

2.4. Risk Prediction related KPIs from D3.7 (RM3)

The main aim of RESISTO is to enhance the resilience of telecommunication infrastructures. In this context, this section provides metrics and KPIs to quantify resilience for the telecommunication infrastructures and in particular, to measure the resilience enhancement and improvement by the implementation of the RESISTO platform.

In detail, the Risk Prediction aims to improve the resilience of the phases of the resilience cycle after the event (after-event phases), that include the stages: “respond” or “remediate and recover”.

Therefore, Table 1 shows metrics and KPIs related to the Response and Recovery stages, described in detail in Deliverable 3.7, indicating if they are already defined by the project (Deliverable 3.8) or can be included and the potential contribution offered by the Risk Prediction.

Table 1 KPIs from D3.7 RISK Predictor related				
Response and Recovery Stages				
No.	KPI / Metric Title	Justification / measurement method	Inclusion in D3.8	Potential Contribution (Applies to) Risk Prediction
2.1	Performance loss	To measure the time-dependent system performance and to quantify resilience	Extended	Contributes to assess the global/holistic level of performance
2.2	Decision-making time (average)	To measure the degree on reducing the decision-making time	Define by the project	May help to reduce
2.3	Mitigation Time (average)	To measure the effectiveness of the RESISTO platform so that performances loss could be recovered in a short time	Define by the project	May help to reduce
2.4	RESISTO platform Reliability	Indicates the success rate in processing the ingested alarms the number of alerts/events sent to the platform should be the same with the number of alerts/events processed	Extended	Applies to
2.5	Incident Correlation / Propagation Index	Measuring the impact of the threat on the network and its propagation likelihood (cyber-physical threats and interconnected CIs)	Extended	Contributes to assess propagation
2.6	Down Time during Incident	Duration of the disruption (time period that the system is "down" / not available)	Define by the project	May help to represent
2.7	Human intervention / automated response	The degree that the platform could enables the reaction and mitigation by automating some of the actions and decreasing the human intervention time	Extended	Risk Prediction increases the situation assessment hence may allow the passage to an automated response

3. REQUIREMENTS

In this Chapter we make a fast analysis of functional and non-functional requirements of RESISTO architecture indicating which are the requirements that can be supported in their fulfilment by the Risk Predictor. In this way, it will be clearer the contribution of such component to the whole platform. A scale Low-Medium-High have been used and some notes try to explain the importance of Risk Predictor when level is High.

3.1. Functional Requirements

Table 2 Functional Requirements		
Requirement Identity Code	Requirement Description	Contribution of Risk Prediction Platform
RES_FUN_0005	RESISTO shall exploit the outcomes of the cyber security and the physical security systems of the TLC infrastructures (if existing).	High – security events will be propagated to the physical infrastructure
RES_FUN_0030	The RESISTO system shall be able to receive, collect and process alert events relevant to physical detection.	High – also physical events will be collected and propagated to the whole infrastructure
RES_FUN_0060	The RESISTO system should collect events coming from the existing external systems of the end users (e.g. notified by the operating system and by the hardware event collector, the removal of system hardware like disks, changes in the Hardware/Software configurations)	Low
RES_FUN_0100	The RESISTO system shall collect non-authorized personnel access inside the telecom facility if provided by the operator	Low
RES_FUN_0110	The RESISTO system should be able to help avoiding telecom facility equipment and/or private information theft by collecting data from specific sensors and providing mitigation measures	Low
RES_FUN_0210	The RESISTO system should state the criticality of the attack	High – a level of risk will be calculated after the propagation of adverse events
RES_FUN_0220	The RESISTO system should inform the operator on first impact	Medium
RES_FUN_0240	The RESISTO system should estimate impact propagation of an attack, also to other interconnected CIs	High – propagation of impacts is the first aim of Risk Predictor
RES_FUN_0275	The RESISTO system should include audio and visual analytics functionalities.	Medium

3.1.1. Input data

Table 3 Input Data		
Requirement Identity Code	Requirement Description	Contribution of Risk Prediction Platform
RES_FUN_0280	The RESISTO system should be able to receive threat and alert related data from the cloud platform or other systems	High – Risk Predictor is able to ingest negative events coming from many sources
RES_FUN_0310	If the operation requires spatial-temporal information, the input data of the RESISTO system should include desensitized/non-desensitized spatial-temporal data, depending on the use cases, e.g. the geo-location information of infected devices	Medium
RES_FUN_0320	The input data of the RESISTO system could also include data sources containing the network information, e.g., the network traffic directional data, if network information are needed for the operation and response	High – network information can be processed and ingested in the Risk Predictor
RES_FUN_0350	RESISTO could be able to receive and process data from Telcos' fault management systems. These include network faults, equipment faults, and etc	Correlator Mediated
RES_FUN_0560	The Risk (Impact) Predictor shall also include a network impact as well	High – the impact on the TLC network is calculated as well
RES_FUN_0570	The Risk and resilience assessment analysis shall also take into consideration network single point of failure nodes, using network metrics such as: <ul style="list-style-type: none"> - Link state protocol databases for alternative IGP routes - BGP secondary paths for EGP routes HSRP/VRRP/GLBP statuses for gateway redundancy. 	High – if connected to such data sources Risk Predictor can better exploit the propagation of negative events

3.1.2. System Reports and Other Outputs

Table 4 System Reports and Other Outputs		
Requirement Identity Code	Requirement Description	Contribution of Risk Prediction Platform
RES_FUN_0845	RESISTO should be able to classify information or security events (for example Traffic Light Protocol - TLP)	High

3.1.3. Functional Requirements related to 5G

Table 5 Functional Requirements related to 5G		
Requirement Identity Code	Requirement Description	Contribution of Risk Prediction Platform
RES_FUN_1107	The RESISTO system shall be able to order the seamless relocation and restoration of virtualized network resources in the event of failure or cyber/physical attack if provided by the operator control system, such that service continuity can be guaranteed	Low

3.2. Non-Functional Requirements

3.2.1. Design Requirements

Table 6 Design Requirements		
Requirement Identity Code	Requirement Description	Contribution of Risk Prediction Platform
RES_DCC_0040	Some modules of the RESISTO system should support virtualization at the OS level for fast horizontal scaling in the Datacenter environment.	High - visualization can scale easily
RES_DCC_0050	The RESISTO system should be available for different network types	High – the modelling approach can be used with different network models

3.2.2. Interface Requirements

Table 7 Interface Requirements		
Requirement Identity Code	Requirement Description	Contribution of Risk Prediction Platform
RES_INT_0010	The user interface of the RESISTO system should give the operator a summary of all the events occurred on systems, with the ability to drill down a particular event to investigate and to have a historical view of similar events, and review the necessary steps taken to resolve the issue	Low
RES_INT_0020	RESISTO should be able to represent several Dashboards, one for Real Time events, and one with historical data	Low
RES_INT_0060	The common user interface components of the RESISTO system could include visual analytics by geo-location	Medium
RES_INT_0080	The user interfaces of the RESISTO system should also include the navigation functionalities to navigate through the spatial representation of the data	High – the Risk Predictor output can be used to navigate data

RES_INT_0090	The RESISTO system should include drill down information and analytics pages or views when clicking on different visualizations of data	High – Risk Prediction software can bring deeper information to the operator
RES_INT_0100	The user interfaces of the RESISTO system should include options for the users to set up and select different models and to visualise the prediction results	High
RES_INT_0120	RESISTO should include alerts and their severities. Clicking alerts should drill down to details of the alerts, i.e. what triggered the alerts and the data behind (evidence support them)	High
RES_INT_0130	The RESISTO system should offer a holistic view of network healthy highlighting what networks running smoothly and what networks have unresolved issues and their severities are color or shape encoded so operators could easily to see	High

4. A TOOL FOR IMPACT ASSESSMENT: CISIAPRO 2.0

The Risk (Impact) Predictor (RP) will simulate the impact of anomalies and security attacks on the Communication Infrastructure and on the interlinked CIs executing at run-time on a model of the Communication Infrastructure. It will also support the decision-making process allowing a “What-If analysis” by simulating the application of countermeasures and reconfiguration and their impact on system resilience. The Risk Predictor is mainly composed by CISIApro 2.0. therefore, the two names are for us equivalent.

CISIApro 2.0 (Critical Infrastructure Simulation by Interdependent Agents) [15] is a software engine able to calculate complex cascading effects, considering (inter)dependencies and faults propagation among the involved complex systems. CISIApro 2.0 can eventually consider also the mitigation and restoration actions to assess the conclusion of an adverse event.

CISIApro 2.0 is an agent-based simulation software and is mainly composed of two modules. The first one is the off-line tool known as CISIApro in which it is possible to design and implement complex and highly interdependent scenarios. While the second one is the on-line tool called CISIAmat which exploits Simulink (Mathworks) for the real-time engine at the core of the Risk Predictor module.

CISIApro 2.0 is a software platform based on a database-centric architecture in which the database plays a crucial role. This means a centralized asynchronous design that allows good modularity and scalability where each element of the informatics infrastructure interfaces, independently, with the centralized database in order to get the last actualized data from the field. For the implementation of the engine simulator, the Matlab language was used to develop a redistributable Matlab App.

4.1. CISIApro 2.0 – Dynamic Risk Analysis Tool

This section describes the Risk Predictor architecture, commonly adopted in Critical Infrastructure Protection (CIP) projects, in order to provide a new type of Dynamic Risk Assessment tool. Such a tool is based on CISIApro (Critical Infrastructure Simulation by Interdependent Agents) software engine, which is able to calculate complex cascading effects, taking into account (inter)dependencies and faults propagation among the involved complex systems. CISIApro has been developed inside the H2020 Project ATENA and in RESISTO will be update to version 2.0 adding some important functionalities related with the modelling of telecommunication infrastructures.

As mentioned in section 5.2 of deliverable D2.4 [16]., modelling complex interdependent systems, using the Mixed-Holistic-Reductionist (MHR) approach, is a prerequisite to produce an effective Risk Predictor tool. Once modelled the involved scenario, with CISIApro 2.0 it is possible to implement the MHR methodology.

CISIApro 2.0 is an Agent-Base simulation software and it is mainly composed by two modules. The first one is the off-line tool known as “CISIApro 2.0 Design” that allows the design and implementation of complex and highly interdependent scenarios. While the second one is the on-line tool called CISIAmat which represents the real engine at the base of the Risk Predictor module. This engine will be integrated in the RESISTO architecture as in Figure 8.

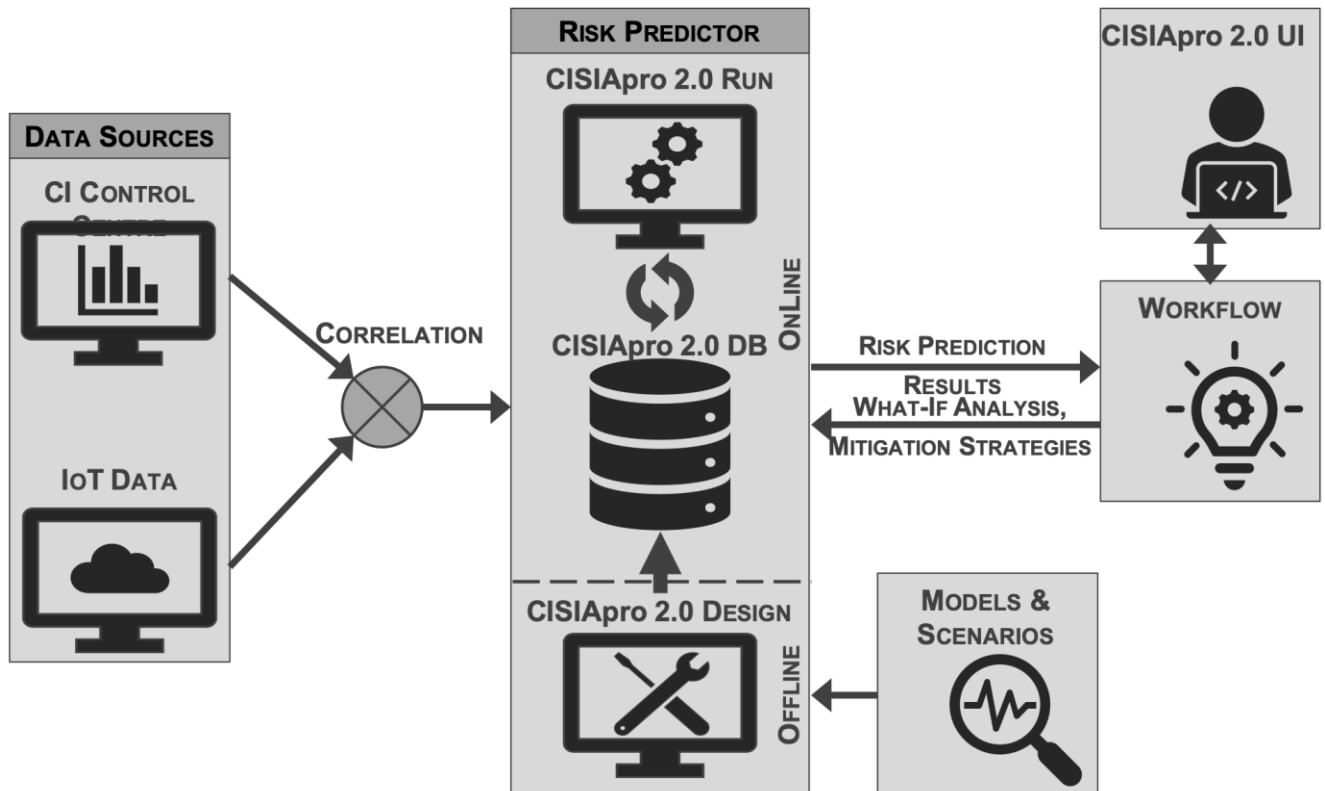


Figure 8 – Risk Predictor Architecture

CISIapro 2.0 is a software platform based on a database-centric architecture in which the database plays a crucial role. This means a centralized asynchronous design that allows a good modularity and scalability where each element of the informatics infrastructure interfaces, independently, with the centralized database (DB) in order to get the last actualized data from the field (e.g. SCADA Systems or Network Operation Centre), Complex Event Processing and generic IoT (Internet of Things) data systems.

From this point of view, CISIAMat engine does not only analyze actual situation and calculate the risk projected in the possible near future but, first, it plays the important role of Hybrid Risk Evaluation Tool. Hybrid because it is able to get information of different natures (sensor and data acquisition and complex event processing systems) and translating them in operational levels of resources, faults or services for the entities introduced in the critical infrastructure model.

With the proposed architecture, through CISIapro 2.0 modelling software, it is possible to dynamically change the interdependencies model and plugin other modules in order to have a pseudo-real-time scalable and flexible system, which can be changed at any time.

Figure 9 shows the database structure. The DB stores the information needed for the representation of several Critical Infrastructures, such as:

- Each entity is a specific instance of an entity type;

- Each entity has a status made of variables with values;
- Each entity has ports for exchanging resources;
- Each resource is associated with a MHR layer/net;
- Each layer has proper interdependencies;
- Each interconnection is made of a couple of ports, associated to two entities.

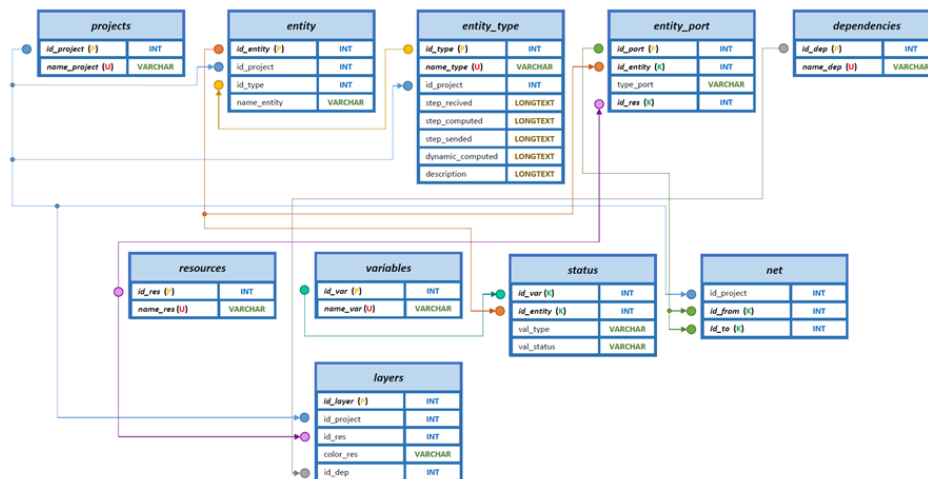


Figure 9 – CISIApro SQL data structure.

Outputs of CISIApro 2.0 are stored in a different database with specific features, see Figure 10, such as the record time-stamp in terms of date, time and milliseconds. In this way, any downstream module can retrieve data regarding the latest actualized critical situation in the modelled scenario. Adjacency matrices which represent interdependencies existing between entities are generated during the design phase. During the simulation, the matrices are represented as queue data structures to speed up computations.

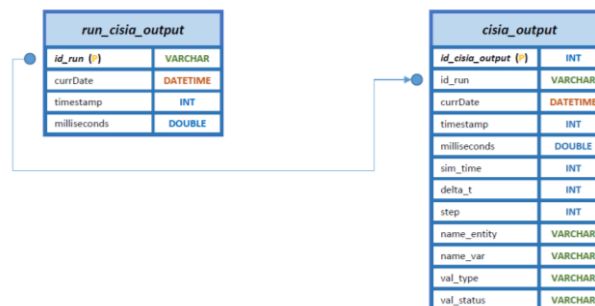


Figure 10 – CISIApro SQL output data structure.

It should be noted that CISIApro 2.0 has introduced efficient ways to model, execute and debug simulations and cascading effects. In particular, an intuitive Graphical User Interface (Figure 11) is provided to create entities and connect them in easy way.

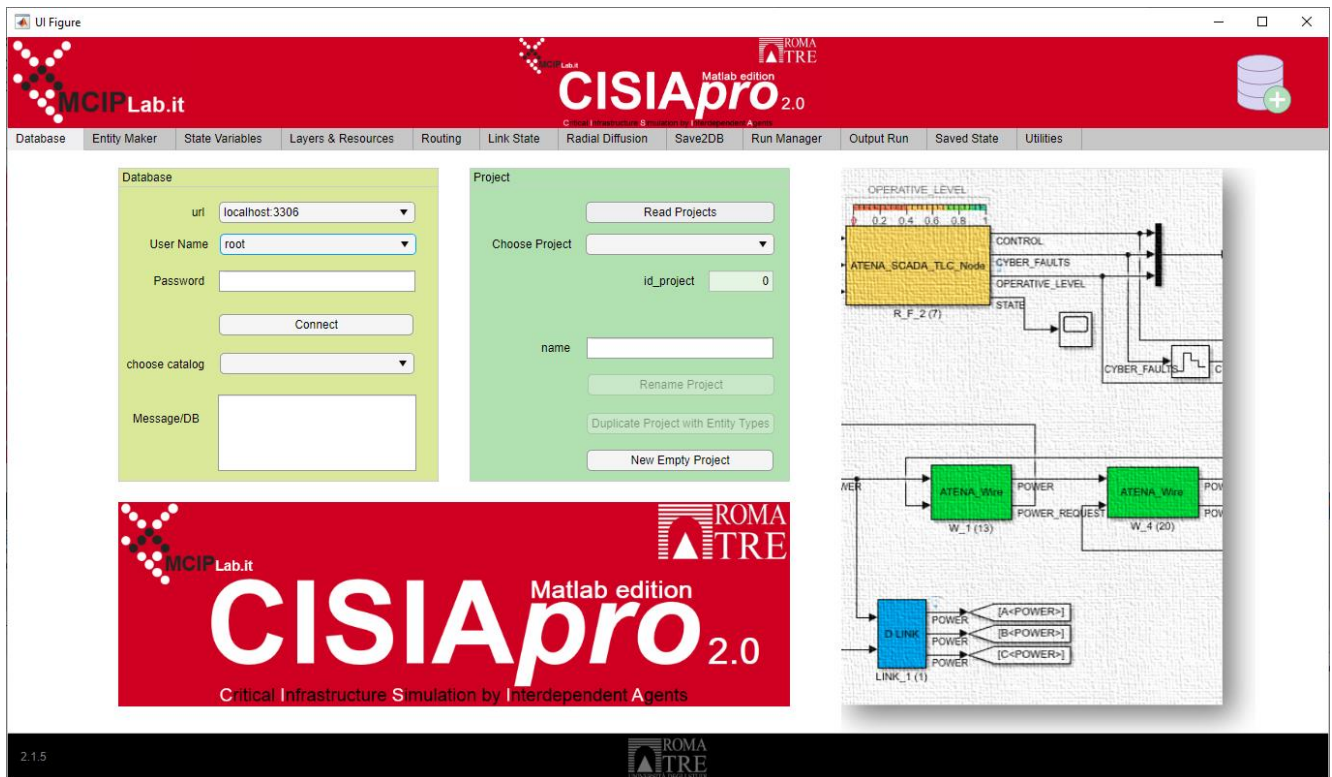


Figure 11 – CISIApro user interface.

Below are presented some brief descriptions regarding the main modules provided by CISIApro design tool to exploit the potential of proposed modelling techniques.

4.2. Layers & Resources Module

Thanks to the Layers & Resources module (Figure 12) it is possible to instantiate all the required layers in a critical infrastructure's scenario model. It is the first step for the simulation implementation. Assign a specific resource to a corresponding dimension also gives us a deeper awareness with respect to the nature of the managed information.

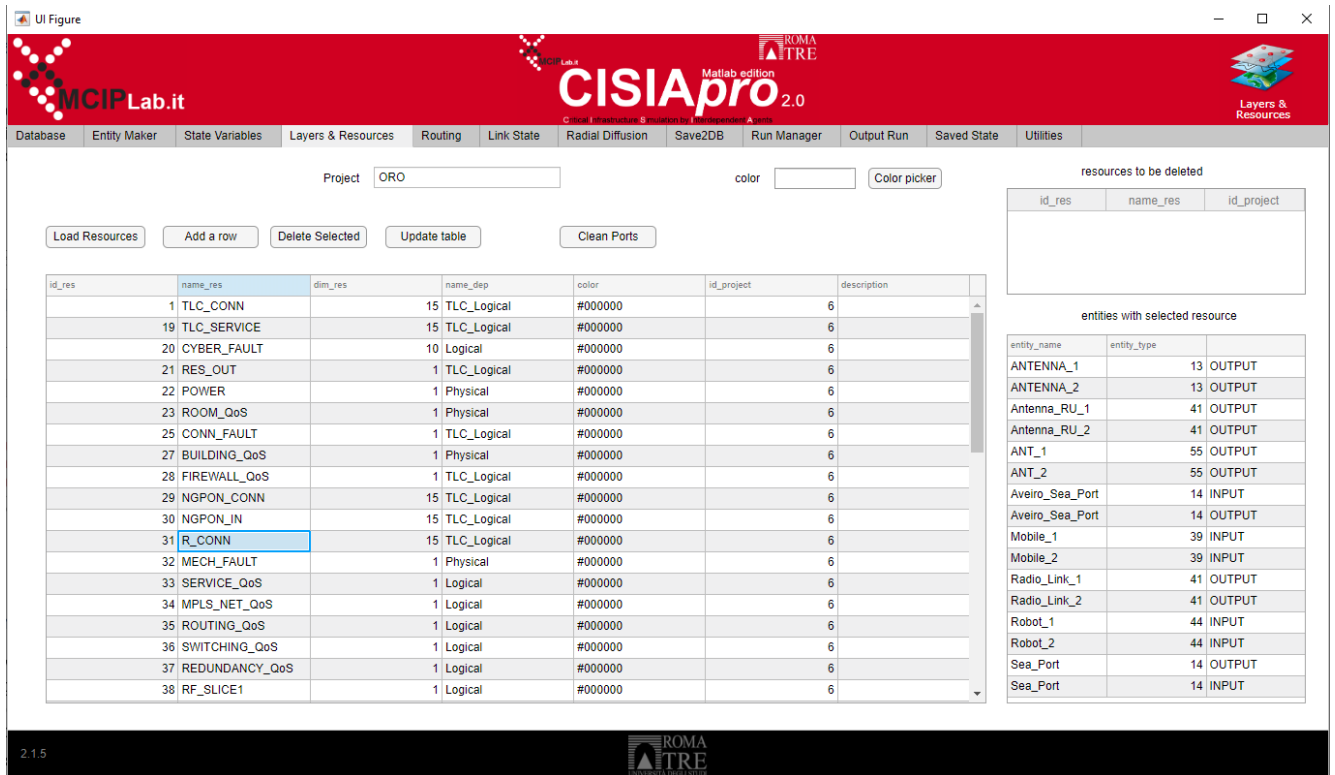


Figure 12 – CISIapro Module: Layers & Resources.

4.3. Entity Maker Module

In the Entity Maker module (Figure 13), using the integrated PHP code editor, it is possible to instantiate and programming behaviours for each considered entity class. Once completed this step, the introduction and duplication in the design phase will be allowed. Each entity class is composed of four modules that are executed, several times, during the simulation run:

- **RECEIVED**, which evaluates the received resources and faults;
- **DYNAMIC COMPUTED**, which implements dynamic evolution;
- **INSTANT COMPUTED**, which implements instantaneous evolution;
- **SENT**, which evaluates the resources that are sent to the downstream entities.

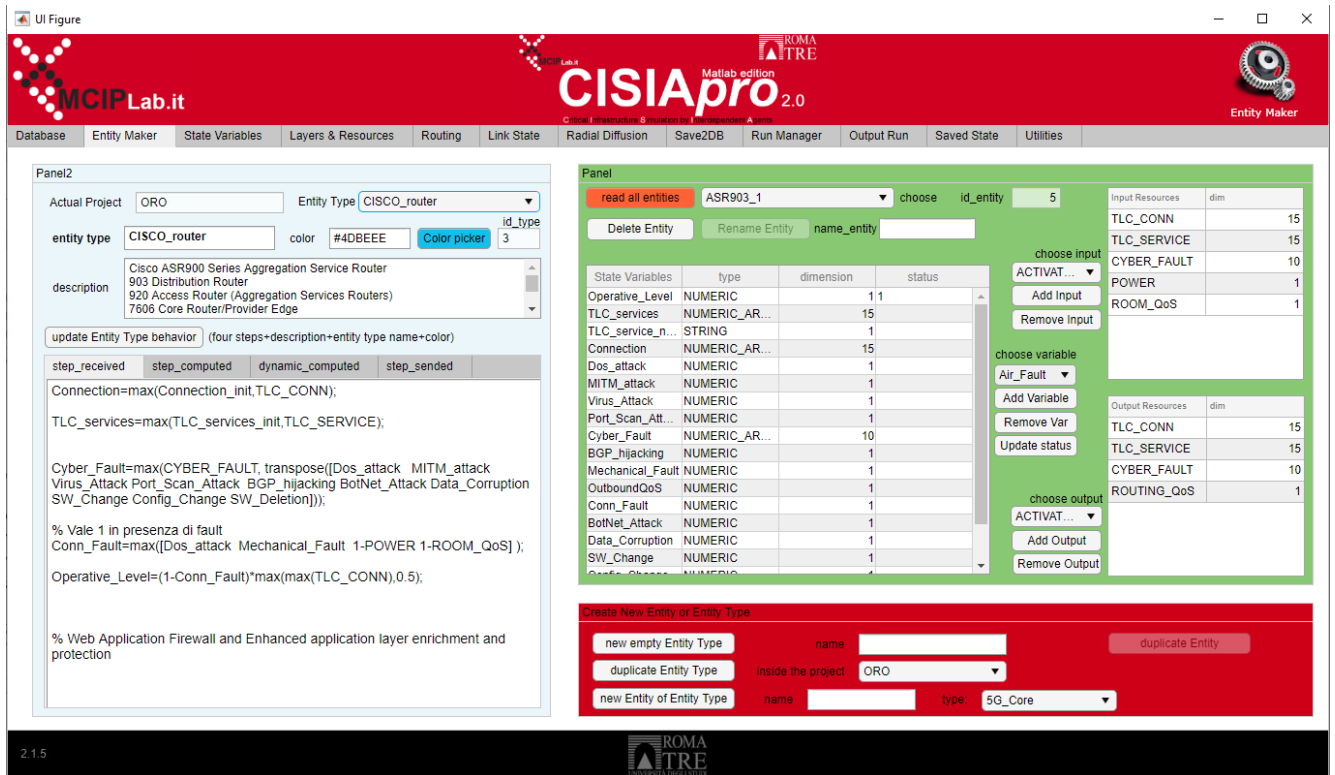


Figure 13 – CISIapro Module: Entity Maker.

4.4. Modeler Module

The Modeler, in the new version of CISIapro 2.0, has been developed using SIMULINK (MATLAB) modelling approach (Figure 14). The choice has been motivated considering the rapid prototyping of such environment and its ability of mixing block of CISIapro with dynamic systems allowing the design of innovative applications.

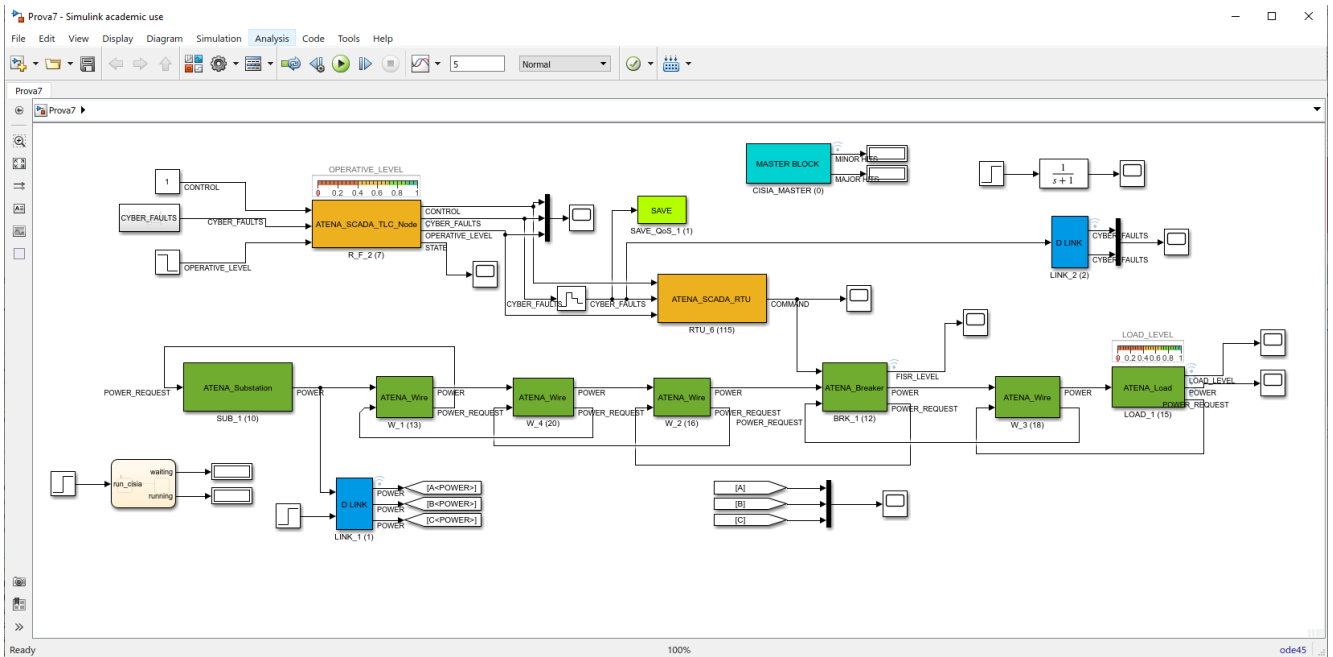


Figure 14 – CISIApro Module: Modeler.

4.5. State Variables Module

As previously mentioned, with CISIApro 2.0 simulation, defining Input and Output is not required. This is possible because they are calculated, instant by instant, during the simulation time, with respect to entity state variables and especially evaluating operational levels related to each modelled element. In State Variables module (Figure 15) indeed it is possible to set the initial state for every variable that is part of the simulation.

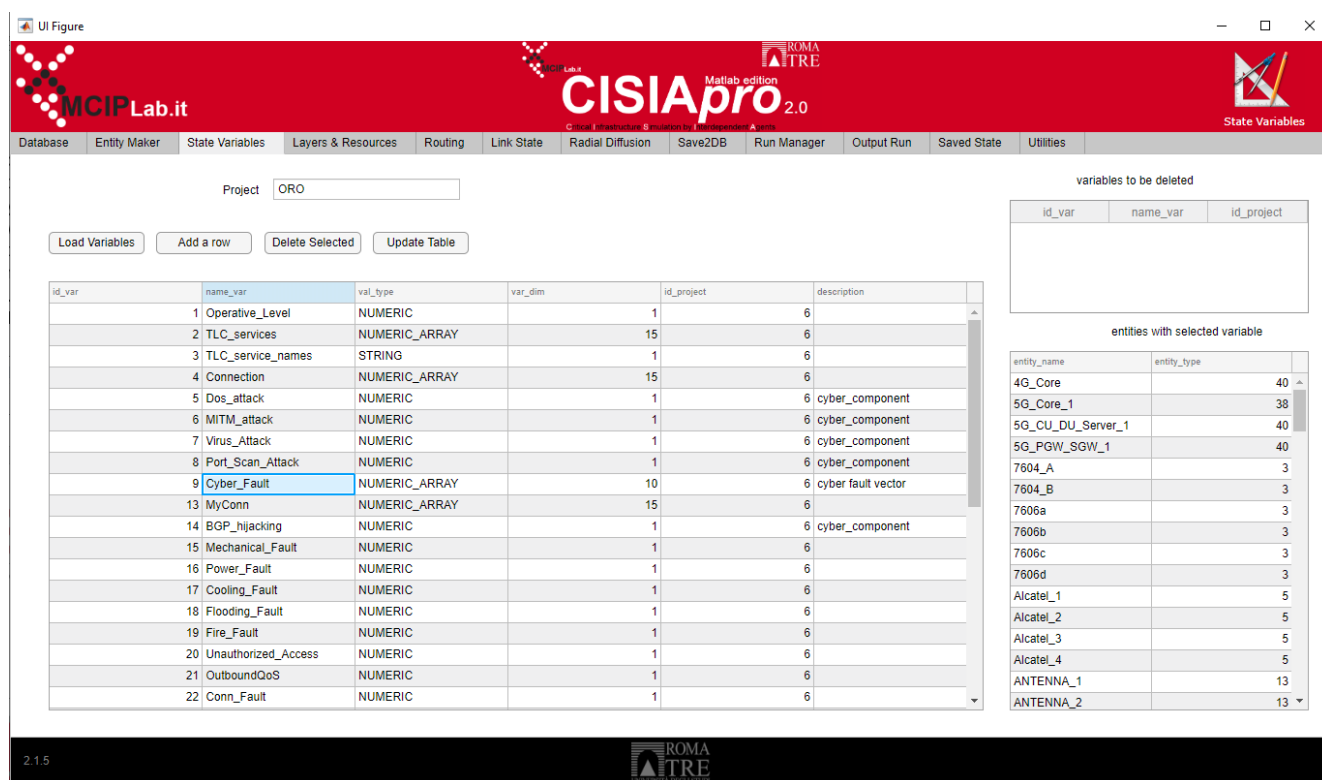


Figure 15 – CISIApro Module: State Variables.

4.6. Link States Module

Dynamic Links is the most recent module tool introduced in CISIApro 2.0 software for RESISTO scenario model needs (Figure 16). Such module was designed in order to be compliant to model in which dynamic links are required. A dynamic link is defined as a link that connects two entities to each other, which could change its state during different simulation. For instance, it allows to model scenarios, like transportation infrastructures or telecommunication networks, where an entity may represent an element of the system and links represent multiple available paths (e.g. SDN dynamic routing). Through this mechanism it will be possible to instantiate all the multiple connection, among the involved entities, activating only one of them at a time.



Figure 16 – CISIapro Module: Link State.

4.7. CISIamat – the CISIapro 2.0 on-line engine

Usually Risk Analysis and Business Continuity are mainly focused on prevention and consequences mitigation. In RESISTO case study a pseudo-real-time performances monitoring is also considered in order to have an ongoing decision support system.

In RESISTO project CISIamat engine is part of the Short-Term Control Loop. The Short-Term Control Loop continuously monitors the CI system and its cyber-physical state, in order to detect the presence of failures/attacks in a real-time environment. To defend against such attacks, the Short-Term Control Loop shall compute domain specific mitigation actions and propose them to the RESISTO operator, in order to enforce them into the underlying plant and preventively mitigate consequences on the service provision. The main aim of the on-line loop is to increase the awareness of the operator, displaying possible impact/consequences and exposure to risk with respect to the actual adverse events on the physical infrastructure and on the telecommunication network.

It is important to understand the primary role played by Risk Predictor (CISIapro On-Line engine) together with the Mitigation Module. First of all, CISIapro On-Line engine provides an impact evaluation of detected anomaly. In order to mitigate the effects, the Decision Maker, also supported by a Workflow Manager, can choose among different sequences of possible reaction strategies to

send to the Risk Predictor module. Risk Predictor, in turn, starting from actualized scenarios and QoS (Quality of Service) levels of involved devices, simulates What-If scenarios to provide useful information for the Decision Maker with respect to ‘forthcoming’ critical situations.

Thanks to CISIamat on-line engine is also possible to create, as already demonstrated in URANIUM [Ref4] and H2020 ATENA [Ref5] European projects, web-based synoptic platforms. Such projects made evident that it is important to provide an intuitive user experience in order to simplify and speed up decision processes in emergency situations. For instance, in URANIUM project (Figure 17) it was developed a GIS (Geographic Information System) demonstrating how it is possible to carry out a What-If analysis taking into account different emergencies procedures and considering available civil protection resources at a specific point in time.



Figure 17 – URANIUM platform civil protection panel.

Another important example is represented by ATENA H2020 synoptic platform (Figure 18). In this case, a What-If analysis procedure was exploited in order to test possible consequences of adopted Electrical Grid reconfiguration with respect to all interconnected critical infrastructure (Water distribution, Gas network and involved SCADA systems).

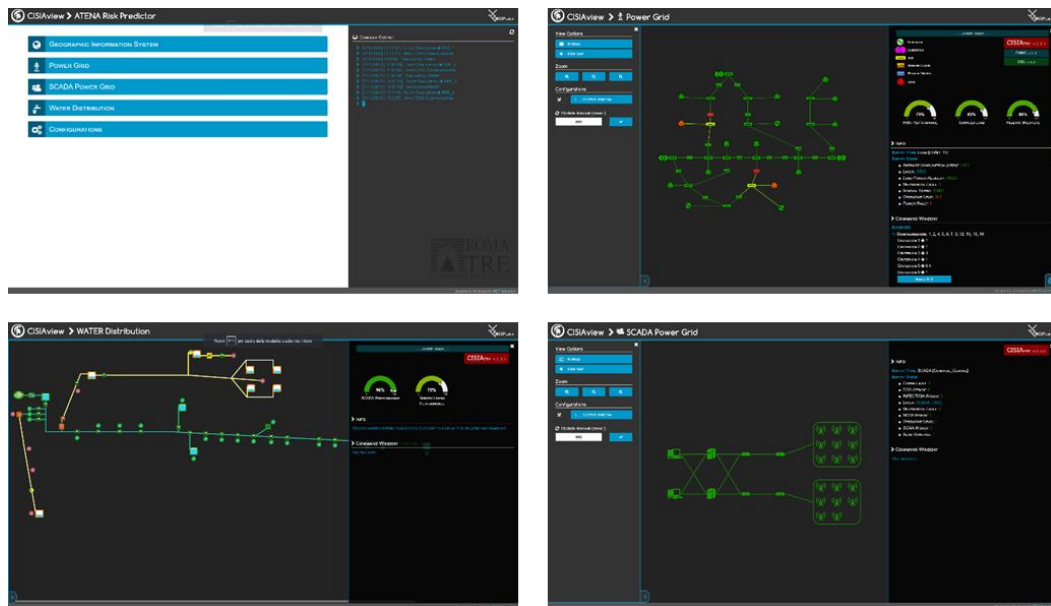


Figure 18 – ATENA Platform.

5. UNIFIED REFERENCE SCENARIOS

5.1. Unified Scenarios

For each use case described in Deliverable 2.8, a unified scenario was created with the aim of describing not only the application scenario but also the entire telecommunication network and the services it offers. Indeed, the use cases were used to extract the system requirements and, starting from these, an appropriate Telecommunication architecture and the services provided were defined, to model the scenarios described.

In this way, each use case becomes a particular instance of the specific unified scenario to evaluate possible impacts that threats or attacks have on the systems and therefore the active and compromised services.

In conclusion, a unified scenario is nothing more than a generalization of the telecommunication network, the services provided and the end users who use these services, to simulate the risk scenario explained in each specific use case.

The following table describes the unified scenarios defined to model the different use cases reported in the Deliverable 2.8.

Table 8 Unified Reference Scenarios		
Unified Scenario	Use Case	Main components
Unified Scenario 1	Use Case 1-2: Core Network Failure caused by Physical & Cyber-attacks or Natural Disasters to Telecommunication sites (OTE testbed)	Metro Network, POP L2 Building
Unified Scenario 2	Use Case 6: Cyber and physical protection of network and network elements mechanisms used by critical services that impact users (ORO testbed)	POP L1, Metro Network, POP L2 Building,
Unified Scenario 3	Use Case 9: 5G network response to a security breach (ALB Testbed)	POP L2, Aveiro Port Area, Mobile User
Unified Scenario 4	Use Case 4: Disruption of major sporting event by combined physical & cyber-attack by a terrorist organization (BTC Testbed)	Streaming Provider, POP L1, POP L2, 21th Century Network, Residential Building
Unified Scenario 5	Use Case 5.1: Protection of Cloud Storage Services - Healthcare system (TIM Testbed)	Core Network Cloud Services, POP L1, POP L2, Hospital

Unified Scenario 6	Use Case 5.2: Protection of Cloud Storage Services - 5G Smart Manufacturing (TIM Testbed)	Core Network Cloud Services, POP L1, POP L2, Smart Factory
Unified Scenario 7	Use Case 7: Maritime Safety and Emergency Case (RTV Testbed)	Core Network Cloud Services, POP L1, POP L2, Maritime Environment

5.2. General Telecommunication architecture for Unified Scenarios

To build the unified scenarios we have considered a general telecommunication architecture composed by core, distribution and access levels that has been customised for the different unified scenario. Here we describe such architecture to have a common reference for unified scenarios description.

The core layer is also referred to as the network backbone and consists of high-speed network devices. These are designed to switch packets as fast as possible and interconnect multiple components, such as distribution modules, service modules and the data-center. The OPB (optical packet backbone) network uses protocols such as MPLS or IP.

The distribution layer aggregates the data received from the access layer switches before they are transmitted to the core layer for routing to their final destination. The distribution network, also known as OPM network, is structured on two levels of multi-layer Switch equipment capable of handling traffic flows at the Ethernet, IP or MPLS level depending on the configuration created. The two levels of equipment are called Metro level and Feeder level. Metro level devices are installed in the PoPs of the OPB backbone and are usually connected to it with 10 Gbit/s connections. The Feeder level devices, that is the POP level 2, are instead installed in some other sites of the same metropolitan and regional area and have the function of collecting and aggregating traffic from the client apparatuses and the access network. The connections between the devices of the Metro level and of the Feeder level are all realized with 10 Gigabit Ethernet flows which guarantee a sufficient amount of bandwidth for the transport of the various types of services that make use of the OPM network for transport between the customer and the PoP of the network of backbone.

The access layer grants end devices access to the network. Serving fixed telephony and more generally telecommunication services dedicated to fixed devices, there are two distinct technologies:

- Connection on copper cable (telephone pair), characteristic for analogic telephone services and broadband in xDSL mode
- Fiber optic connection for access to broadband services

For mobile telephony, the access network consists of a network of two-way radio stations (base stations) arranged so as to cover adjacent areas of territory (cells), thus ensuring the continuity of radio coverage even in the face of end-user shifts.

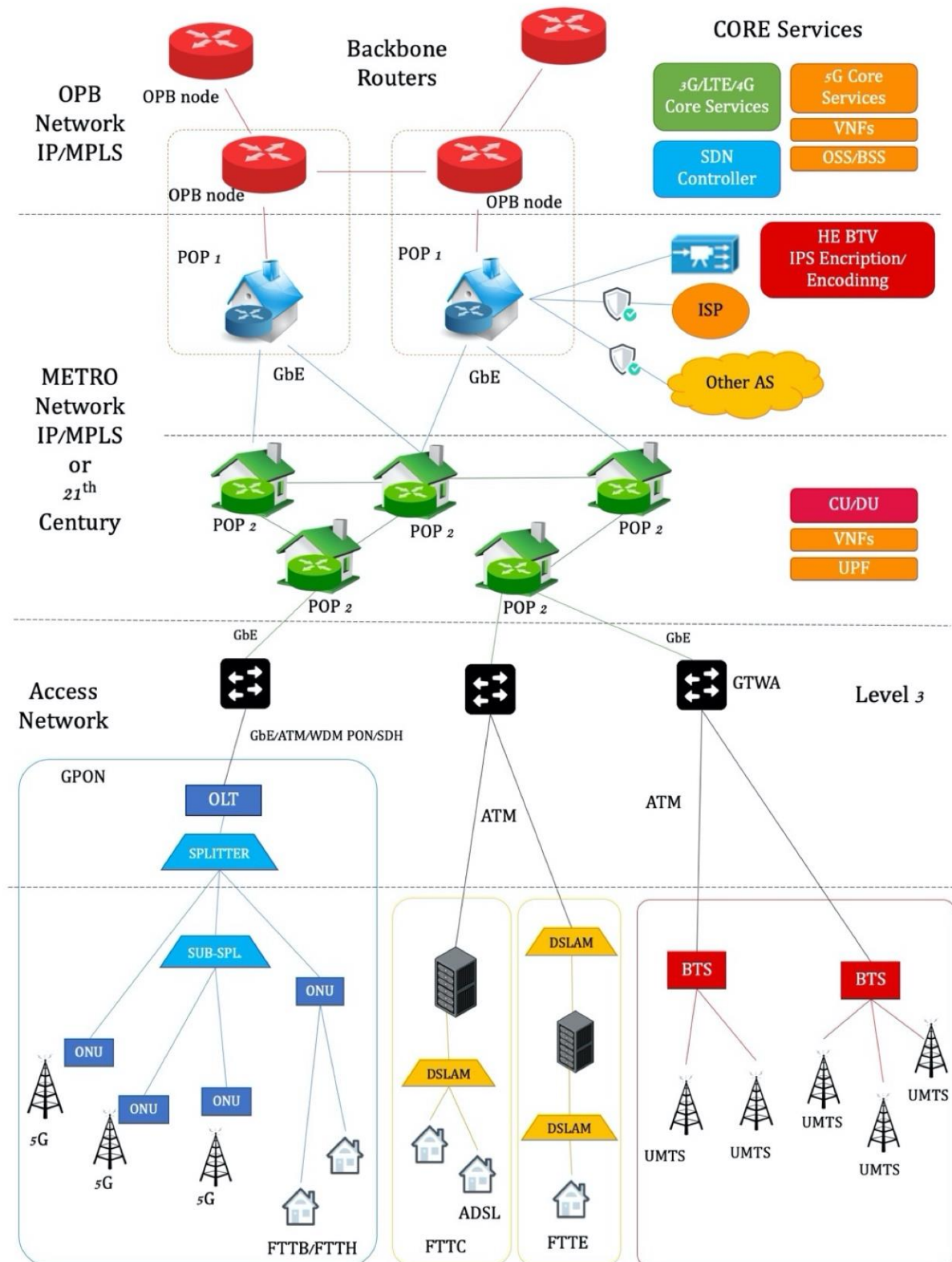


Figure 19 General Telecom architecture for Unified Scenario

5.3. End users modelling

Here we describe the end user models that have been used in conjunction with the Unified Scenarios to build the Use Cases.

5.3.1. Hospital

The hospital is a health care institution and consists of a complex of buildings and facilities, where specialized staff provide treatments to nurse patients. A health facility represents a critical infrastructure sector and as such, even if subjected to continuous criminal attacks, it must still guarantee adequate reception and care to people and, at the same time, minimize vulnerabilities.

The critical infrastructure that is taken into consideration is a single hospital ward, which is modelled as follows:

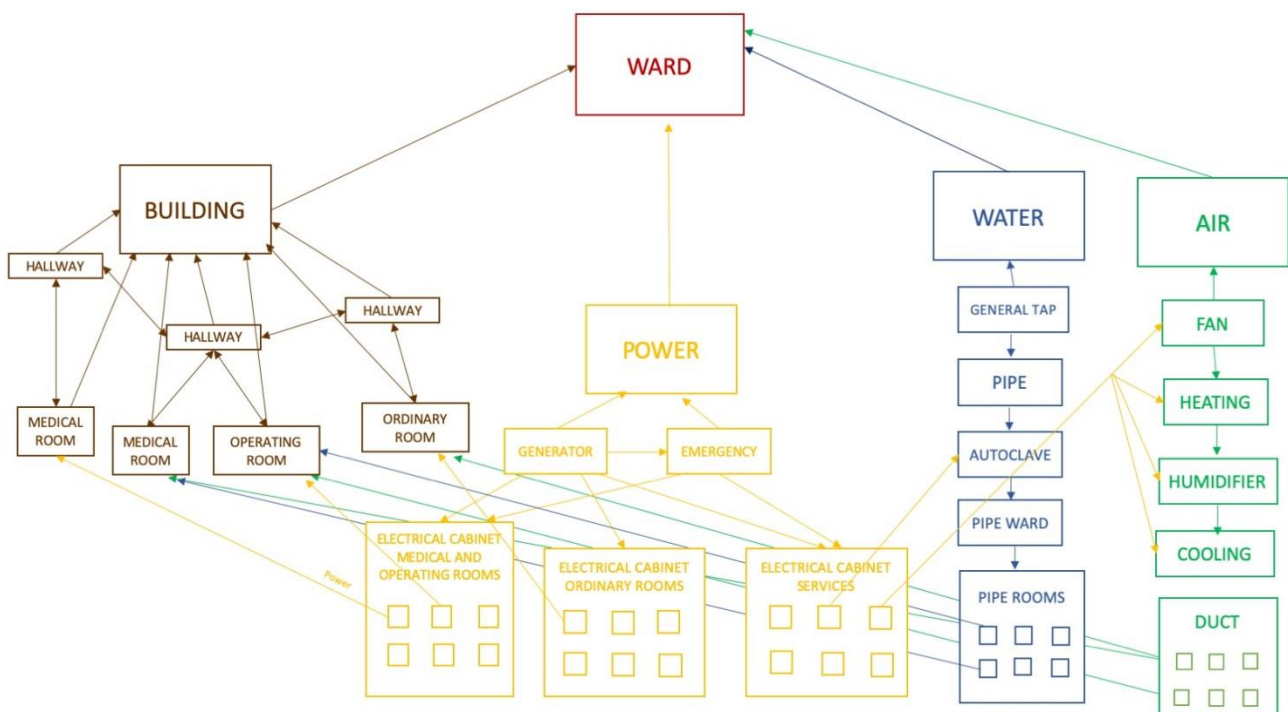


Figure 20 Model of hospital ward

The critical infrastructure is characterized by different systems, which are now described in detail.

From the plan, you can see that the structure consists of operating rooms, medical rooms for patients, ordinary rooms (such as doctors' room, staff room, waiting room, drug store...), emergency exits and hallway.

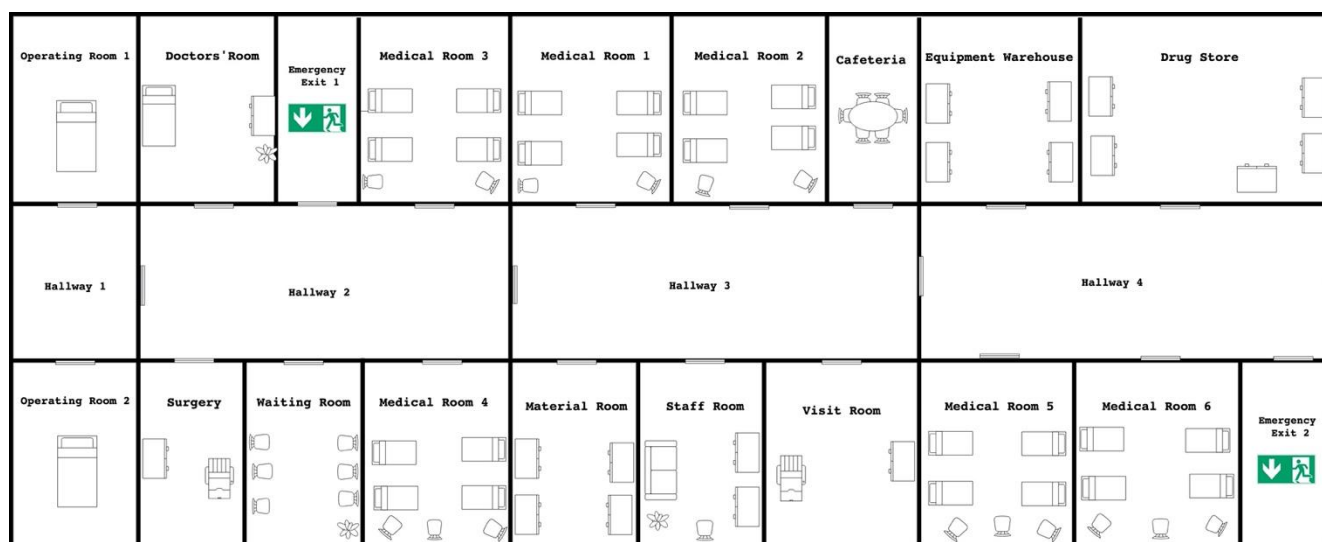


Figure 21 Plan of hospital ward

The medical and operating rooms are dedicated to the care of patients and for this they must continue to provide the services requested in an optimal manner even after a fault, unlike ordinary rooms that are less important than the previous ones: their malfunctioning does not clearly impact the quality of the service offered by the ward.

As discussed above, for each medical room a dedicated wire is defined: in this way, even in the event of fault, only the entity supplied by the specific faulty electrical cable suffers a lowering of the operative level, while the other rooms continue to function optimally. Instead for ordinary rooms and hallways, there are no dedicated cables, but a same wire supplies more rooms at the same time. The same reasoning is found for the water system: each medical room and each operating room has a dedicated pipe.

The state variables that characterize the entities for the building are:

- **Building**

Table 9 Entities and Variables for Building	
Entity	Variable
Ordinary Room	Operative Level
Emergency Exit	Power Fault
Hallway	Fire Fault
Medical Room	Operative Level
Operating Room	Power Fault
	Fire Fault

- **Electrical System**

The electrical network consists of a main generator, an emergency generator that is activated when the main generator stops working and a network of cables for distribution. Two different types of cables have been modelled: cables for medical rooms and services and cables for ordinary rooms: the first type of cable is connected both to the main generator and to the emergency generator so that the current, even after failures, continues to be supplied and to serve the main premises and services of the structure, while ordinary rooms, when there is a service interruption from the generator, will no longer be powered by any light source.

The variables considered for each entity are shown in the following table:

Table 10 Entities and Variables for Electrical system	
Entity	Variable
Generator	Operative Level Mechanical Fault
Emergency_Power	Operative Level Mechanical Fault
Wire_Medical_Room	Operative Level
Wire_Operating_Room	Mechanical Fault
Wire_Ordinary_Room	Power Fault
Wire_Service	

- **Water System**

The building's water system is equipped with a general tap, necessary to interrupt the supply of water in the event of leakage or maintenance. From the general tap, a pipe takes care of replenishing the first floors of the hospital, while for the rooms located on the upper floors it is necessary to equip the building with an autoclave to have enough pressure to push the water up to such heights. The general pipe of the ward branches off into a network of pipes, which is responsible for supplying water to the various rooms.

Table 11 Entities and Variables for Water system	
Entity	Variable
Tap	Operative Level Mechanical Fault
Autoclave	Operative Level Mechanical Fault Power Fault Water Fault
Pipe Pipe_Ward Pipe_Medical_Room Pipe_Operating_Room	Operative Level Mechanical Fault Power Fault Water Fault

- **Air Conditioning System**

Air conditioning systems are used in all health facilities to provide safe and comfortable environments for both patients and healthcare staff.

In hospitals air plays a key role: dirty environments, uncontrolled humidity and temperature, can be risky for both patients and staff, especially in particularly critical environments, such as operating rooms and analysis laboratories. Ventilation is the means to remove and replace air in the environment; in addition, ventilation equipment can also be required to eliminate smells and ensure the availability of fresh air. Air conditioning represents the ability to heat, cool, dehumidify and filter the air. This means that the climate in the rooms served can be maintained at a specific level regardless of the external conditions or the activities taking place in the rooms.

So, the HVAC system is characterized by following entities:

Table 12 Entities and Variables for Air Conditioning system	
Entity	Variable
Fan	Operative Level Mechanical Fault Power Fault
Heating Coil Humidifier Cooling Coil	Operative Level Mechanical Fault Power Fault Air Fault
Duct	Operative Level Mechanical Fault Air Fault

5.3.2. Smart Factory

A smart factory is characterized by automated and intelligent systems, which operate independently and in contact with the surrounding environment.

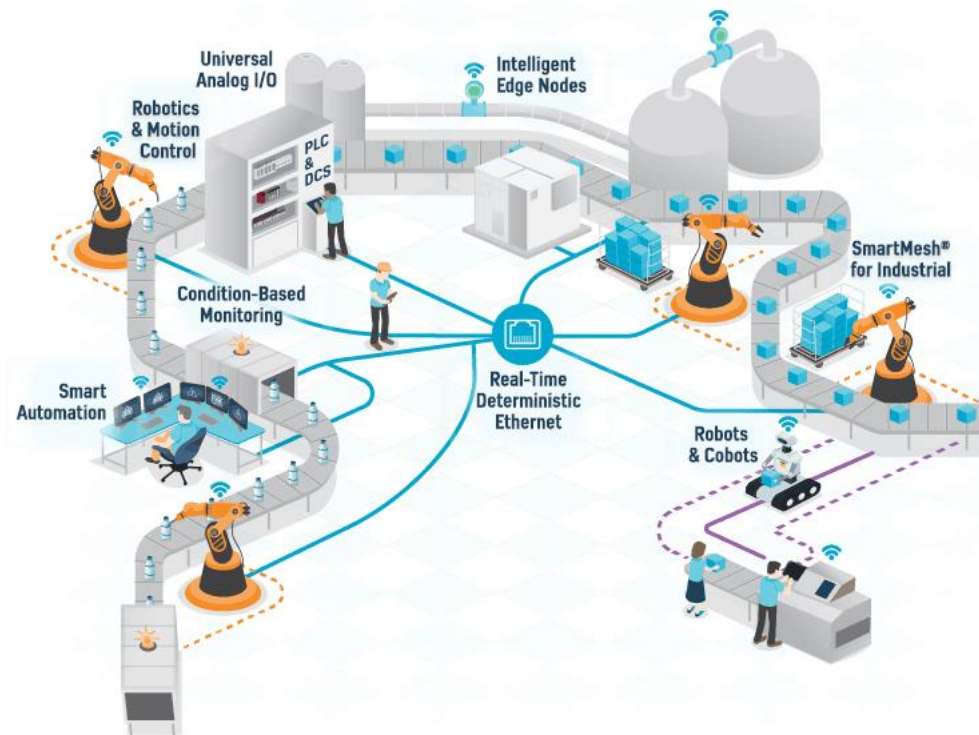


Figure 22 Smart Factory

The 5G network is the best solution for this scenario because it can provide the required wireless connectivity that allows mobility for connected devices, agility in operations and efficient connection to a cloud system.

As Ericsson states in the article “4G/5G RAN Architecture”, some 5G requirements, such as ultra-low latency and ultra-high throughput, require highly flexible RAN architecture and topology. This will be enabled by splitting RAN functions, including the separation of the user plane (UP) and the control plane (CP) in higher layers.

To model the smart factory, we refer to the following figure that shows an on-premises architecture that is fully self-contained using pico base stations and an on-premises data-center hub that stores content and carries out processing locally. In this case, all four RAN nodes (RF, BPF, PPF, and RCF) are integrated onto the same chip. The ideal split architecture contains pools of hardware (an SPP and GPP) strategically deployed in selected RBS and CO sites.

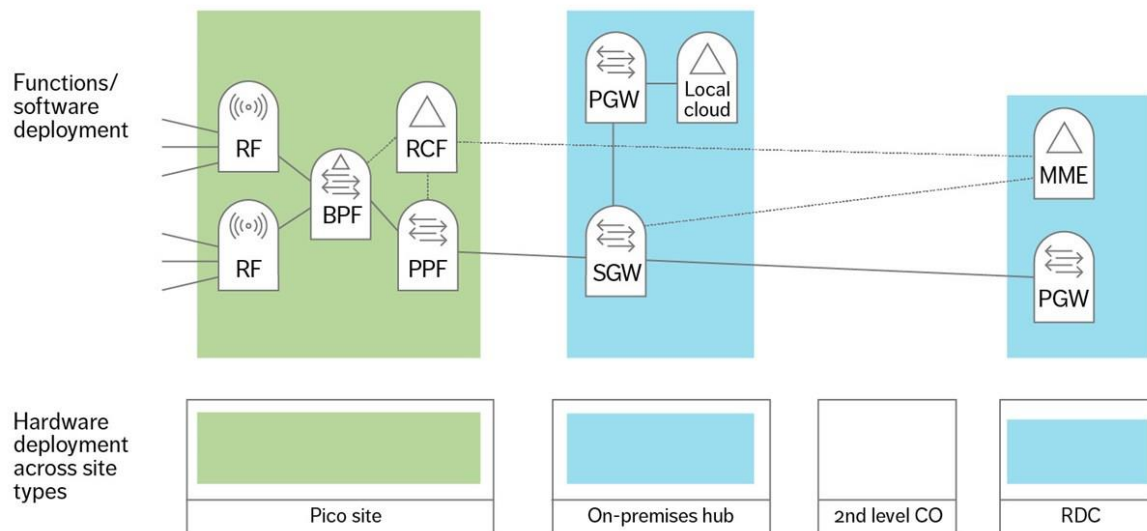


Figure 23 Factory deployment using pico 4G/5G base stations (green) and with on-premises breakout possibility

The design of the 4G/5G split RAN architecture focuses on increased spectrum efficiency, full deployment flexibility, and elasticity; processing is carried out where resources are available and needed. The split RAN architecture consists of the two user-plane network functions: a packet processing function (PPF) and a baseband processing function (BPF), together with the antenna-near radio function (RF), and the control-plane radio control function (RCF).

The PPFs and RCFs can each be deployed either in classical pre-integrated nodes or in fully virtualized environments as VNFs or any combination thereof. Both functions are suitable for virtualization with existing technology, with benefits to the PPF brought by packet accelerators and ciphering support in the underlying hardware.

The RCF takes holistic responsibility for Radio Resource Management, RAN analytics and SON, it maintains policy and bearer information, and interworks with non-RAN domains such as the EPC and resource orchestration layers. Deploying the user-plane BPF (processing synchronous to the TTI) and PPF (asynchronous packet processing) can be achieved in a variety of ways, as long as the BPF is within one to two TTIs from the antenna points. The PPF, on the other hand, can be more centralized, with a distance of up to 5-7ms from the radio functions. And so user-plane functions can be deployed to match service requirements, and maximize spectrum efficiency according to the spectrum, transport, and site availability, as well as the particular local geography.

The split architecture results in the necessary scaling dimensions to support 5G use cases and traffic structures in a cost-efficient way. Its flexibility and decoupling of hardware from software enables a software-defined elastic resilient RAN.

5.3.3. Aveiro Port

For Aveiro Port, we supposed to have an area within the Aveiro Port that is covered by two different Level 2 POPs and that the end-user is a mobile phone.

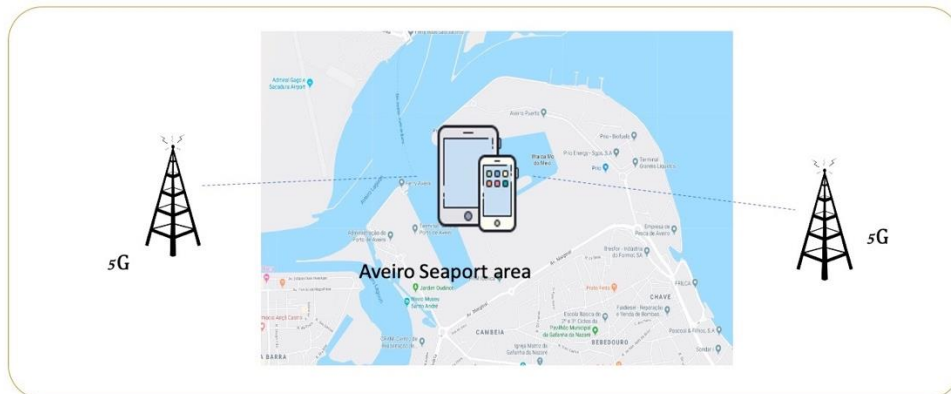


Figure 24 Aveiro Port

5.3.4. Maritime Environment

For the maritime scenario, we have considered Figure 25 in which a port authority is modelled. IoT sensors and video, taken from drones and cameras, are used to control boat access in the port. VHF Data Exchange System (VDES) is a radio communication system that operates between ships, shore stations and satellites on Automatic Identification System (AIS), Application Specific Messages (ASM) and VHF Data Exchange (VDE) frequencies in the Marine Mobile VHF band.

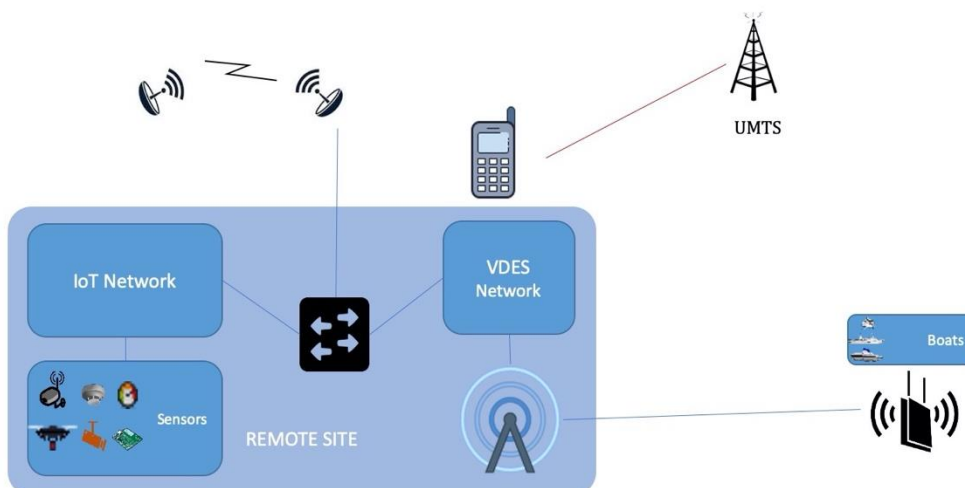


Figure 25 Maritime Environment

5.4. Emergency Warning Communications (EWC) and the RESISTO PLATFORM

The Emergency Warning Communication (EWC) is an application server created with the aim of extending RESISTO for the communication of emergency information to the "physical security" team. As soon as RESISTO identifies a fault or an unauthorized access to a remote site, it sends the alarm to the security team, through the EWFC app installed on the tablets, so that they can intervene suddenly in the field. EWC is able to warn several operators at the same time and to tell each of them how to act to solve the detected problem. The application server is equipped with a chat through which operators can communicate with each other and allows each member of the team to locate themselves on the field in order to make their coordinates known in real time.

In detail, if someone unauthorized is accessing the remote site, the various steps are the following:

- An alarm is sent to the "physical security" team through the security interface that is not connected directly to RESISTO.
- RESISTO identifies this unauthorized access, looking at the local server logs or based on the fact that the visit was not planned and alarms have been raised at the telecom company NOC, and sends this access event to the group "security company" that has EWFC App installed on a tablet in the security room. RESISTO issues a damage inspection order to "physical security" team.
- The "physical security" team shall perform a damage inspection procedure using security cameras and inspecting the premises affected by the "suspect" access. The "physical security" team sends a report after detecting the damages.
- The RESISTO system identifies the damage and suggests suitable mitigation actions to be imposed as early as possible, i.e. traffic redirection and or activation of auxiliary network resources.

In case of emergency, RESISTO can send a "friendly" UAV, as an additional member of the security team, for damage inspection.

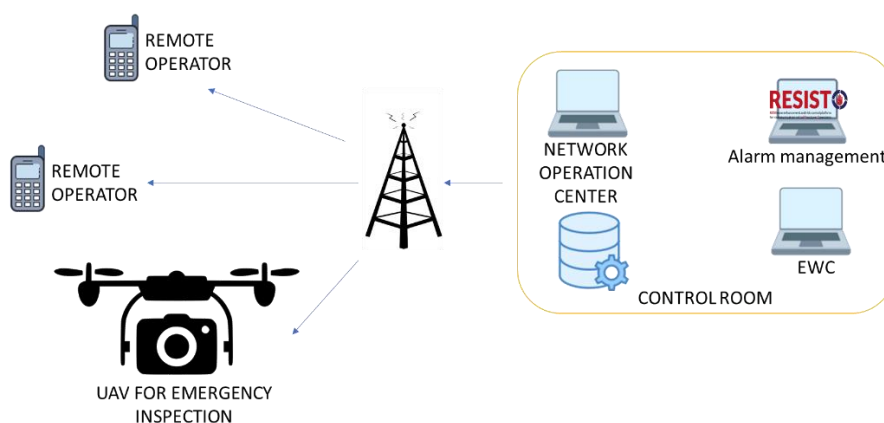


Figure 26 Emergency Warning Communications (EWC)

5.5. CISI Apro implementation of all unified reference scenarios

This chapter shows the entity types that have been defined to model the different telecommunications network components of each unified scenario.

Each entity is characterized by specific state variables and input/output resources, which are explained in detail in the following paragraphs.

5.5.1. Entity Types used in the unified scenarios

Here we report the description of all entity types used in the RESISTO project.

Table 13 Entity Type		
Entity Type	Description	
Optical_Wire	this is an optical wire	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Connection Dos_attack MITM_attack Port_Scan_Attack Virus_Attack TLC_services Cyber_Fault Mechanical_Fault	TLC_SERVICE TLC_CONN CYBER_FAULT MECH_FAULT	TLC_CONN TLC_SERVICE CYBER_FAULT MECH_FAULT
Step Received		
<pre> Connection=TLC_CONN; TLC_services=TLC_SERVICE; Cyber_Fault=CYBER_FAULT; Mechanical_Fault=max([Mechanical_Fault MECH_FAULT Mechanical_Fault_init]); Operative_Level=1-Mechanical_Fault; </pre>		
Step Sended		

TLC_CONN=Connection*Operative_Level; TLC_SERVICE=TLC_services*Operative_Level; CYBER_FAULT=Cyber_Fault*Operative_Level; MECH_FAULT=Mechanical_Fault;		
Entity Type		
Description		
Nexus93180Switch	Switch - Used for cabling in testbed	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Connection Dos_attack MITM_attack Port_Scan_Attack Virus_Attack TLC_services Cyber_Fault Mechanical_Fault BGP_hijacking Conn_Fault BotNet_Attack Config_Change Data_Corruption SW_Change SW_Deletion	TLC_CONN TLC_SERVICE CYBER_FAULT POWER ROOM_QoS	CYBER_FAULT TLC_CONN TLC_SERVICE SWITCHING_QoS
Step Received		
Connection=max(Connection_init,TLC_CONN); TLC_services=max(TLC_services_init,TLC_SERVICE); Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack MITM_attack Virus_Attack Port_Scan_Attack BGP_hijacking BotNet_Attack Data_Corruption SW_Change Config_Change SW_Deletion])); % Vale 1 in presenza di fault Conn_Fault=max([Dos_attack Mechanical_Fault 1-POWER 1-ROOM_QoS]); Operative_Level=(1-Conn_Fault)*max(max(TLC_CONN),0.5);		

<p>% Web Application Firewall and Enhanced application layer enrichment and protection</p>		
Step Sended		
<pre>TLC_CONN=Connection*(1-Conn_Fault); TLC_SERVICE=TLC_services*(1-Conn_Fault); CYBER_FAULT=Cyber_Fault*(1-Conn_Fault); SWITCHING_QoS=Operative_Level;</pre>		
Entity Type	Description	
CISCO_router	<p>Cisco ASR900 Series Aggregation Service Router</p> <p>903 Distribution Router</p> <p>920 Access Router (Aggregation Services Routers)</p> <p>7606 Core Router/Provider Edge</p> <p>7609 Router 720 Gbps of switching capacity in a 40 Gigabit/slot</p> <p>9006 Border Router/Core Router</p> <p>CRS-X (400Gb) Carrier Routing System modular and distributed core router</p> <p>ICS 7750 service router for voice/data applications and services</p> <p>7600 Series is an edge router with aggregation capabilities</p> <p>7604 Router for deployment at the network edge</p> <p>NCS 5002 MPLS aggregation router</p>	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES

Operative_Level Connection Dos_attack MITM_attack Virus_Attack TLC_services Cyber_Fault Mechanical_Fault BGP_hijacking OutboundQoS Conn_Fault TLC_service_names Congestion_Fault SW_Change SW_Deletion Port_Scan_Attack BotNet_Attack Data_Corruption Config_Change	TLC_CONN TLC_SERVICE CYBER_FAULT POWER ROOM_QoS	TLC_CONN TLC_SERVICE CYBER_FAULT ROUTING_QoS
Step Received		
<pre> Connection=max(Connection_init,TLC_CONN); TLC_services=max(TLC_services_init,TLC_SERVICE); Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack MITM_attack Virus_Attack Port_Scan_Attack BGP_hijacking BotNet_Attack Data_Corruption SW_Change Config_Change SW_Deletion])); % Vale 1 in presenza di fault Conn_Fault=max([Dos_attack Mechanical_Fault 1-POWER 1-ROOM_QoS]); Operative_Level=(1-Conn_Fault)*max(max(TLC_CONN),0.5); % Web Application Firewall and Enhanced application layer enrichment and protection </pre>		
Step Sented		

<pre>TLC_CONN=Connection*(1-Conn_Fault); TLC_SERVICE=TLC_services*(1-Conn_Fault); CYBER_FAULT=Cyber_Fault*(1-Conn_Fault); ROUTING_QoS=Operative_Level;</pre>		
Entity Type	Description	
OLT	NGPOP_CONN è alta se è vera la connessione con il POP1 (il servizio 1)	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level TLC_services Connection Cyber_Fault Mechanical_Fault Virus_Attack Port_Scan_Attack MITM_attack Dos_attack BGP_hijacking Conn_Fault Consumed_Services Service_Fault Redundancy_Fault MyConn BotNet_Attack Data_Corruption Config_Change SW_Change SW_Deletion My_Service	TLC_CONN TLC_SERVICE CYBER_FAULT POWER ROOM_QoS NGPON_IN	TLC_CONN TLC_SERVICE CYBER_FAULT NGPON_CONN

Step Received		
<pre> Connection=max(Connection_init,TLC_CONN); TLC_services=max(TLC_services_init,TLC_SERVICE); Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack MITM_attack Virus_Attack Port_Scan_Attack BGP_hijacking BotNet_Attack Data_Corruption SW_Change Config_Change SW_Deletion])); % Vale 1 in presenza di fault Conn_Fault=max([Dos_attack Mechanical_Fault 1-POWER 1-ROOM_QoS]); Service_Fault=max(abs(Consumed_Services.*TLC_SERVICE-Consumed_Services)); Redundancy_Fault=max(abs(Consumed_Services.*TLC_CONN-Consumed_Services)); Operative_Level=(1-Conn_Fault)*max(max(TLC_CONN),0.5)*((2*(1- Service_Fault)+(1-Redundancy_Fault))/3); % Il servizio utilizzato My_Service=max([(1-Service_Fault) (1-Redundancy_Fault)/2]); Operative_Level=(1-Conn_Fault)*My_Service; </pre>		
Step Sended		
<pre> TLC_CONN=Connection*(1-Conn_Fault); TLC_SERVICE=TLC_services*(1-Conn_Fault); CYBER_FAULT=Cyber_Fault*(1-Conn_Fault); NGPON_CONN=TLC_CONN; </pre>		
Entity Type		
Description		
Alcatel7750	Alcatel-Lucent 7750 Service Router Core Router/Provider Edge	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES

Operative_Level TLC_services TLC_service_names Dos_attack MITM_attack Port_Scan_Attack Virus_Attack Connection Cyber_Fault BGP_hijacking Mechanical_Fault Conn_Fault BotNet_Attack Config_Change Data_Corruption SW_Change SW_Deletion	TLC_CONN TLC_SERVICE CYBER_FAULT POWER ROOM_QoS	TLC_CONN TLC_SERVICE CYBER_FAULT ROUTING_QoS
Step Received		
<pre> Connection=max(Connection_init,TLC_CONN); TLC_services=max(TLC_services_init,TLC_SERVICE); Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack MITM_attack Virus_Attack Port_Scan_Attack BGP_hijacking BotNet_Attack Data_Corruption SW_Change Config_Change SW_Deletion])); % Vale 1 in presenza di fault Conn_Fault=max([Dos_attack Mechanical_Fault 1-POWER 1-ROOM_QoS]); Operative_Level=(1-Conn_Fault)*max(max(TLC_CONN),0.5); % Web Application Firewall and Enhanced application layer enrichment and protection </pre>		
Step Sended		
<pre> TLC_CONN=Connection*(1-Conn_Fault); TLC_SERVICE=TLC_services*(1-Conn_Fault); CYBER_FAULT=Cyber_Fault*(1-Conn_Fault); </pre>		

Entity Type	Description	
FortiGate1500D	Fortinet FortiGate 1500D Firewalls / UTM Firewall, IPS/IDS, Malware Detection&Protection	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Connection Dos_attack MITM_attack Port_Scan_Attack Virus_Attack TLC_services Mechanical_Fault BGP_hijacking Cyber_Fault Conn_Fault Consumed_Services Redundancy_Fault Service_Fault BotNet_Attack Data_Corruption SW_Change SW_Deletion Config_Change	TLC_CONN TLC_SERVICE CYBER_FAULT POWER ROOM_QoS	TLC_CONN TLC_SERVICE CYBER_FAULT FIREWALL_QoS REDUNDANCY_QoS
Step Received		

```

Connection=max(Connection_init,TLC_CONN);

TLC_services=max(TLC_services_init,TLC_SERVICE);

Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack   MITM_attack
Virus_Attack Port_Scan_Attack   BGP_hijacking BotNet_Attack Data_Corruption
SW_Change Config_Change SW_Deletion]));

% Vale 1 in presenza di fault
Conn_Fault=max([Dos_attack   Mechanical_Fault   1-POWER 1-ROOM_QoS] );

Service_Fault=max(abs(Consumed_Services.*TLC_SERVICE-Consumed_Services));
Redundancy_Fault=max(abs(Consumed_Services.*TLC_CONN-Consumed_Services));

Operative_Level=(1-Conn_Fault)*max(max(TLC_CONN),0.5)*((2*(1-
Service_Fault)+(1-Redundancy_Fault))/3);

```

Step Sended

```

TLC_CONN=Connection*(1-Conn_Fault);
TLC_SERVICE=TLC_services*(1-Conn_Fault);
CYBER_FAULT=Cyber_Fault*(1-Conn_Fault);

FIREWALL_QoS=(1-Service_Fault)*(1-Conn_Fault);

REDUNDANCY_QoS=(1-Redundancy_Fault);

```

Entity Type	Description	
F5BIGP	F5 BigIp Load Balancers, Web App Firewalls	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES

Operative_Level TLC_services TLC_service_names Connection Dos_attack MITM_attack Port_Scan_Attack Virus_Attack Mechanical_Fault BGP_hijacking Cyber_Fault Conn_Fault BotNet_Attack Data_Corruption SW_Change SW_Deletion Config_Change	TLC_CONN TLC_SERVICE CYBER_FAULT POWER ROOM_QoS	TLC_CONN TLC_SERVICE CYBER_FAULT
Step Received		
<pre> Connection=max(Connection_init,TLC_CONN); TLC_services=max(TLC_services_init,TLC_SERVICE); Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack MITM_attack Virus_Attack Port_Scan_Attack BGP_hijacking BotNet_Attack Data_Corruption SW_Change Config_Change SW_Deletion])); % Vale 1 in presenza di fault Conn_Fault=max([Dos_attack Mechanical_Fault 1-POWER 1-ROOM_QoS]); Operative_Level=(1-Conn_Fault)*max(max(TLC_CONN),0.5); % Web Application Firewall and Enhanced application layer enrichment and protection </pre>		
Step Sended		
<pre> TLC_CONN=Connection*(1-Conn_Fault); TLC_SERVICE=TLC_services*(1-Conn_Fault); CYBER_FAULT=Cyber_Fault*(1-Conn_Fault); </pre>		

Entity Type	Description	
PowerSource		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Power_Fault		POWER
Step Received		
Operative_Level=1-Power_Fault;		
Step Sended		
POWER=Operative_Level;		
Entity Type	Description	
Room		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Unauthorized_Access Power_Fault Flooding_Fault Fire_Fault Cooling_Fault Operative_Level Earthquake_Fault	POWER	ROOM_QoS
Step Received		
Operative_Level=min([1-Power_Fault 1-Flooding_Fault 1-Fire_Fault 1-Cooling_Fault POWER]); Operative_Level=Operative_Level*max((1-Unauthorized_Access),0.5);		
Step Sended		
ROOM_QoS=Operative_Level;		

Entity Type	Description	
Building		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Perimeter_Security_Fault Security_Camera_Fault Unauthorized_Access Conn_Fault Earthquake_Fault	ROOM_QoS	BUILDING_QoS
Step Received		
Operative_Level=ROOM_QoS/2;		
Step Sended		
BUILDING_QoS=Operative_Level;		
Entity Type	Description	
Splitter		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES

Operative_Level Connection Dos_attack MITM_attack Port_Scan_Attack Virus_Attack BGP_hijacking Mechanical_Fault MyConn Conn_Fault TLC_services Cyber_Fault BotNet_Attack Data_Corruption Config_Change SW_Change SW_Deletion	NGPON_CONN TLC_SERVICE CYBER_FAULT	NGPON_CONN NGPON_IN TLC_SERVICE CYBER_FAULT
Step Received		
<pre> %MyConn=NGPON_CONN; % Operative_Level=MyConn; Connection=NGPON_CONN; TLC_services=max(TLC_services_init,TLC_SERVICE); Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack MITM_attack Virus_Attack Port_Scan_Attack BGP_hijacking BotNet_Attack Data_Corruption SW_Change Config_Change SW_Deletion])); % Vale 1 in presenza di fault Conn_Fault=max([Dos_attack Mechanical_Fault]); Operative_Level=(1-Conn_Fault)*max(max(NGPON_CONN),0.5); </pre>		
Step Sendet		

<pre> NGPON_IN=Connection; NGPON_CONN=Connection*(1-Conn_Fault); TLC_SERVICE=TLC_services*(1-Conn_Fault); CYBER_FAULT=Cyber_Fault*(1-Conn_Fault); ROUTING_QoS=Operative_Level; </pre>		
Entity Type		
Description		
ONU		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level MyConn MITM_attack Dos_attack Port_Scan_Attack Virus_Attack BGP_hijacking Mechanical_Fault Consumed_Services Redundancy_Fault Service_Fault My_Service Conn_Fault TLC_services Cyber_Fault BotNet_Attack Data_Corruption Config_Change SW_Change SW_Deletion Connection	NGPON_CONN TLC_SERVICE CYBER_FAULT POWER	TLC_SERVICE NGPON_CONN CYBER_FAULT
Step Received		

```
%MyConn=NGPON_CONN;
%Operative_Level=MyConn;

Connection=NGPON_CONN;

Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack MITM_attack
Virus_Attack Port_Scan_Attack BGP_hijacking BotNet_Attack Data_Corruption
SW_Change Config_Change SW_Deletion]));

% Vale 1 in presenza di fault
Conn_Fault=max([Dos_attack Mechanical_Fault 1-POWER] );

Service_Fault=max(abs(Consumed_Services.*TLC_SERVICE-Consumed_Services));
Redundancy_Fault=max(abs(Consumed_Services.*NGPON_CONN-Consumed_Services));

Operative_Level=(1-Conn_Fault)*max(max(NGPON_CONN),0.5)*((2*(1-
Service_Fault)+(1-Redundancy_Fault))/3);

% Il servizio utilizzato
My_Service=max([(1-Service_Fault) (1-Redundancy_Fault)/2]);

Operative_Level=(1-Conn_Fault);
```

Step Sended		
NGPON_CONN=Connection;		
Entity Type	Description	
RU-DU_ANTENNA		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES

Operative_Level Dos_attack MITM_attack Port_Scan_Attack Virus_Attack BGP_hijacking Mechanical_Fault Consumed_Services My_Service MyConn Conn_Fault TLC_services Cyber_Fault Connection SW_Deletion SW_Change BotNet_Attack Data_Corruption Config_Change	NGPON_CONN CYBER_FAULT TLC_SERVICE POWER	CYBER_FAULT TLC_SERVICE R_CONN RF_QoS
Step Received		

<pre> MyConn=NGPON_CONN; %Operative_Level=MyConn; Connection=NGPON_CONN; Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack MITM_attack Virus_Attack Port_Scan_Attack BGP_hijacking BotNet_Attack Data_Corruption SW_Change Config_Change SW_Deletion])); % Vale 1 in presenza di fault Conn_Fault=max([Dos_attack Mechanical_Fault 1-POWER]); TLC_services=TLC_SERVICE; Service_Fault=max(abs(Consumed_Services.*TLC_SERVICE-Consumed_Services)); Redundancy_Fault=max(abs(Consumed_Services.*NGPON_CONN-Consumed_Services)); Operative_Level=(1-Conn_Fault)*max(max(NGPON_CONN),0.5)*((2*(1- Service_Fault)+(1-Redundancy_Fault))/3); % Il servizio utilizzato My_Service=max([(1-Service_Fault) (1-Redundancy_Fault)/2]); </pre>		
Step Sended		
<pre> R_CONN=Connection*(1-Conn_Fault); TLC_SERVICE=TLC_services*(1-Conn_Fault); CYBER_FAULT=Cyber_Fault*(1-Conn_Fault); RF_QoS=My_Service; </pre>		
Entity Type	Description	
Cell_Area		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Security_Camera_Fault Perimeter_Security_Fault Unauthorized_Access	TLC_SERVICE CYBER_FAULT R_CONN	TLC_SERVICE CYBER_FAULT CELL_QoS R_CONN
Step Received		

Step Sented		
Entity Type	Description	
Aggregation_Services_Router	Cisco ASR 9000 Series Aggregation Services Routers Designed for Metro Ethernet networks Designed for video and other high bandwidth applications	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Connection Dos_attack MITM_attack Port_Scan_Attack Virus_Attack TLC_services Cyber_Fault Mechanical_Fault	TLC_SERVICE TLC_CONN CYBER_FAULT MECH_FAULT	TLC_CONN TLC_SERVICE CYBER_FAULT MECH_FAULT
Step Received		
Step Sented		
Entity Type	Description	
Layer3Switch		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	TLC_CONN TLC_SERVICE CYBER_FAULT	TLC_CONN TLC_SERVICE CYBER_FAULT
Step Received		
Step Sented		

Entity Type	Description	
Streamer		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	STREAM	TLC_CONN TLC_SERVICE CYBER_FAULT
Step Received		
Step Sent		
Entity Type	Description	
Entry_2i_CPE	Modem	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	ADSL_CONN TLC_SERVICE	ADSL_CONN TLC_SERVICE
Step Received		
Step Sent		
Entity Type	Description	
Television		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	ADSL_CONN TLC_SERVICE	TV_QoS
Step Received		

Step Sented		
Entity Type	Description	
DSLAM	ADSL_CONN è alta se è vera la connessione con il POP1 (il servizio 1) https://italian.alibaba.com/product-detail/huawei-smartax-ma5603-adsl2-ip-dslam-60084758532.html	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	TLC_CONN TLC_SERVICE CYBER_FAULT POWER	CYBER_FAULT ADSL_CONN TLC_SERVICE TLC_CONN
Step Received		
Step Sented		
Entity Type	Description	
Redundant_Wire	this is an optical wire	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Cyber_Fault TLC_services Connection Mechanical_Fault	TLC_CONN TLC_SERVICE CYBER_FAULT MECH_FAULT	TLC_CONN TLC_SERVICE CYBER_FAULT MECH_FAULT
Step Received		

<pre> Connection=TLC_CONN; TLC_services=TLC_SERVICE; Cyber_Fault=CYBER_FAULT; Mechanical_Fault=max([Mechanical_Fault MECH_FAULT Mechanical_Fault_init]); Operative_Level=1-Mechanical_Fault; </pre>		
Step Sended		
<pre> TLC_CONN=Connection*Operative_Level; TLC_SERVICE=TLC_services*Operative_Level; CYBER_FAULT=Cyber_Fault*Operative_Level; MECH_FAULT=Mechanical_Fault; </pre>		
Entity Type		
Description		
HuaweiSwitch	Huawei Quidway S8500 Serie 10G Core Routing Switch Quidway® S85021, Quidway® S8505, Quidway® S8508 , Quidway® S8512 Huawei Quidway® S3300 switches Layer-3 100-megabit Ethernet switches s3328, Huawei 9306 Switch	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Connection BGP_hijacking BotNet_Attack Cyber_Fault Dos_attack Mechanical_Fault MITM_attack Conn_Fault BotNet_Attack Config_Change Data_Corruption	TLC_CONN TLC_SERVICE CYBER_FAULT POWER ROOM_QoS	TLC_CONN TLC_SERVICE CYBER_FAULT ROUTING_QoS

SW_Change SW_Deletion		
Step Received		
<pre> Connection=max(Connection_init,TLC_CONN); TLC_services=max(TLC_services_init,TLC_SERVICE); Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack MITM_attack Virus_Attack Port_Scan_Attack BGP_hijacking BotNet_Attack Data_Corruption SW_Change Config_Change SW_Deletion])); % Vale 1 in presenza di fault Conn_Fault=max([Dos_attack Mechanical_Fault 1-POWER 1-ROOM_QoS]); Operative_Level=(1-Conn_Fault)*max(max(TLC_CONN),0.5); % Web Application Firewall and Enhanced application layer enrichment and protection </pre>		
Step Sended		
<pre> TLC_CONN=Connection*(1-Conn_Fault); TLC_SERVICE=TLC_services*(1-Conn_Fault); CYBER_FAULT=Cyber_Fault*(1-Conn_Fault); ROUTING_QoS=Operative_Level; </pre>		
Entity Type	Description	
CISCOswitch	Cisco SG300-28 28-Port Gigabit Managed Switch Catalyst 3750	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES

Operative_Level	TLC_CONN TLC_SERVICE CYBER_FAULT	TLC_CONN TLC_SERVICE CYBER_FAULT
Step Received		
Step Sended		
Entity Type	Description	
Layer2Switch		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level BGP_hijacking BotNet_Attack Config_Change Dos_attack MITM_attack Port_Scan_Attack SW_Change SW_Deletion Virus_Attack Data_Corruption	POWER TLC_CONN TLC_SERVICE CYBER_FAULT ROOM_QoS	TLC_CONN TLC_SERVICE CYBER_FAULT
Step Received		

<pre> Connection=max(Connection_init,TLC_CONN); TLC_services=max(TLC_services_init,TLC_SERVICE); Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack MITM_attack Virus_Attack Port_Scan_Attack BGP_hijacking BotNet_Attack Data_Corruption SW_Change Config_Change SW_Deletion])); % Vale 1 in presenza di fault Conn_Fault=max([Dos_attack Mechanical_Fault 1-POWER 1-ROOM_QoS]); Operative_Level=(1-Conn_Fault)*max(max(TLC_CONN),0.5); % Web Application Firewall and Enhanced application layer enrichment and protection </pre>		
Step Sended		
<pre> TLC_CONN=Connection*(1-Conn_Fault); TLC_SERVICE=TLC_services*(1-Conn_Fault); CYBER_FAULT=Cyber_Fault*(1-Conn_Fault); ROUTING_QoS=Operative_Level; </pre>		
Entity Type	Description	
Medical_Room		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Fire_Fault Power_Fault Water_Fault Air_Fault	POWER AIR WATER CYBER_FAULT TLC_CONN TLC_SERVICE MOBILE_QoS OXYGEN	MEDICAL_ROOM_QoS
Step Received		

<pre> Connection=TLC_CONN; TLC_services=TLC_SERVICE; Cyber_Fault=CYBER_FAULT; Mechanical_Fault=max([Mechanical_Fault MECH_FAULT Mechanical_Fault_init]); Operative_Level=1-Mechanical_Fault; </pre>		
Step Sended		
<pre> TLC_CONN=Connection*Operative_Level; TLC_SERVICE=TLC_services*Operative_Level; CYBER_FAULT=Cyber_Fault*Operative_Level; MECH_FAULT=Mechanical_Fault; </pre>		
Entity Type	Description	
Ordinary_Room		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Power_Fault Operative_Level Fire_Fault Air_Fault	AIR POWER	ORDINARY_ROOM_QoS
Step Received		
<pre> Power_Fault=1-POWER; Air_Fault=1-AIR; Operative_Level=min([1-Power_Fault 1-Fire_Fault 1-Air_Fault]); </pre>		
Step Sended		
ORDINARY_ROOM_QoS=Operative_Level;		
Entity Type	Description	

Generator		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Mechanical_Fault		POWER ACTIVATOR GENERATOR_QoS
Step Received		
Operative_Level=1- Mechanical_Fault;		
Step Sended		
<pre> if (Mechanical_Fault==0) POWER=1; ACTIVATOR=0; else POWER=0; ACTIVATOR=1; end GENERATOR_QoS= Operative_Level; </pre>		
Entity Type	Description	
Emergency_Power		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Mechanical_Fault Operative_Level	ACTIVATOR	POWER EMERGENCY_POWER_ QoS
Step Received		

Operative_Level=1-Mechanical_Fault;		
Step Sended		
<pre> if (ACTIVATOR==1 && Mechanical_Fault==0) POWER=1; else POWER=0; end EMERGENCY_POWER_QoS=Operative_Level; </pre>		
Entity Type	Description	
Wire_Medical_Room		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Mechanical_Fault Power_Fault	POWER	WIRE_QoS POWER
Step Received		
<pre> Power_Fault=1-POWER; Operative_Level = min([1-Mechanical_Fault 1-Power_Fault]); </pre>		
Step Sended		
<pre> if (Operative_Level==1) POWER=1; else POWER=0; end WIRE_QoS=Operative_Level; </pre>		

Entity Type	Description	
Tap		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Mechanical_Fault		WATER
Step Received		
Operative_Level=1- Mechanical_Fault;		
Step Sended		
WATER=1-Mechanical_Fault; %if(Mechanical_Fault==1) % WATER=0; %else % WATER=1; %end		
Entity Type	Description	
Pipe		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Water_Fault Operative_Level Mechanical_Fault	WATER	WATER PIPE_QoS
Step Received		

Water_Fault= 1- WATER; Operative_Level=min([1-Mechanical_Fault 1-Water_Fault]);		
Step Sended		
if(Operative_Level==1) WATER=1; else WATER=0; end PIPE_QoS=Operative_Level;		
Entity Type	Description	
Autoclave		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Water_Fault Operative_Level Power_Fault Mechanical_Fault	WATER POWER	WATER
Step Received		
Water_Fault=1-WATER; Power_Fault=1-POWER; Operative_Level=min([1-Mechanical_Fault 1-Power_Fault 1-Water_Fault]);		
Step Sended		
if(Operative_Level==1) WATER=1; else WATER=0; end		

Entity Type	Description	
Fan		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Mechanical_Fault Operative_Level Power_Fault	POWER	AIR
Step Received		
Power_Fault=1-POWER; Operative_Level=min([1-Mechanical_Fault 1-Power_Fault]);		
Step Sended		
if(Operative_Level==1) AIR=1; else AIR=0; end		
Entity Type	Description	
Air_Conditioning_Element		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Power_Fault Air_Fault Mechanical_Fault Operative_Level	AIR POWER	AIR
Step Received		
Power_Fault=1-POWER; Air_Fault=1-AIR; Operative_Level=min([1-Mechanical_Fault 1-Power_Fault 1-Air_Fault]);		
Step Sended		

<pre> if(Operative_Level==1) AIR=1; else AIR=0; end </pre>		
Entity Type	Description	
Duct		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Air_Fault Mechanical_Fault Operative_Level	AIR	AIR DUCT_QoS
Step Received		
<pre> Air_Fault=1-AIR; Operative_Level=min([1-Mechanical_Fault 1-Air_Fault]); </pre>		
Step Sended		
<pre> if(Operative_Level==1) AIR=1; else AIR=0; end DUCT_QoS=Operative_Level; </pre>		
Entity Type	Description	
House		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES

Operative_Level Flooding_Fault Perimeter_Security_Fault Security_Camera_Fault Temperature_Fault Unauthorized_Access Water_Fault	TLC_SERVICE CYBER_FAULT NGPON_CONN	HOME_QoS
Step Received		
Step Sended		
Entity Type	Description	
5G_Core	MME (Mobility Management Entity) SGW (Service Gateway) PGW (Packet Gateway) HSS (Home Subscriber Server)	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level TLC_services BGP_hijacking BotNet_Attack Config_Change Cyber_Fault Data_Corruption Dos_attack Mechanical_Fault MITM_attack SW_Change SW_Deletion syslog_adm_login Virus_Attack Connection Conn_Fault Port_Scan_Attack	CYBER_FAULT POWER ROOM_QoS TLC_CONN TLC_SERVICE	TLC_CONN TLC_SERVICE CYBER_FAULT
Step Received		

<pre> Connection=max(Connection_init,TLC_CONN); TLC_services=max(TLC_services_init,TLC_SERVICE); Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack MITM_attack Virus_Attack Port_Scan_Attack BGP_hijacking BotNet_Attack Data_Corruption SW_Change Config_Change SW_Deletion])); % Vale 1 in presenza di fault Conn_Fault=max([Dos_attack Mechanical_Fault 1-POWER 1-ROOM_QoS]); Operative_Level=(1-Conn_Fault)*max(max(TLC_CONN),0.5); </pre>		
Step Sended		
<pre> TLC_CONN=Connection*(1-Conn_Fault); TLC_SERVICE=TLC_services*(1-Conn_Fault); CYBER_FAULT=Cyber_Fault*(1-Conn_Fault); </pre>		
Entity Type	Description	
MobileUnit		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Dos_attack MITM_attack Port_Scan_Attack SW_Change SW_Deletion Virus_Attack BGP_hijacking BotNet_Attack Config_Change Data_Corruption Connection Mechanical_Fault Service_Fault Redundancy_Fault My_Service Consumed_Services	TLC_SERVICE CYBER_FAULT R_CONN	MOBILE_QoS
Step Received		

<pre> Connection=max(Connection_init,R_CONN); TLC_services=TLC_SERVICE; % OBIETTIVO DI CYBER-ATTACK Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack MITM_attack Virus_Attack Port_Scan_Attack BGP_hijacking BotNet_Attack Data_Corruption SW_Change Config_Change SW_Deletion])); % CONSUMATORE DI SERVIZI EVENTUALMENTE RIDONDATI Service_Fault=max(abs(Consumed_Services.*TLC_SERVICE-Consumed_Services)); Redundancy_Fault=max(abs(Consumed_Services.*R_CONN-Consumed_Services)); % Vale 1 in presenza di fault Conn_Fault=max([Dos_attack Mechanical_Fault]); Operative_Level=(1-Conn_Fault)*max(max(R_CONN),0.5)*((2*(1- Service_Fault)+(1-Redundancy_Fault))/3); % Il servizio utilizzato My_Service=max([(1-Service_Fault) (1-Redundancy_Fault)/2]); </pre>		
Step Sended		
MOBILE_QoS=My_Service;		
Entity Type	Description	
App_Server		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level BGP_hijacking BotNet_Attack Config_Change Conn_Fault Cooling_Fault Cyber_Fault Congestion_Fault Mechanical_Fault Port_Scan_Attack SW_Change SW_Deletion syslog_adm_login	TLC_CONN TLC_SERVICE CYBER_FAULT ROOM_QoS POWER	TLC_CONN TLC_SERVICE CYBER_FAULT
Step Received		

Step Sended		
Entity Type	Description	
RU_ANTENNA	RF+Antenna	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Power_Fault Congestion_Fault	TLC_SERVICE CYBER_FAULT POWER TLC_CONN	TLC_SERVICE CYBER_FAULT R_CONN
Step Received		
Step Sended		
Entity Type	Description	
5G_CU_DU	PPF (PDCP) + BPF + RCF	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level BGP_hijacking BotNet_Attack Config_Change Data_Corruption Dos_attack MITM_attack Port_Scan_Attack SW_Change SW_Deletion Virus_Attack TLC_services Conn_Fault	TLC_CONN TLC_SERVICE POWER CYBER_FAULT	TLC_CONN TLC_SERVICE CYBER_FAULT
Step Received		

<pre> Connection=max(Connection_init,TLC_CONN); TLC_services=max(TLC_services_init,TLC_SERVICE); Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack MITM_attack Virus_Attack Port_Scan_Attack BGP_hijacking BotNet_Attack Data_Corruption SW_Change Config_Change SW_Deletion])); % Vale 1 in presenza di fault Conn_Fault=max([Dos_attack Mechanical_Fault 1-POWER 1-ROOM_QoS]); Operative_Level=(1-Conn_Fault)*max(max(TLC_CONN),0.5); </pre>		
Step Sended		
<pre> TLC_CONN=Connection*(1-Conn_Fault); TLC_SERVICE=TLC_services*(1-Conn_Fault); CYBER_FAULT=Cyber_Fault*(1-Conn_Fault); </pre>		
Entity Type	Description	
Workstation		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	TLC_CONN CYBER_FAULT POWER	WORKSTATION_QoS
Step Received		
Step Sended		
Entity Type	Description	
Robot		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level Mechanical_Fault	POWER R_CONN	ROBOT_QoS
Step Received		
Step Sended		

Entity Type	Description	
Boat		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	VDES_CONN AIS_CONN	BOAT_QoS AIS_CONN
Step Received		
Step Sent		
Entity Type	Description	
VDES_ANTENNA		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	TLC_SERVICE CYBER_FAULT POWER VDES_CONN	VDES_CONN TLC_CONN TLC_SERVICE CYBER_FAULT
Step Received		
Step Sent		
Entity Type	Description	
Alcatel_Lucent_SDH	The Alcatel-Lucent 1660 Synchronous Multiplexer (SM) multiservice SDH metro and regional transport networks.	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES

Operative_Level	TLC_CONN TLC_SERVICE CYBER_FAULT POWER ROOM_QoS	TLC_CONN TLC_SERVICE CYBER_FAULT ROUTING_QoS
Step Received		
Step Sended		
Entity Type	Description	
Alcatel_Lucent_TSS	Alcatel-Lucent 1850 TRANSPORT SERVICE SWITCH Switches packets and circuits, and transports any kind of service in any possible mix	
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	TLC_CONN TLC_SERVICE CYBER_FAULT POWER ROBOT_QoS	TLC_CONN TLC_SERVICE CYBER_FAULT ROUTING_QoS
Step Received		
Step Sended		
Entity Type	Description	
JuniperBEA		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	TLC_CONN TLC_SERVICE CYBER_FAULT POWER ROOM_QoS	TLC_CONN TLC_SERVICE CYBER_FAULT ROUTING_QoS

Step Received		
Step Sended		
Entity Type	Description	
BRAS		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	TLC_CONN TLC_SERVICE CYBER_FAULT POWER ROOM_QoS	TLC_CONN TLC_SERVICE CYBER_FAULT ROUTING_QoS
Step Received		
Step Sended		
Entity Type	Description	
ISP		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	TLC_CONN TLC_SERVICE CYBER_FAULT	TLC_CONN TLC_SERVICE CYBER_FAULT
Step Received		
Step Sended		
Entity Type	Description	
Camera		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level		STREAM
Step Received		

Step Sended		
Entity Type	Description	
CloudServer		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	TLC_CONN TLC_SERVICE CYBER_FAULT BUILDING_QoS POWER	TLC_CONN TLC_SERVICE CYBER_FAULT
Step Received		
Step Sended		
Entity Type	Description	
BaseTransceiverStation		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	TLC_CONN TLC_SERVICE CYBER_FAULT	TLC_SERVICE CYBER_FAULT BTS_CONN
Step Received		
Step Sended		
Entity Type	Description	
BTS_ANTENNA		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES

Operative_Level Power_Fault Congestion_Fault	TLC_SERVICE CYBER_FAULT POWER BTS_CONN	TLC_SERVICE CYBER_FAULT R_CONN
Step Received		
<pre> Connection=max(Connection_init,TLC_CONN); TLC_services=max(TLC_services_init,TLC_SERVICE); Cyber_Fault=max(CYBER_FAULT, transpose([Dos_attack MITM_attack Port_Scan_Attack Virus_Attack BGP_hijacking])); % Vale 1 in presenza di fault Conn_Fault=max([Dos_attack Mechanical_Fault 1-POWER 1-ROOM_QoS]); Operative_Level=(1-Conn_Fault)*max(max(TLC_CONN),0.5); % Web Application Firewall and Enhanced application layer enrichment and protection </pre>		
Step Sended		
<pre> TLC_CONN=Connection*(1-Conn_Fault); TLC_SERVICE=TLC_services*(1-Conn_Fault); CYBER_FAULT=Cyber_Fault*(1-Conn_Fault); ROUTING_QoS=Operative_Level; </pre>		
Entity Type	Description	
OXYGEN_Element		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	POWER	OXYGEN
Step Received		
Step Sended		

Entity Type	Description	
OXYGEN_Duct		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Mechanical_Fault Operative_Level	OXYGEN	OXYGEN
Step Received		
Step Sendend		
Entity Type	Description	
Working_Cell		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	ROBOT_QoS	WORKING_CELL_QoS
Step Received		
Step Sendend		
Entity Type	Description	
VDES_RECEIVER		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	VDES_CONN	VDES_CONN
Step Received		
Step Sendend		
Entity Type	Description	
IoT_Gateway		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	TLC_CONN TLC_SERVICE CYBER_FAULT IoT_CONN	IoT_CONN TLC_CONN TLC_SERVICE CYBER_FAULT

Step Received		
Step Sended		
Entity Type	Description	
Radio_Bridge		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	TLC_CONN TLC_SERVICE CYBER_FAULT	CYBER_FAULT TLC_CONN TLC_SERVICE
Step Received		
Step Sended		
Entity Type	Description	
IoT_Sensor		
State Variables	INPUT RESOURCES	OUTPUT RESOURCES
Operative_Level	IoT_CONN	IoT_CONN
Step Received		
Step Sended		

5.5.2. Description of State Variables

According to use cases described in Deliverable 2.8 and definitions of Cyber-Physical threats in Deliverable 2.3, the following state variables in Table 14 are introduced to model risk scenarios in CISIApro.

Table 14 CISIApro State Variables	
State Variable	Description
Connection	Variable propagated in all directions to check for connection
TLC_Services	Vector used to identify which specific rout works
Operative_Level	Holistic variable collecting all information about health state of the entity
OutboundQoS	Holistic variable used to evaluate the quality of service of the antenna
Consumed_Services	Vector of entity required services
Sylog_adm_login	Cyber-attack related to an admin login made by unauthorized user
Unauthorized_Access	An unauthorized person gains entry into a protected area
Perimeter_Security_Fault	The perimeter protection system (video / audio analysis) is no longer in operation for the detection/classification of anomalous activities
Security_Camera_Fault	Attacker shuts down internet-connected security cameras
Congestion_Fault	Network congestion is the reduced quality of service that occurs when a network node or link is carrying more data than it can handle. Typical effects include queueing delay, packet loss or the blocking of new connections. A consequence of congestion is that an incremental increase in offered load leads either to a decrease in network throughput.
Conn_Fault	Loss of connectivity
Service_Fault	Service delivery failure
Redundancy_Fault	Fault to the redundancy equipment can fail to provide the expected level of resilience
Power_Fault	Telecoms infrastructure is dependent on a continuous supply of power. Power failure occurs when power is no longer supplied due to a malicious attack or severe weather
Air_Fault	Air duct failure
Earthquake_Fault	Fault due to an earthquake
Water_Fault	Fault related to the pump that does not distribute water

Cooling_Fault	HVAC related fault
Flooding_Fault	Flooding due to water system failure
Fire_Fault	A fire breaks out in the building
Bursting_Fault	Terrorist attack to destroy some elements of telecommunications network
Temperature_Fault	A sensor detects a temperature increase out of range
Mechanical_Fault	Fault of a physical component of telecommunications network
Rogue_Access	An unauthorized person accesses a computer system
Stream_source	Data flow transmitted by cameras
Cyber-attacks	
DoS_attack	Cyber-attacks in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack. This is known as a distributed-denial-of-service (DdoS) attack.
MITM_attack	Communication between two parties may be covertly intercepted, recorded, and even altered by an attacker. Information collected may then be used for identity or data theft.
Port_Scan_Attack	A port scan is an attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service. Scanning, as a method for discovering exploitable communication channels, has been around for ages. The idea is to probe as many listeners as possible and keep track of the ones that are receptive or useful to your particular need.
Virus_Attack	Virus is a type of malwares that can self-replicate but needs to insert or attach themselves into other mediums to make the infection happen. Viruses include file infectors, boot sector viruses and interpreted viruses.
BGP_hijacking	BGP hijacking is a malicious rerouting of internet traffic that exploits the trusting nature of BGP, the routing protocol of the Internet. Attackers reroute Internet traffic by falsely announcing ownership of groups of IP addresses, called IP prefixes, that they do not actually own, control, or route to.
BotNet_Attack	Cybercriminals use special Trojan viruses to breach the security of

	several users' computers, take control of each computer and organise all of the infected machines into a network of 'bots' that the criminal can remotely manage. Therefore, a botnet is a network of infected computers remotely controlled by cybercriminals.
Data_Corruption	Data tampering and modification after a successful illicit system intrusion
Config_Change	A cybercriminal starts a program from a privilege folder or temporary folder of system to change system configuration
SW_Change	A cybercriminal changes a software in a computer system
SW_Deletion	A cybercriminal deletes a software in a computer system
HW_Theft	<i>Hardware theft is act of stealing computer equipment</i>

5.5.3. Description of Input-Output Resources

Table 15 describes the input and output resources that are used in CISIApro to model the unified scenarios above.

Table 15 Input-Output Resources	
Resource	Description
TLC_CONN	Resource propagated in all directions of the network
TLC_SERVICE	Resource that has a selective route
POWER	Resource necessary for the functioning of telecommunications network components
RF_SLICE	Signal transmitted by the antenna
NGPON_CONN	Signal transmitted by the NGPON
NGPON_IN	Signal received by the NGPON
R_CONN	Radio signal
WATER	Resource distributed by pumps
AIR	Resource distributed by ducts
ACTIVATOR	Resource propagated to activate the emergency generator
ADSL_CONN	Resource for digital Internet access with twisted pair
VDES_CONN	Resource distributed by radio communication system that operates between ships, shore stations and satellites.
AIS_CONN	Resource distributed by Automatic Identification System

STREAM	Signal transmitted by cameras or streamers
BTS_CONN	Radio signal transmitted and received by a base transceiver station
OXYGEN	Resource present in Medical Rooms of Hospital
IoT_CONN	Resource that connects IoT sensors
Resources KPI	
ROOM_QoS	Resource propagated to evaluate the quality of service of the room
GLOBAL_QoS	QoS of the whole scenario
BUILDING_QoS	Resource propagated to evaluate the quality of service of the building
FIREWALL_QoS	Resource that evaluates firewall operations
SERVICE_QoS	Resource that evaluates the quality of the services provided
MPLS_NET_QoS	Resource propagated to evaluate the quality of Multiprotocol Label Switching
ROUTING_QoS	Resource that evaluates the correct routing of packages to the right destination
SWITCHING_QoS	Resource propagated to evaluate the quality of service of the routing
RF_QoS	Resource that evaluates the quality of the signal transmitted by the antenna
REDUNDANCY_QoS	Resource that evaluates the level of resilience
MEDICAL_ROOM_QoS	Resource that evaluates the quality of Medical Rooms in the Hospital
ORDINARY_ROOM_QoS	Resource that evaluates the quality of Ordinary Rooms in the Hospital
GENERATOR_QoS	Resource that evaluates the quality of power generator
EMERGENCY_POWER_QoS	Resource that evaluates the quality of emergency generator
WIRE_QoS	Resource propagated to evaluate the quality of service of the wire
PIPE_QoS	Resource propagated to evaluate the quality of service of the pipe
DUCT_QoS	Resource propagated to evaluate the quality of service of the duct
MOBILE_QoS	Resource propagated to evaluate the quality of the mobile connection
TV_QoS	Resource that assesses the quality of data flow that reaches TVs
ROBOT_QoS	Resource propagated to evaluate the functioning of robots in Smart Factory
WORKSTATION_QoS	Resource that estimates the quality of service provided by a workstation

BOAT_QoS	Resource that estimates the quality of service of boats in the Maritime Site
CELL_QoS	Resource that estimates the quality of service of cell area
Resources Alert	
SW_CHANGE	Resource propagated when a cybercriminal changes a software in a computer system
CONFIG_CHANGE	Resource propagated when a cybercriminal starts a program from a privilege folder or temporary folder of system to change system configuration
SW_DELETION	Resource propagated when a cybercriminal deletes a software in a computer system
Fault	
CYBER_FAULT	Resource propagated when a cyber fault is detected in the network
MECH_FAULT	Resource propagated when there is a fault of a physical component of telecommunications network
CONGEST_FAULT	Resource propagated when there is a network congestion
CONN_FAULT	Resources propagated when there is a loss of connectivity

6. USE CASE 1-2: CORE NETWORK FAILURE CAUSED BY PHYSICAL & CYBER-ATTACKS OR NATURAL DISASTERS TO TELECOMMUNICATION SITES (OTE TESTBED)

6.1. Unified Reference Scenario 1

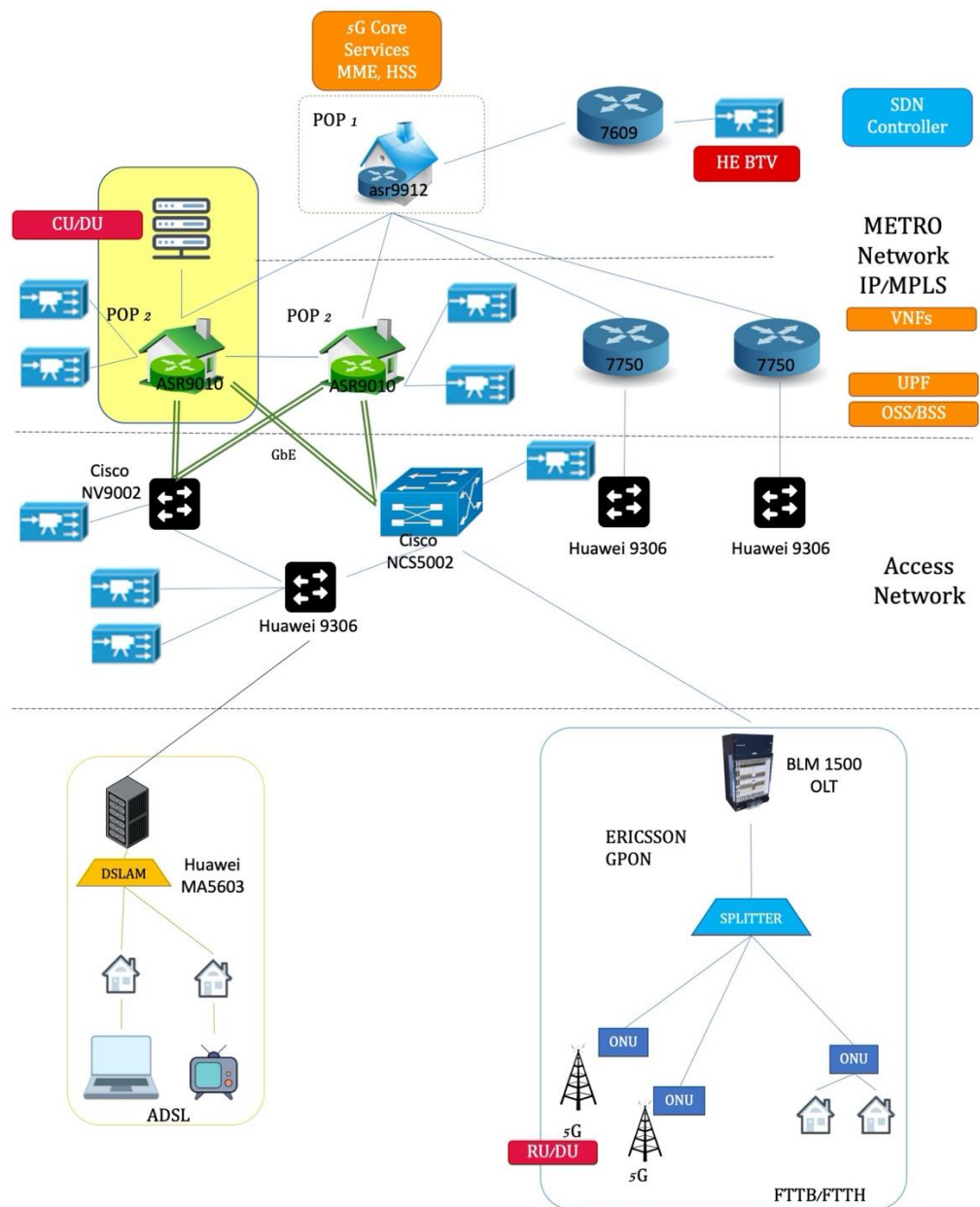


Figure 27 Unified Scenario 1: Use Case 1-2 – OTE Testbed

The Unified Scenario 1, shown in Figure 27, is defined with the aim of simulating use cases 1 and 2. The telecommunication network architecture takes inspiration from Figure 28, it represents the RESISTO slice Core Lab.

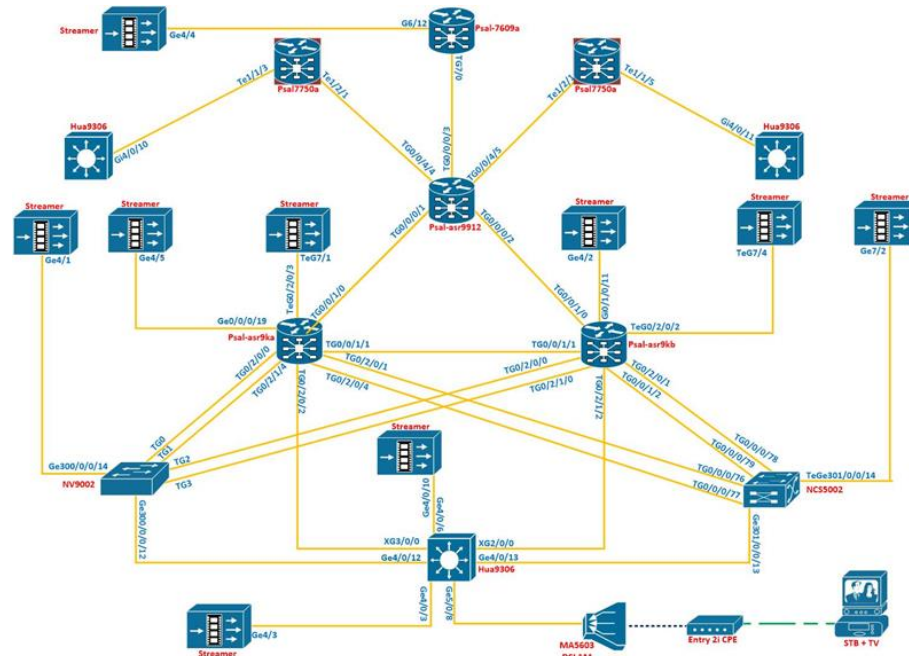


Figure 28 RESISTO slice Core Lab Description

The different components that characterized the TLC network are described in detail in the following table.

Table 16 TLC Network Elements for Reference Scenario 1					
TLC Network Elements	Network	Services	Testbed Components		
			Component	Name	Description
CORE network	MPLS		7609		
METRO nodes/ POP level 1			ASR9912		
METRO network	MPLS				

POP level 2			ASR9010		
Access Network			NV9002, NCS5002, Huawei 9396		
Access Nodes			DSLAM, SPLITTER		
Premises nodes		RU	ONU, ANTENNA		
End Users			TV, PC, Mobile		

6.2. Sub Scenarios for Use Case 1 and Impacts on the Unified Scenario

Telecom networks as critical infrastructures are meant to provide multiple types of services with predefined and guaranteed Quality of Service. Mobile network operators focus on protecting their existing networks and telecom infrastructures from attacks originating from outside. In the most devious attacks, rather than trying to gain full access into the system, an attacker may only want to open up a few strategic holes to the cyber domain of a network that will cause severe problems or failures to the offered services either immediately or at a later time. Thus, the attackers can exploit vulnerabilities in the physical domain of an infrastructure, to gain access to the cyber domain. These physical intrusions (such as unauthorized access to a building without obvious, direct or severe damage on the telecom infrastructure) may be initially seen as assaults of a lesser importance in respect to their consequences on the cyber domain.

In this use case, the physical attack on the premises of OTE will take place on two fronts:

- the attackers use a UAV to overcome the physical protection and execute the cyber-attack
- an unauthorized person enters the building, gains access to an unattended computer and installs malware

The main objective of the Use Case 1 (both subcases scenarios) is to enhance the resilience of the existing communication infrastructures towards both the domains of physical security and cyber protection.

Table 17 Sub Scenarios for Use Case 1		
Sub Use Case	Scenario	Description
1.1		The UAV flies over the fence and approaches the building ignoring the physical security of the location, i.e., secure fence and building, and connects wirelessly to the wireless network from the exterior of the building, gaining access to a network switch and initiating a DDoS attack which targets the switch.
1.2		An unauthorized person breaches the secure perimeter and tries to gain access to the interior of the building. As soon as the unauthorized person enters the building, he gains access to an unattended computer and installs dormant malware that will be activated at some point in the future.

According to Use Case 1 described in deliverable D2.8, impacts that can be derived for the Unified Scenario 1 are reported in the following Table 18.

Table 18 Impacts on the Unified Scenario 1 for Use Case 1	
Type	Description
Operational	Risk of connectivity loss, denial of service and service delivery failure which would also potentially affect PPDR / emergency services as well, if the imposed cyber-attacks are not detected. The direct physical attacks affect the existing security systems (access or entrance breaches) which would need immediate attention and change of protocols.
Technical	Network connectivity failure / data corruption / telephony (fixed, mobile) & internet services (wired / wireless) at risk depending on the severity of the imposed cyber-attacks consequences. In case of core network failure (severe damage), services could be restored through traffic rerouting or secondary resilience centers until the problems are solved. However, this may also affect the networks in the surrounding areas near OTE's premises, especially when other critical infrastructures are in the vicinity.
Economic	Apart from the damage in building security, large economic impact would be created due to the loss (partially or wholly) of network functionalities for the telecom provider since SLAs are at risk due to service delivery failure.

Societal	If the imposed cyber-attacks remain undetected, this would cause severe problems in the wider telecom network and the customers' telecom services (telephony, fixed or mobile & internet services wired or wireless or WLANs / private networks).
----------	---

6.3. Sub Scenarios for Use Case 2 and Impacts on the Unified Scenario

Mobile communications are rapidly evolving into complex systems both in terms of the network architecture and the types of connected devices. This increasing complexity naturally results in an increasing number of security threats. It is well known that these networks support a large number of services that go beyond traditional voice and short messaging traffic to include high bandwidth data communications.

As all critical infrastructures, telecom assets and facilities are vulnerable to malicious attacks intending their destruction as well as to natural disasters like earthquakes and severe weather conditions, where significant direct and indirect consequences emerge caused by the effects that loss functionality might have on large communities.

In this use-case, a physical attack (sub-scenario 1) or a natural disaster (sub-scenario 2) affects severely the telecom provider's network: in fact unlike the use-case 1, where different physical intrusions enable similar types of cyber threats within a telecom operator's system, in use-case 2, physical threats may result in network service unavailability, but with different causes (either man-

Table 19 Sub Scenarios for Use Case 2		
Sub Use Case	Scenario	Description
2.1	Terrorist Attack in telecom asset cause severe network failure	A hostile UAV is approaching a telecom asset, namely one or more antenna pillars with various types of antennas (base station, links etc.) that are part of the backhaul network. The UAV attack renders the telecom asset (antenna pillar) inoperable because destroyed by bomb. Subsequently the telecom provider's network experiences severe network loss in an extended level. It is considered that mobile communications and generally all the services are down at least in a wide area surrounding the antenna pillar / park.

made or natural disaster), that may require different mitigation measures.

2.2	Natural Disasters affect telecom assets – network loss and telecommunication congestion	A natural disaster, i.e. very severe weather conditions causing twisters and hurricanes or an earthquake, damages telecom assets and facilities located in sub-urban or rural, remote areas. The telecom assets include antenna pillars and buildings containing critical routing circuits (switches, routers etc.) supporting part of the backhaul network. A network failure is caused by the damage on the pillar and the building, leading to a telecommunication congestion in the mobile network.
-----	---	---

According to Use Case 2 described in deliverable D2.8, impacts that can be derived for the Unified Scenario 1 are reported in the following Table 20.

Table 20 Impacts on the Unified Scenario 1 for Use Case 2	
Type	Description
Operational	Risk of Service delivery and network failure especially for mobile communications which would also potentially affect PPDR services as well, if the problem is not quickly restored. Local users would experience prolonged delays in completing voice calls through cellular services, leading to an experience of wireless congestion. The local users may also experience lack of broadcast (TV or radio services) if the antenna pillar incorporates relevant transmission infrastructure. In addition, communication interoperability is scarcely available, accounting for low percent of service and repairs are urgently needed.
Technical	Telecommunications and data connectivity are at risk; network connectivity failure / telephony & internet services face severe problems; especially cellular communications are lost, initially in the proximity to the incident and then in a wider area and routes, especially if the problems caused by the attack or the natural disaster remains unrestored for a significant time period. Heightened usage could stress local telecommunications carriers' network capacity and could result in periods of network congestion on public cellular infrastructure at least in a local level. Congestion could also increase switched-circuit use within the region, leading to "all circuits are busy" messages. In the regions surrounding the most impacted area, communications would likely operate after significant time or be restored through resilience / disaster centers, with the exception of communications facilities that directly rely on the damaged / destroyed underlying infrastructure located in the impacted area.

Economic	A direct impact is the loss of facilities and infrastructure for the telecom provider. Additionally, a significant economic impact is the consumption in time and resources attempting to tackle and restore the problem with the conventional manner (i.e. without the RESISTO system implementation). Although the scenarios are unlikely to create widespread service outages, the surge in demand could impede local commercial or private network customers from accessing and using the network as they would under normal conditions. The precise levels of network failure resulting from both these scenarios would depend on the nature, duration, and exact locations of the events; nonetheless, the network user experience would be substantially reduced in the local level.
Societal	Critical public safety issues, needing further investigation, arise by the facts that on the one hand, an airborne threat hit and destroyed a telecom asset even in a remote location and on the other hand, that a natural disaster damaged the same facility; both incidents would initiate central civil protection actions by the state. The potential scale of public safety coordination could also incorporate other separate public safety agencies. The network disruption or failure could impact other critical infrastructures that may happen to be on the vicinity; offices and homes could suffer significant damage as well. If the problem remains unrestored for a significant period of time, it would cause severe problems in the wider telecom network of the area and the customers' telecom services, while TV and radio may be affected as well.

6.4. Threats and Impacts on CISI Apro

The following table describes cyber and physical threats and shows impacts on CISI Apro, taking into consideration Table 14, where state variables are defined.

Table 21 Cyber and Physical security events for the Unified Scenario 1				
Type	Threat	Sub Use Case	Description	Impacts on CISI Apro
Physical	A UAV (drone) attacks a facility (rooftop antenna or a building)	2.1	Partially or total damage of the facility will result in interruption of services and since this asset supports the wireless backhaul, the telecom service goes down, especially the mobile communications. Thus, network failure and a general DoS at the broader vicinity surrounding the antenna park takes place and the respective users experience total lack of service or telecommunication congestion. Even more, in case that this antenna pillar is a part of a serial sequence of similar assets within the backhaul path, the network failure caused by the damaged antenna pillar is propagated.	Perimeter_Security_Fault Service_fault
Physical	An intruder by an attacker	1.2	The unauthorized person enters the building, gains access to an unattended computer and installs dormant malware that will be activated at some point in the future	Unauthorized_Access

Physical	Earthquake	2.2	Communications assets have not been destroyed, but telecom network is congested as people are seeking information on the earthquake, from both mobile and WiFi networks	Congestion_Fault
Cyber	Cyber-attack through jamming by drones/UAVs	1.1	UAVs, drones or small aircrafts are used by attackers to create undesired electromagnetic signals that could affect a wireless infrastructure: wireless interference of this kind could impose viruses or similar cyber threats by having the drone wirelessly intruding and penetrating to the wireless network of an infrastructure	Service_fault
Cyber	Attacker shuts down internet-connected security cameras		The perimeter protection system (video / audio analysis) is no longer in operation for the detection/classification of anomalous activities	Security_Camera_Fault
Cyber	Malware	1.2	Malware (active or dormant) can be loaded onto a switch initiating a DoS to a server cluster. Thus, network traffic is being caused and specific systems of the core network are being attacked and potentially partially shut down.	Dos_attack

6.5. CISIApro implementation

The Unified Scenario 1, defined to simulate possible terrorist attacks and natural disasters, shown in Figure 27, has been implemented in CISIApro.

The components illustrated and the services provided by the TLC network are described in detail in the following paragraphs.

6.5.1. Description of CISIApro model

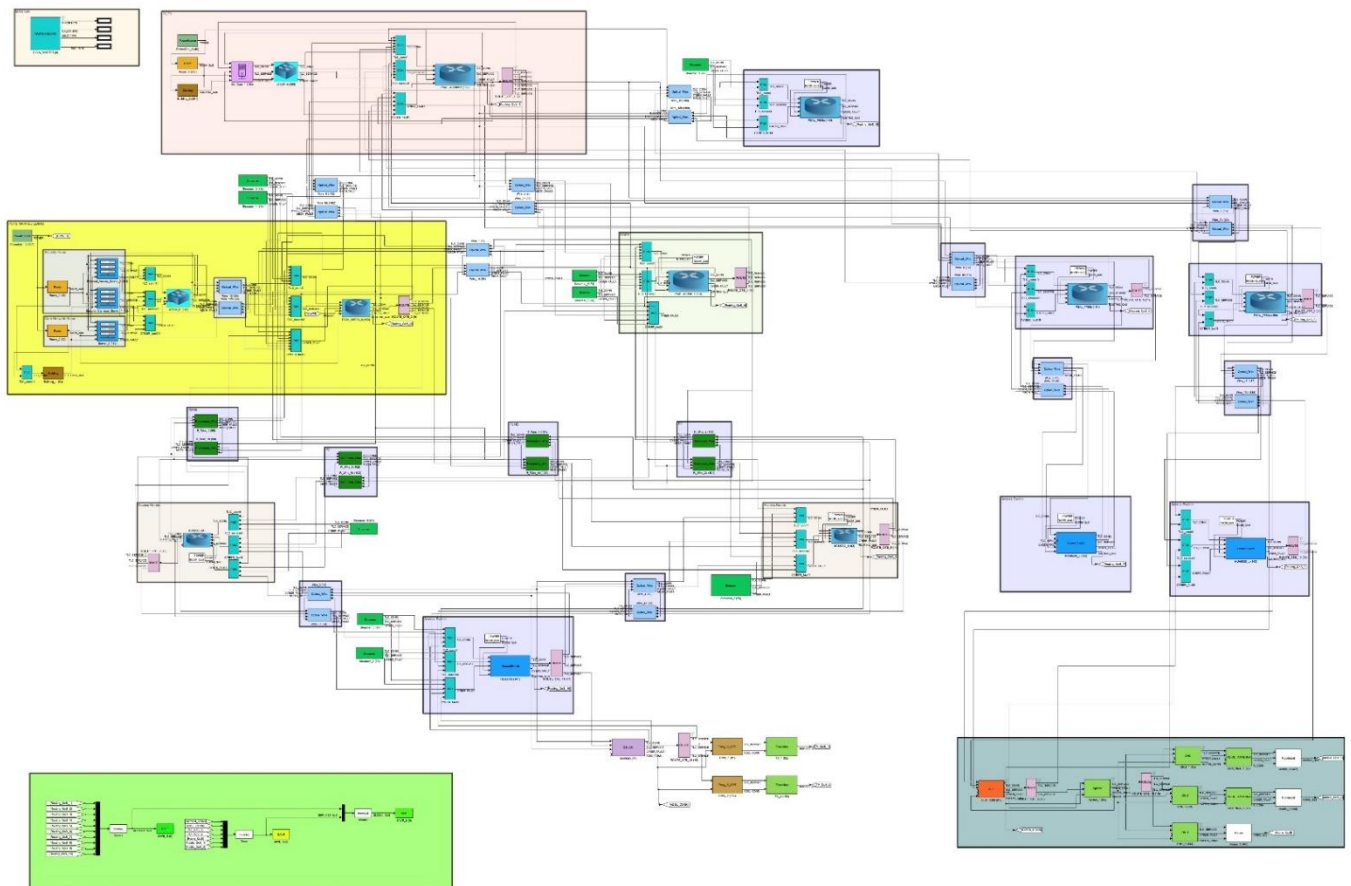


Figure 29 Unified Reference Scenario 1 CISIApro Model top view

The scenario, to simulate the events described in Use Cases 1 and 2, is a building, with antennas on the roof, containing a local POP, a surveillance system (video cameras, radar for detecting air threats, perimeter security, doors with card access ...) and servers with security services.

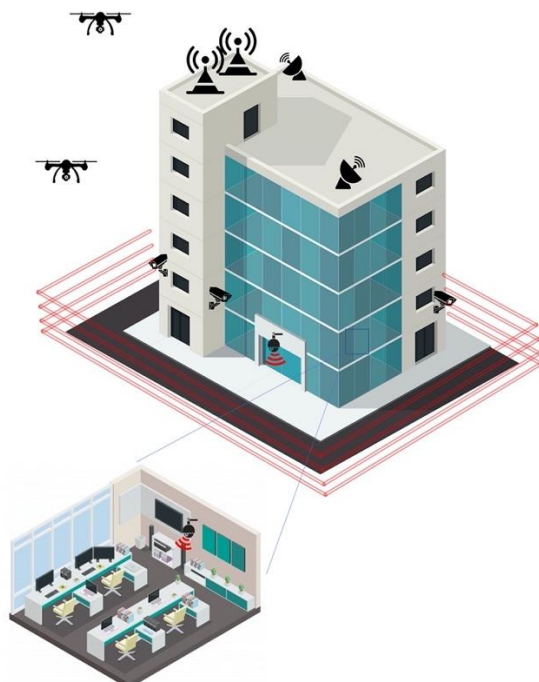


Figure 30 Scenario used for Use Case 1 and 2

The building used as application scenario for the use cases described above, is characterized as follows in CISIApro.

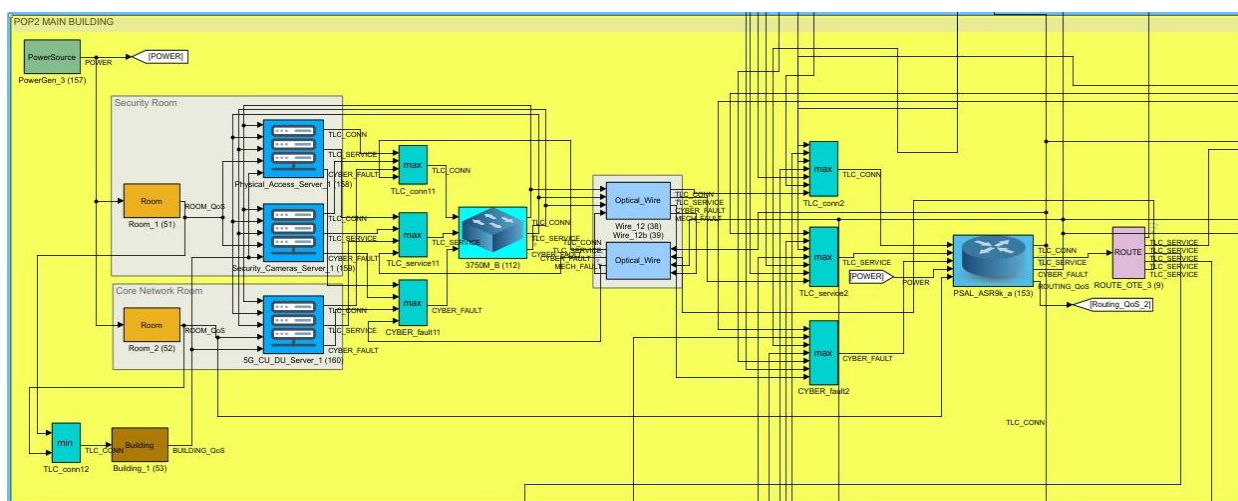


Figure 31 Scenario in CISIApro

6.5.2. Model design: entities for Unified Scenario 1

In order to better understand the CISIApro diagram in Figure 27, all the components defined to model the Unified Scenario 1 have been reported in the following table.

As can be seen from Table 22, the corresponding entity type is also reported for each component.

Table 22 Entities for Unified Scenario 1	
Entity Name	Entity Type
3750M_A	CISCOswitch
3750M_B	CISCOswitch
5G_Core_1	5G_Core
ANTENNA_1	RU-DU_ANTENNA
ANTENNA_2	RU-DU_ANTENNA
BLM_1500	OLT
Building_1	Building
Building_2	Building
Entry_1	Entry_2i_CPE
Entry_2	Entry_2i_CPE
HUA9306	HuaweiSwitch
HUA9306_b	HuaweiSwitch
HUA9306_c	HuaweiSwitch
House_1	House
MA5603	DSLAM
Mobile_1	MobileUnit
Mobile_2	MobileUnit
NCS5002_1	CISCO_router
NV9200	CISCO_router
ONU_1	ONU
ONU_2	ONU
ONU_3	ONU
PSAL_7609a	CISCO_router

PSAL_7750a	CISCO_router
PSAL_7750b	CISCO_router
PSAL_ASR9912	CISCO_router
PSAL_ASR9k_a	CISCO_router
PSAL_ASR9k_b	CISCO_router
Physical_Access_Server_1	App_Server
PowerGen_1	<i>PowerSource</i>
PowerGen_3	PowerSource
ROUTE_OTE_1	<i>ROUTE</i>
ROUTE_OTE_10	ROUTE
ROUTE_OTE_11	ROUTE
ROUTE_OTE_12	ROUTE
ROUTE_OTE_13	ROUTE
ROUTE_OTE_3	ROUTE
ROUTE_OTE_4	ROUTE
ROUTE_OTE_5	ROUTE
ROUTE_OTE_6	ROUTE
ROUTE_OTE_7	ROUTE
ROUTE_OTE_8	ROUTE
ROUTE_OTE_9	ROUTE
R_Wire_1	Redundant_Wire
R_Wire_1b	Redundant_Wire
R_Wire_2	Redundant_Wire
R_Wire_2b	Redundant_Wire
R_Wire_3	Redundant_Wire
R_Wire_3b	Redundant_Wire
R_Wire_4	Redundant_Wire
R_Wire_4b	Redundant_Wire
Room_1	Room

Room_2	Room
Room_3	Room
Security_Cameras_Server_1	App_Server
5G_CU_DU_Server_1	App_Server
Splitter_1	Splitter
Streamer_1	Streamer
Streamer_2	Streamer
Streamer_3	Streamer
Streamer_4	Streamer
Streamer_5	Streamer
Streamer_6	Streamer
Streamer_7	Streamer
Streamer_8	Streamer
Streamer_9	Streamer
TV_1	Television
TV_2	Television
Wire_1	Optical_Wire
Wire_12	Optical_Wire
Wire_12b	Optical_Wire
Wire_17	Optical_Wire
Wire_17b	Optical_Wire
Wire_18	Optical_Wire
Wire_18b	Optical_Wire
Wire_1b	Optical_Wire
Wire_2	Optical_Wire
Wire_2b	Optical_Wire
Wire_3	Optical_Wire
Wire_3b	Optical_Wire
Wire_4	Optical_Wire

Wire_4b	Optical_Wire
Wire_5	Optical_Wire
Wire_5b	Optical_Wire
Wire_6	Optical_Wire
Wire_6b	Optical_Wire
Wire_7	Optical_Wire
Wire_7b	Optical_Wire

6.5.3. Model design: services associated to entities

The following table shows the services associated with each entity used in CISIApro model.

Table 23 Services for Unified Scenario 1	
Entity Name	Services
Security_Cameras_Server_1	security_cameras
Physical_Access_Server_1	door_access
Physical_Access_Server_1	perimeter_security
5G_CU_DU_Server_1	5G_core
5G_CU_DU_Server_1	CU_DU
Streamer_1	HE-BTV 1
Streamer_2	HE-BTV 1
Streamer_3	HE-BTV 1
Streamer_4	HE-BTV 1
Streamer_5	HE-BTV 1
Streamer_6	HE-BTV 1
Streamer_7	HE-BTV 1
Streamer_8	HE-BTV 1
Streamer_9	HE-BTV 1

7. USE CASE 6: CYBER AND PHYSICAL PROTECTION OF NETWORK AND NETWORK ELEMENTS MECHANISMS USED BY CRITICAL SERVICES THAT IMPACT USERS (ORO TESTBED)

7.1. Unified Reference Scenario 2

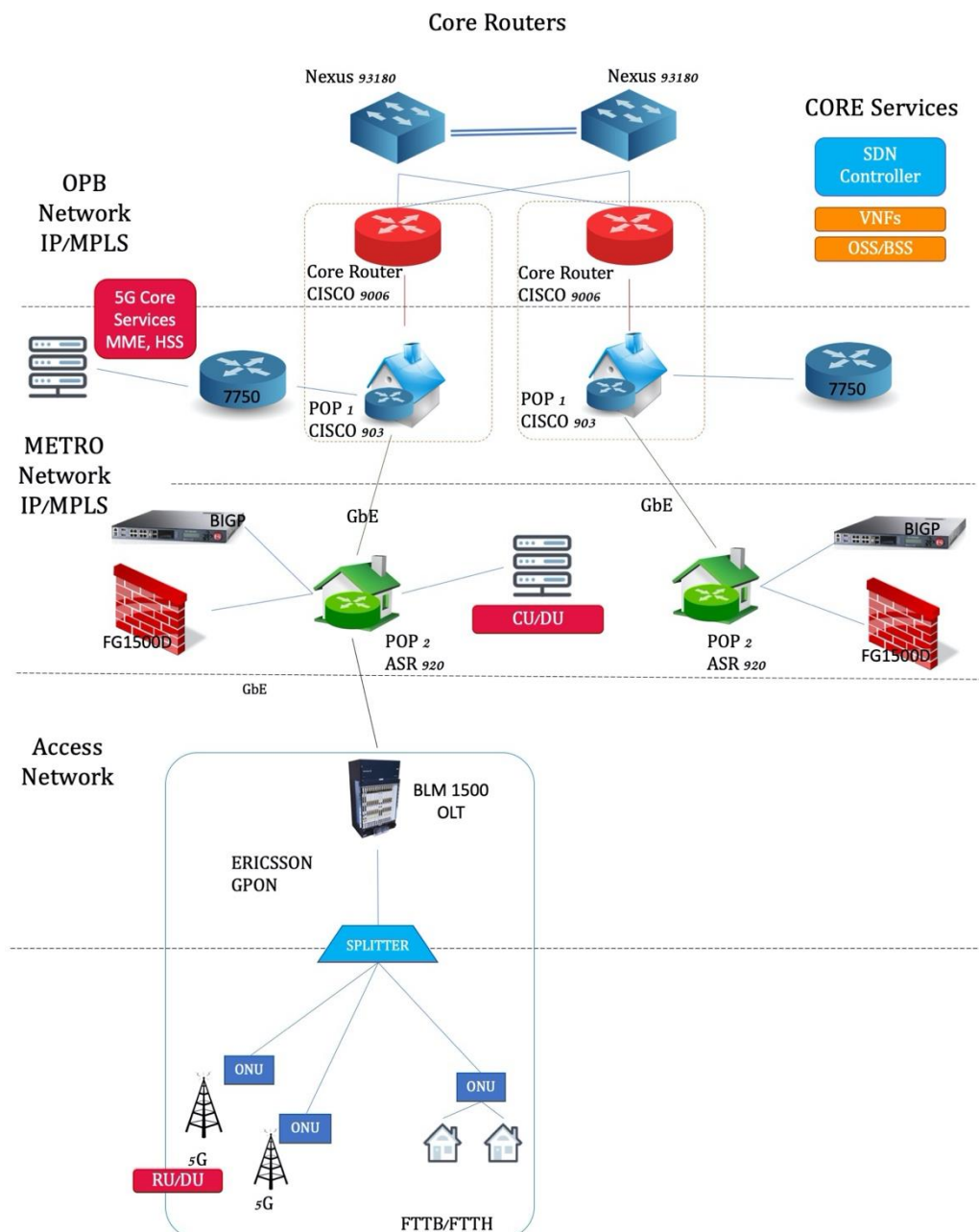


Figure 32 Unified Scenario 2: Use Case 6 – ORO Testbed

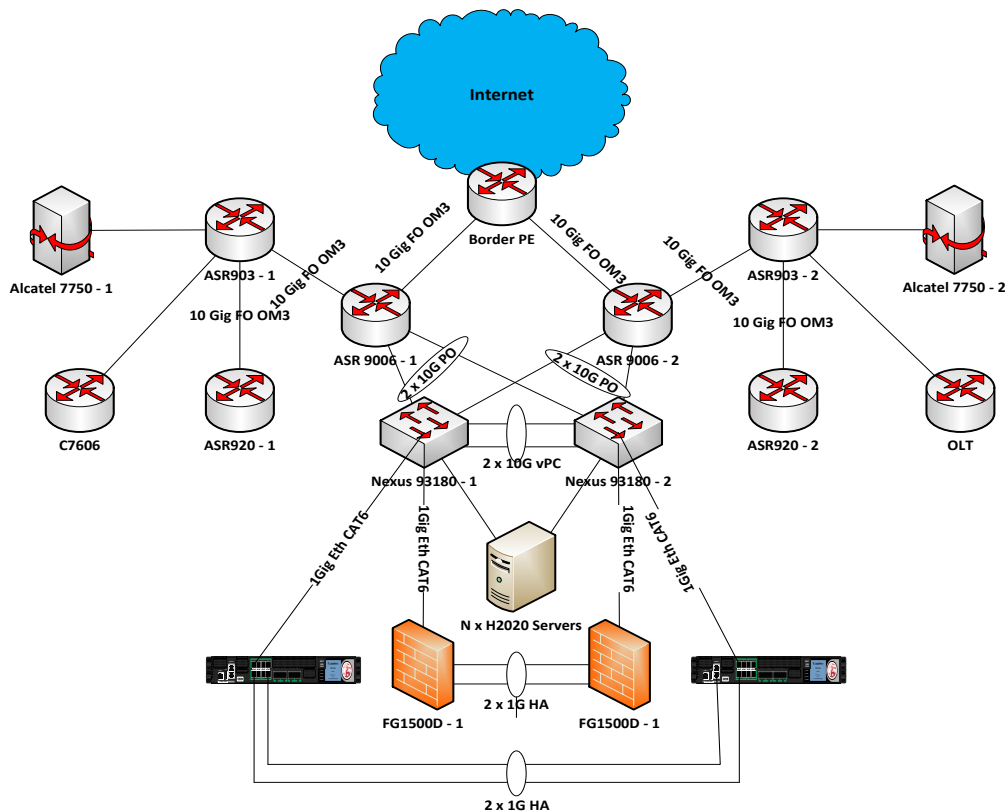


Figure 33 ORO Testbed

The testbed shown in Figure 33 is created with the aim of showing the effects that the combined threats to cyber and physical security have on fixed and 4G / 5G services that affect users.

The ORO Test Bed has a redundant architecture: most resources, both physical equipment and virtual machines, are indeed doubled. This is equipped with various network elements ranging from high speed backbone routers to mobile and B2B access routers. The equipment forms a MPLS network and are aggregated using high speed links on the pair of Nexus switches.

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

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

Starting from the Testbed in Figure 33, the network architecture for the Unified Scenario 2 is characterized by the components that are described in Table 24.

Table 24 TLC Network Elements for Reference Scenario 2					
TLC Network Elements	Network	Services	Testbed Components		
			Component	Name	Description
CORE network	MPLS	OpenStack	ASR 9006-1 ASR 9006-2 Nexus 93180	Cisco ASR9000 Series Aggregation Service Router	Border Router/ Core Router
METRO nodes/ POP level 1			ASR 903-1 ASR 903-2	Cisco ASR9000 Series Aggregation Service Router	Distribution Router
METRO network	MPLS				
POP level 2			ASR 920-1 ASR 920-2	Cisco ASR920 Series Aggregation Service Router	Access Router
Access Network	Passive Optical Network		OLT	Optical Line Terminal	
Access Node					
Premises node		RU	ONU, Antenna		
End Users			Mobile		

7.2. Threats and Impacts on CISI Apro

The following table describes cyber and physical threats and shows impacts on CISI Apro, taking into consideration Table 14, where state variables are defined.

Table 25 Cyber and Physical security events for the Unified Scenario 2			
Type	Threat	Description	Impacts on CISI Apro
Cyber	DDoS attack on border router	A Distributed Denial of Service attack on a border router point, stemming from OROs networks (both fixed and mobile will be tested).	<i>Service_fault</i>
Cyber	DDoS attack on peering point (in conjunction with partner TELCO)	A DDoS attack on a peering router used for interconnection with another ISP/TELCO.	<i>Service_fault</i>
Cyber	Routing Table Poisoning on Core Network	A modification of the routing table(s) of network equipment used in OROs networks that re-routes legitimate traffic from the legitimate destination(s)	<i>Service_fault</i>
Cyber	Botnet C2C server communication from internal network end-points	Communication between infected end-points inside OROs security perimeter to a known Command and Control (C2C) server used by a Bot Network	<i>Service_fault</i>
Physical	Link Disruption (Cable cut)	A simulation of a fiber cut between MSC Sites – in the Test Bed this will be performed by physically disconnecting the equipment	<i>Conn_fault</i>
Physical	Rogue access to MSC Site (break in)	Unauthorized access to a MSC Site by breaking through the physical security perimeter, gaining access to the equipment hosted in the site	<i>Perimeter_Security_Fault</i>
Physical	Rogue access to OROs Core Network Datacenter(s)	Unauthorized access to OROs Core Network Datacenter(s) by breaking through the physical security perimeter, gaining access to the equipment hosted in the site	<i>Perimeter_Security_Fault</i>

Physical	Power Outage in MSC Site (unintentional)	The interruption of power delivery to a MSC Site due to severe weather breaking the power lines	<i>Power_Fault Conn_fault</i>
----------	--	---	-----------------------------------

7.3. Sub Use Cases and Impacts on the Unified Scenario

In ORO use case, two sub-cases are considered to test the scenarios.

Table 26 Sub Use Cases for Use Case 6		
Sub Use Case	Scenario	Description
6.1	DDoS Attack and Fiber Cut	An unintentional fiber cut, resulting from civil works, will sever the connections between the two MSCs in ORO's Test Bed. The fiber cut will be followed by a large-scale DDoS attack on one of OROs border routers
6.2	Rogue access to OROs Core Network and Routing Table Poisoning	A human actor enters in one of OROs Core Network and attempts to connect to a border router, access its administrative console and maliciously change a route to one of OROs servers hosting a critical part of OROs Core Network.

According to Use Case 6 described in deliverable D2.8, impacts that can be derived for the Unified Scenario 2 are reported in the following Table 27.

Table 27 Impacts on the Unified Scenario 2	
Type	Description
Operational	Risk of connectivity loss and service delivery failure
Technical	Connectivity Failure, Data Integrity Corruption, Data Confidentiality Corruption. Impacted areas will deal with loss of connectivity to voice and/or data services
Economic	SLAs will be breached for most customers
Societal	Telephony, Internet Services will be affected in large areas causing disruption of normal social interactions in both Consumer and Business areas

7.4. CISIApro implementation

The goal of Use Case 6 is to understand how physical and cyber-attacks affect the functionality of critical services such as voice and data communications on 4G / 5G and fixed networks. To simulate the events described in this Use Case, the following CISIApro model was designed, where the end users are the mobile units and the houses that require voice and data services.

7.4.1. Description of CISIApro model



Figure 34 Unified Scenario 2 CISIApro Model top view

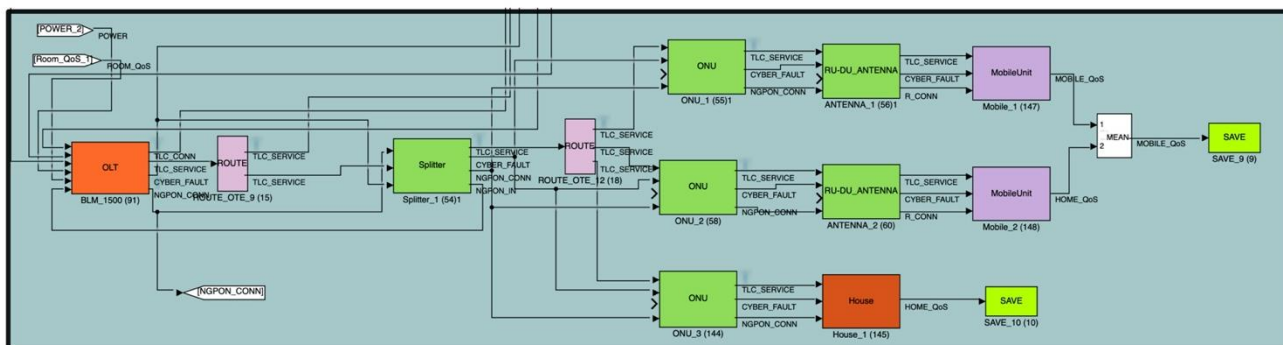


Figure 35 End Users in Unified Scenario 2

7.4.2. Model design: entities for Unified Scenario 2

The following table lists all the entities that have been implemented for this examined scenario.

Table 28 Entities for Unified Scenario 2	
Entity Name	Entity Type
5G_CU_DU_Server_1	App_Server
5G_Core_1	5G_Core
ANTENNA_1	RU-DU_ANTENNA
ANTENNA_2	RU-DU_ANTENNA
ASR9006_1	CISCO_router
ASR9006_2	CISCO_router
ASR903_1	CISCO_router
ASR903_2	CISCO_router
ASR920_1	CISCO_router
ASR920_2	CISCO_router
Alcatel_1	Alcatel7750
Alcatel_2	Alcatel7750
BIGP_1	F5BIGP
BIGP_2	F5BIGP

BLM_1500	OLT
Building_1	Building
Building_1	Building
Building_3	Building
Building_4	Building
FG1500_1	FortiGate1500D
FG1500_2	FortiGate1500D
House_1	House
Mobile_1	MobileUnit
Mobile_2	MobileUnit
Nex_1	Nexus93180Switch
Nex_2	Nexus93180Switch
ONU_1	ONU
ONU_2	ONU
ONU_3	ONU
PowerGen_1	PowerSource
PowerGen_2	PowerSource
PowerGen_3	PowerSource
PowerGen_4	PowerSource
ROUTE_1	ROUTE
ROUTE_2	ROUTE
ROUTE_OTE_12	ROUTE
ROUTE_OTE_9	ROUTE
R_Wire_1	Redundant_Wire
R_Wire_1b	Redundant_Wire
Room_1	Room
Room_2	Room
Room_2	Room
Room_3	Room

Splitter_1	Splitter
Wire_1	Optical_Wire
Wire_10	Optical_Wire
Wire_10b	Optical_Wire
Wire_11	Optical_Wire
Wire_11b	Optical_Wire
Wire_12	Optical_Wire
Wire_12b	Optical_Wire
Wire_13	Optical_Wire
Wire_13b	Optical_Wire
Wire_14	Optical_Wire
Wire_14b	Optical_Wire
Wire_15	Optical_Wire
Wire_15a	Optical_Wire
Wire_1b	Optical_Wire
Wire_2	Optical_Wire
Wire_2b	Optical_Wire
Wire_3	Optical_Wire
Wire_3b	Optical_Wire
Wire_4	Optical_Wire
Wire_4b	Optical_Wire
Wire_5	Optical_Wire
Wire_5b	Optical_Wire
Wire_6	Optical_Wire
Wire_6b	Optical_Wire
Wire_7	Optical_Wire
Wire_7b	Optical_Wire
Wire_8	Optical_Wire
Wire_8b	Optical_Wire

Wire_9	Optical_Wire
Wire_9b	Optical_Wire

7.4.3. Model design: services associated to entities

The following Table 29 shows the TLC services provided by the entities outlined in the CISIApro model, relating to Unified Scenario 2.

Table 29 Services for Use Case 6	
Entity Name	Services
5G_CU_DU_Server_1	CU_DU
5G_Core_1	5G_Core
BIGP_1	Web Application Firewall
BIGP_1	Enhanced application layer enrichment and protection
BIGP_2	Web Application Firewall
BIGP_2	Enhanced application layer enrichment and protection
FG1500_1	URL Filtering
FG1500_1	Centralised Antivirus
FG1500_1	IDS and IPS
FG1500_1	DLP
FG1500_1	E-mail filtering
FG1500_1	Layer 4 Firewall
FG1500_2	URL Filtering
FG1500_2	Centralised Antivirus
FG1500_2	IDS and IPS
FG1500_2	DLP
FG1500_2	E-mail filtering
FG1500_2	Layer 4 Firewall

8. USE CASE 9: 5G NETWORK RESPONSE TO A SECURITY BREACH (ALB TESTBED)

8.1. Unified Reference Scenario 3

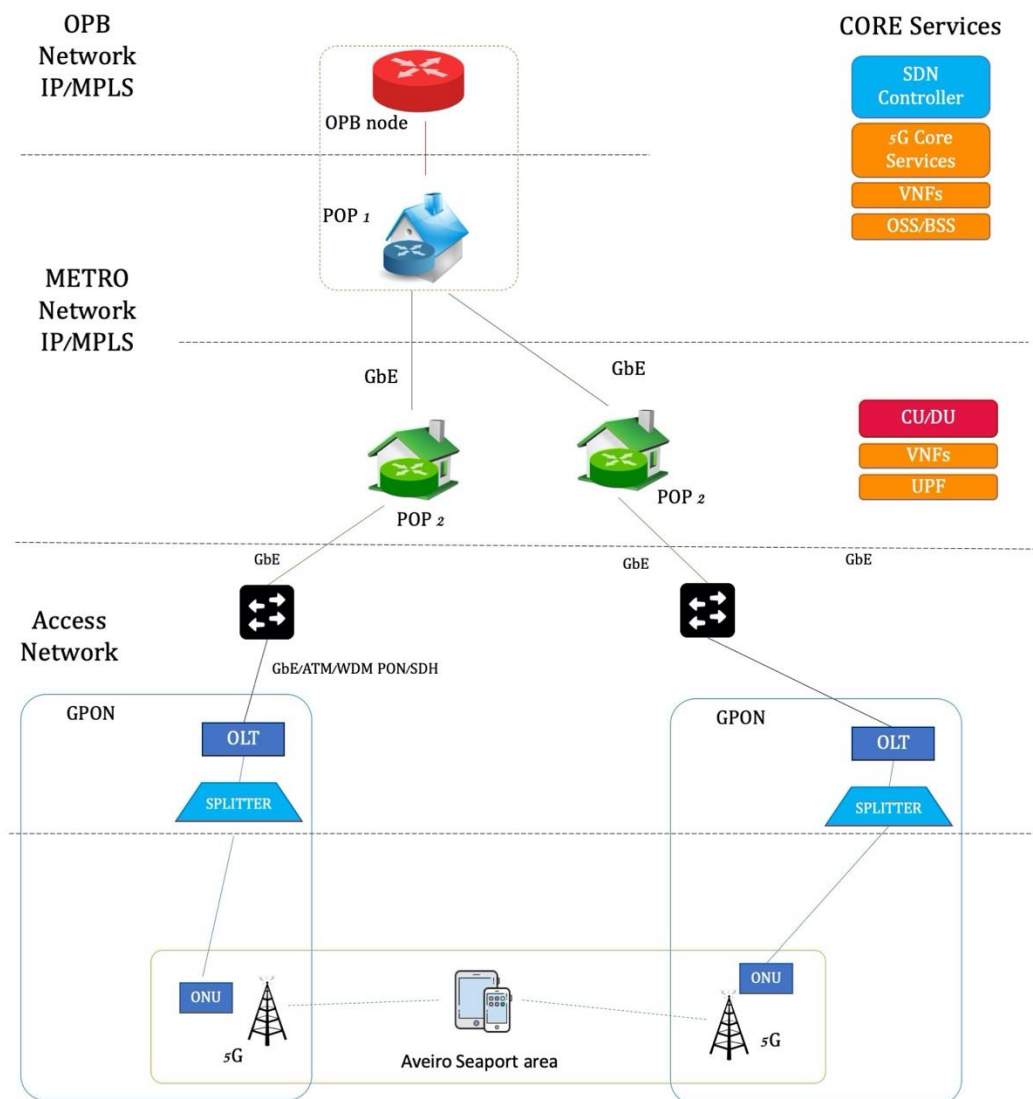


Figure 36 Unified Scenario 3: Use Case 9 – ALB Testbed

5G systems are the next step in the evolution of mobile communication: these need to provide capabilities, not only for voice and data communication, but also for new use cases and new industries, and for a multitude of devices and applications to connect society at large.

In addition, 5G provides a number of tools to avoid or mitigate the effects of security and resilience threats.

Figure 37 illustrates the topology of the testbed that will support the 5G use case, from which the Unified Scenario 3 was outlined, as well as the main components, which are described in Table 30.

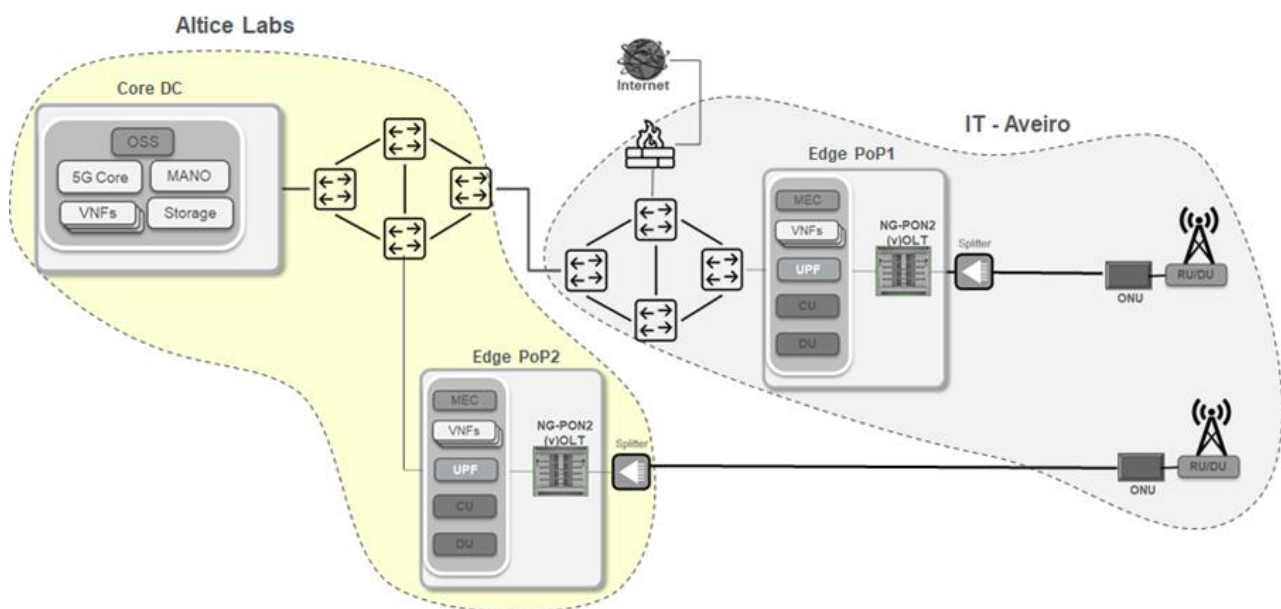


Figure 37 ALB Testbed

Table 30 TLC Network Elements for Reference Scenario 3

TLC Network Elements	Network	Services	Testbed Components		
			Component	Name	Description
CORE network	MPLS	5G Core MANO VNFs Storage			
METRO nodes/ POP level 1					
METRO network	MPLS				
POP level 2		MEC VNFs UPF CU DU	2 Edge POP		
Access Network	Passive Optical Network		OLT	Optical Line Terminal	
Access Node			SPLITTER, FTTP, FTTC		
Premises node		RU	ONU, Antenna		
End Users			Factory IT Area		

8.2. Threats and Impacts on CISIApro

Table 31 describes cyber and physical threats and shows impacts on CISIApro, taking into consideration Table 14, where state variables are defined.

Table 31 Cyber and Physical security events for the Unified Scenario 3			
Type	Threat	Description	Impacts on CISIApro
Cyber	DoS attacks in the infrastructure		Service_fault
Cyber	DoS attacks on end-user devices		Service_fault
Physical	Terrorism sabotage	A terrorism sabotage produces the Network Outage and the Service delivery failure in a geographical area	Service_fault
Physical	Forest Fire	This event endangers significant components of the network infrastructure physically located in that area	Mechanical_Fault

8.3. Impacts on the Unified Scenario

According to Use Case 9 described in deliverable D2.8, impacts that can be derived for the Unified Scenario 3 are reported in Table 32.

Table 32 Impacts on the Unified Scenario 3	
Type	Description
Operational	Service delivery failure in a geographical area, as a result of intentional malicious actions (e.g. cyber-physical attacks, motivated either by terrorism and economic sabotage), equipment malfunctions or natural events (e.g. forest fire, potentially endangering significant components of the network infrastructure physically located on that zone)
Economic	Financial losses, both to operators (loss of income, customer churn) and end users (especially businesses for which communication is a critical requirement)
Societal	Damages caused by network disruptions, especially in emergency scenarios, potentially exposing human lives to risk

8.4. CISIApro implementation

This chapter shows the CISIApro scheme implemented to simulate the Use Case 9 and describes the different entities used and the related services.

As shown in the Testbed in Figure 37, also in the following diagram the physical resources are located in two sites, Alice Labs headquarters and the Institute of Telecommunications, both located in the city of Aveiro.

8.4.1. Description of CISIApro model

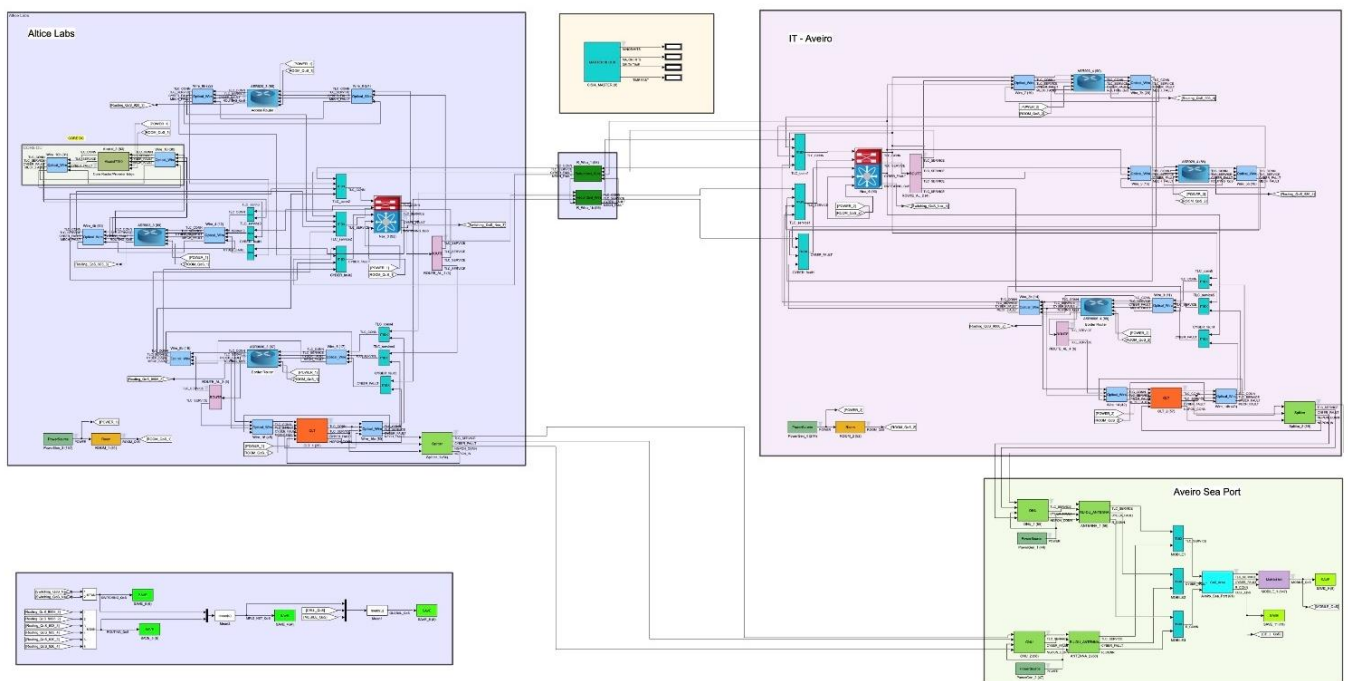


Figure 38 Unified Scenario 3 CISIApro Model top view

In CISIApro, Aveiro Sea Port was designed as shown in Figure 39, where it is possible to notice that the services and the connection are provided to the Cell_Area through an RU-DU Antenna.

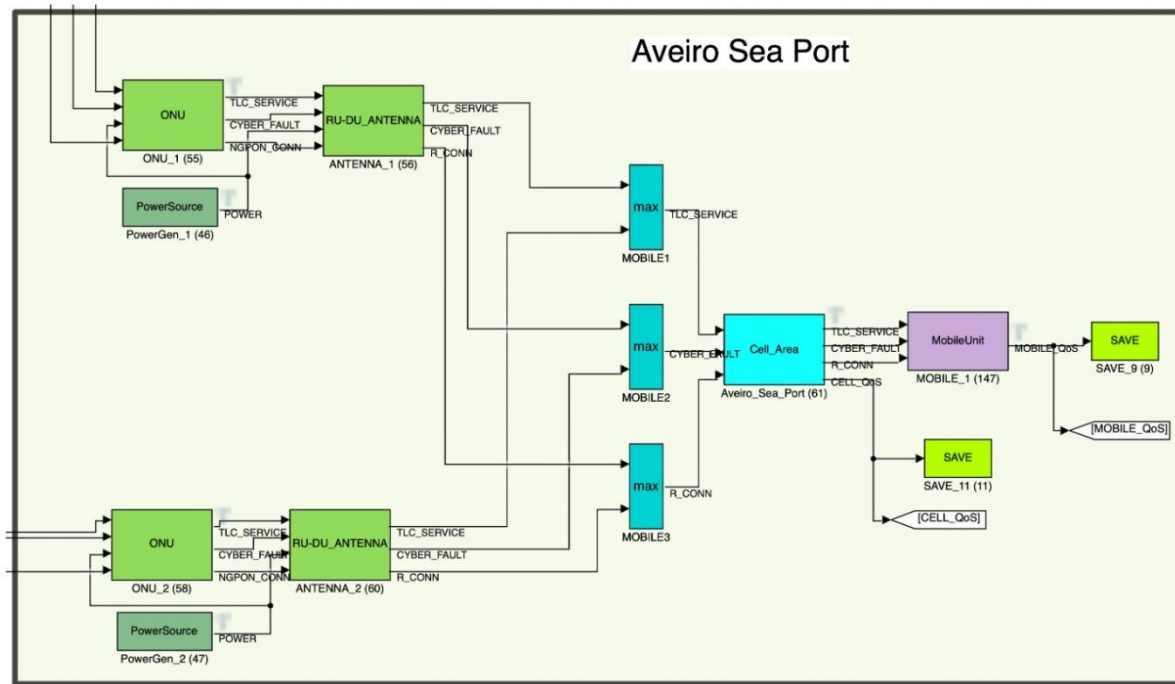


Figure 39 Aveiro Sea Port in CISIApro

8.4.2. Model design: entities for Unified Scenario 3

All the entities explained in the diagram in Figure 38 are listed in the following table, in which also the type of entity is specified.

Table 33 Entities for Unified Scenario 3	
Entity Name	Entity Type
ANTENNA_1	RU-DU_ANTENNA
ANTENNA_2	RU-DU_ANTENNA
ASR9006_3	CISCO_router
ASR9006_4	CISCO_router
ASR903_3	CISCO_router
ASR903_4	CISCO_router
ASR920_3	CISCO_router
ASR920_4	CISCO_router

Alcatel_3	Alcatel7750
Aveiro_Sea_Port	Cell_Area
MOBILE1	MobileUnit
MOBILE2	MobileUnit
MOBILE3	MobileUnit
MOBILE_1	MobileUnit
Nex_3	Nexus93180Switch
Nex_4	Nexus93180Switch
OLT_1	OLT
OLT_2	OLT
ONU_1	ONU
ONU_2	ONU
PowerGen_1	PowerSource
PowerGen_2	PowerSource
PowerGen_3	PowerSource
PowerGen_4	PowerSource
ROOM_1	Room
ROOM_2	Room
ROUTE_AL_1	ROUTE
ROUTE_AL_2	ROUTE
ROUTE_AL_3	ROUTE
ROUTE_AL_4	ROUTE
R_Wire_1	Redundant_Wire
R_Wire_1b	Redundant_Wire
Splitter_1	Splitter
Splitter_2	Splitter
Wire_10	Optical_Wire
Wire_10b	Optical_Wire
Wire_14	Optical_Wire

Wire_14b	Optical_Wire
Wire_16	Optical_Wire
Wire_16a	Optical_Wire
Wire_3	Optical_Wire
Wire_3b	Optical_Wire
Wire_4	Optical_Wire
Wire_4b	Optical_Wire
Wire_5	Optical_Wire
Wire_5b	Optical_Wire
Wire_6	Optical_Wire
Wire_6b	Optical_Wire
Wire_7	Optical_Wire
Wire_7b	Optical_Wire
Wire_8	Optical_Wire
Wire_8b	Optical_Wire

8.4.3. Model design: services associated to entities

The TLC services associated with the model's entities in Figure 38 are specified below.

Table 34 Services for Use Case 9	
Entity Name	Services
ANTENNA_1	Antenna_Slice_5G
ANTENNA_2	Antenna_Slice_5G

9. USE CASE 4: DISRUPTION OF MAJOR SPORTING EVENT BY COMBINED PHYSICAL & CYBER-ATTACK BY TERRORIST ORGANIZATION (BTC TESTBED)

9.1. Unified Reference Scenario 4

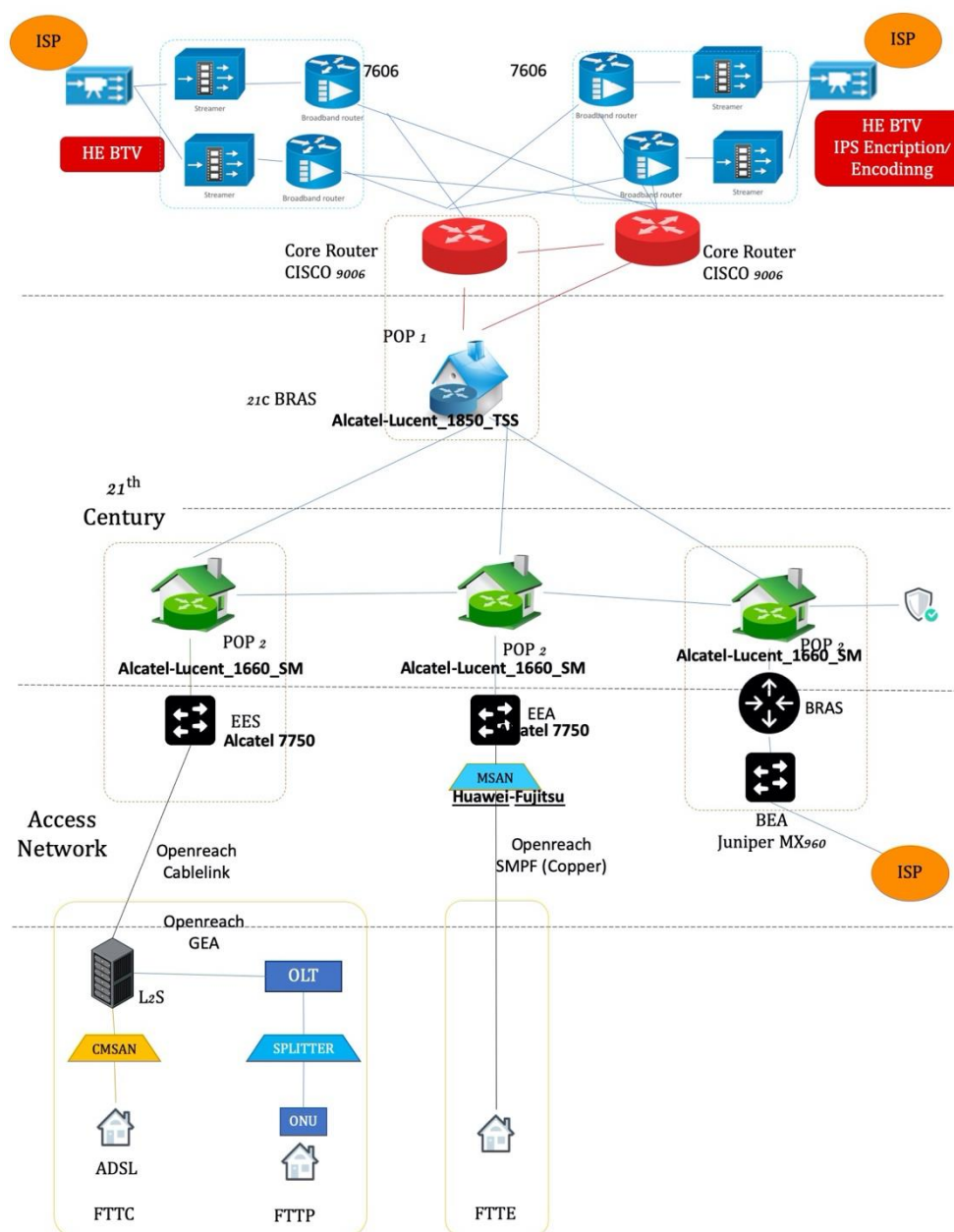


Figure 40 Unified Scenario 4: Use Case 4 – BTC Testbed

Use Case 4 focuses mainly on disruptions and resilience during major sporting events on communication infrastructure by studying IPTV delivery over IP networks. In fact, in a major sporting event, such as the Olympic or World Cup football championships, smooth delivery of live, linear TV streams to a variety of IP devices such as digital TV boxes, tablets or smartphones can be a challenge for the underlying communication infrastructures due to the expected high number of users/viewers and the huge growth in video to mobile devices.

The Unified Scenario 4 in Figure 40 was designed in order to assess the system's resilience following a physical or cyber-attack during an important sporting event.

The TLC network architecture takes inspiration from the BTC testbed in Figure 41.

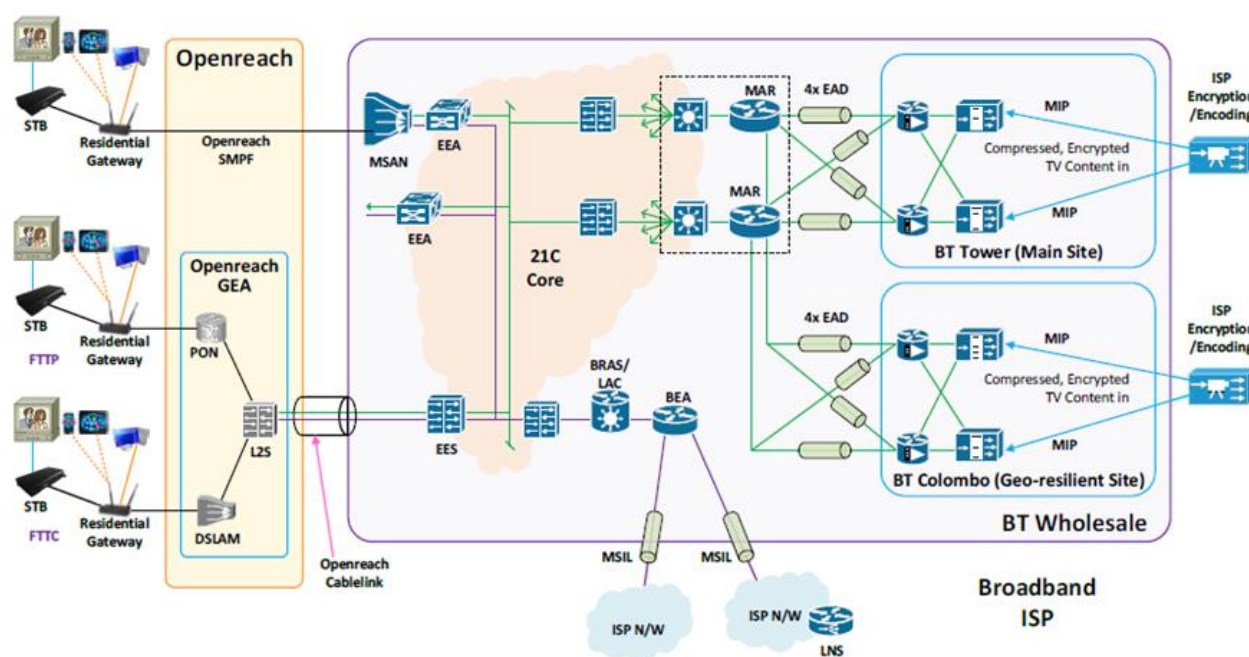


Figure 41 BTC Testbed

The elements of the Unified Scenario 4 are expressed in the following table and divided according to the level of the network to which they belong.

Table 35 TLC Network Elements for Reference Scenario 4					
TLC Network Elements	Network	Services	Testbed Components		
			Component	Name	Description
CORE network	IP	ISP, ISP Encryption/ Encoding, IPTV service	Cisco Router 9006		
METRO nodes/ POP level 1			Alcatel-Lucent 1850 TSS		
METRO network	IP				
POP level 2			Alcatel-Lucent 1660 SM		
Access Network			EEA, EES, BRAS, BEA		
Access Node			C-MSAN, F-MSAN (FTTC – FTTP)		
Premises node			Residential Gateway		
End Users			SBT+TV, PC, Mobile		

9.2. Threats and Impacts on CISI Apro

Table 36 describes cyber and physical threats and shows impacts on CISI Apro, taking into consideration Table 14, where state variables are defined.

Table 36 Cyber and Physical security events for the Unified Scenario 4			
Type	Threat	Description	Impacts on CISI Apro
Physical	Terroristic Attacks	Terroristic Attacks on BT Tower and BT Geo-resilient site	Service_fault
Physical	Cable cuts		Conn_fault
Physical	Unauthorized access		Unauthorized_Access

Cyber	DdoS Attack to multicast routers	In the DdoS attack during a major sporting event, a sudden flood of packet retransmission requests will be received by the retransmission server. Since the lost packets are retransmitted to a huge number of end-devices within the same time using unicast (one-to-one) transmission, it may unbalance and overload the core network which may lead to interrupted video delivery	<i>Congestion_Fault</i>
Cyber	DdoS attacks using end user devices	If end-user devices are used to launch DdoS attacks, then end-user device logs can be used to identify abnormal activity by disabling these devices or by analysing the traffic model to discover these attacks	<i>Congestion_Fault</i>
Cyber	Injecting wrong video contents for terrorist propaganda	Terrorists attack core CDN routers / servers for initiating incorrect content	Data_Corruption
Cyber	Modification of messages		Data_Corruption

9.3. Impacts on the Unified Scenario

According to Use Case 4 described in deliverable D2.8, impacts that can be derived for the Unified Scenario 4 are reported in Table 37.

Table 37 Impacts on the Unified Scenario 4

Type	Description
Operational	Risk of linear TV service loss (unavailable service), degradation of quality of service, unbalanced network loads (network congestion).
Technical	Unicast or multicast nodes running at maximum capacity, corrupted multicast packets, high multicast transmission error rates.

Economic	Breach of SLA with end-users and wholesale customers which may lead to financial loss due to compensation arrangement.
Societal	Loss of good reputations of the IPTV providers and loss of consumer data such as identity and transactions.

9.4. CISIApro implementation

The Unified Scenario 4, created to simulate BTC Use Case, is modelled in CISIApro as shown in Figure 42. This model represents the typical network infrastructure for delivering video streams to different types of video clients or end-devices.

9.4.1. Description of CISIApro model

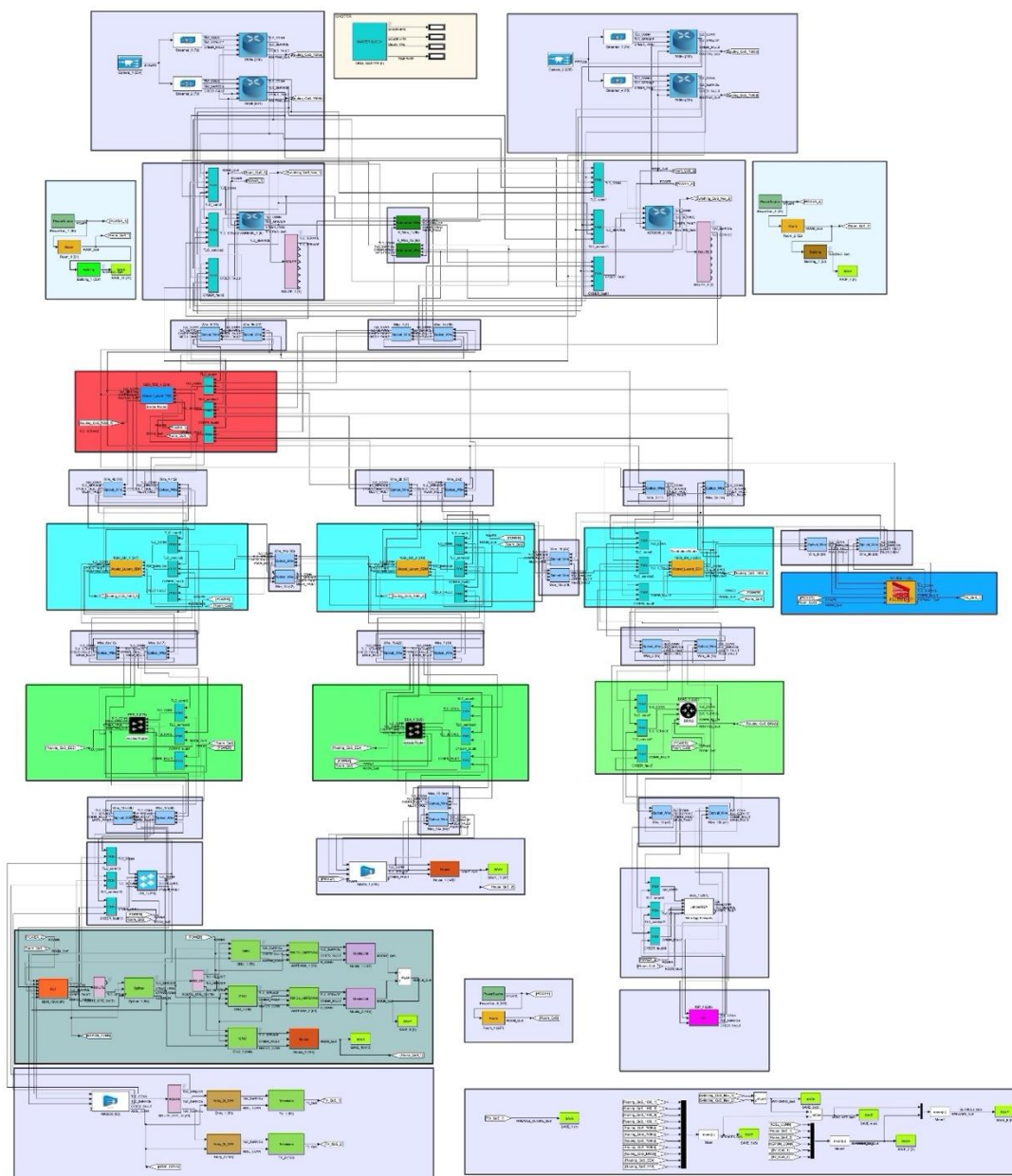


Figure 42 Unified Scenario 4 CISIApro Model top view

The clients in the network consuming the video streams simultaneously are defined in Figure 43.

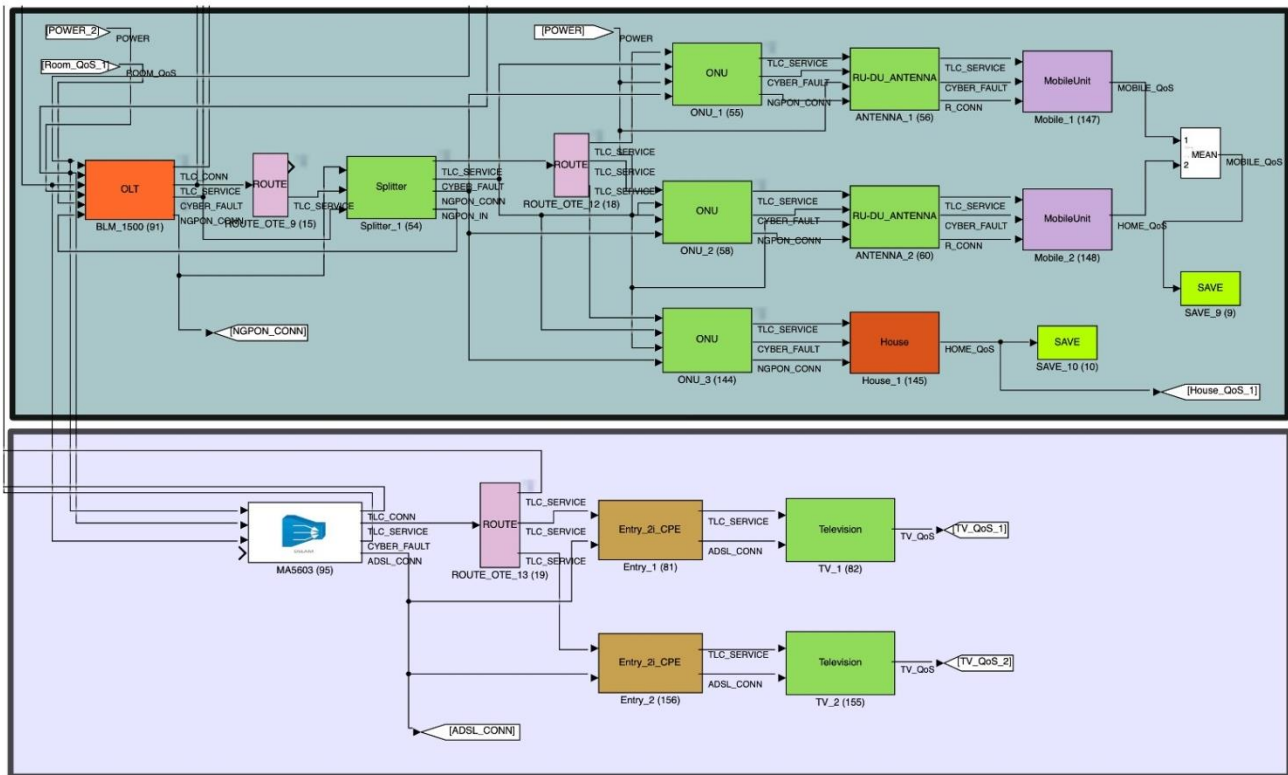


Figure 43 End-devices in Unified Scenario 4

9.4.2. Model design: entities for Unified Scenario 4

All the components in the infrastructure in Figure 42 that could suffer cyber-physical attacks are listed in the following table.

Table 38 Entities for Unified Scenario 4	
Entity Name	Entity Type
1660_SM_1	Alcatel_Lucent_SDH
1660_SM_2	Alcatel_Lucent_SDH
1660_SM_3	Alcatel_Lucent_SDH
1850_TSS_1	Alcatel_Lucent_TSS
7606a	CISCO_router
7606b	CISCO_router

7606c	CISCO_router
7606d	CISCO_router
ANTENNA_1	RU-DU_ANTENNA
ANTENNA_2	RU-DU_ANTENNA
ASR9006_1	CISCO_router
ASR9006_2	CISCO_router
BEA_1	JuniperBEA
BLM_1500	OLT
BRAS_1	BRAS
Building_1	Building
Building_1	Building
Camera_1	Camera
Camera_2	Camera
EEA_1	Alcatel7750
EES_1	Alcatel7750
Entry_1	Entry_2i_CPE
Entry_2	Entry_2i_CPE
FG1500_1	FortiGate1500D
House_1	House
House_1	House
ISP_1	ISP
L2S_1	Layer2Switch
MA5603	DSLAM
MSAN_1	DSLAM
Mobile_1	MobileUnit
Mobile_2	MobileUnit
ONU_1	ONU
ONU_2	ONU
ONU_3	ONU

PowerGen_1	PowerSource
PowerGen_2	PowerSource
PowerGen_5	PowerSource
ROUTE_1	ROUTE
ROUTE_2	ROUTE
ROUTE_OTE_12	ROUTE
ROUTE_OTE_13	ROUTE
ROUTE_OTE_9	ROUTE
R_Wire_1	Redundant_Wire
R_Wire_1b	Redundant_Wire
Room_1	Room
Room_2	Room
Room_4	Room
Splitter_1	Splitter
Streamer_1	Streamer
Streamer_2	Streamer
Streamer_3	Streamer
Streamer_4	Streamer
TV_1	Television
TV_2	Television
Wire_1	Optical_Wire
Wire_12	Optical_Wire
Wire_12b	Optical_Wire
Wire_13	Optical_Wire
Wire_13b	Optical_Wire
Wire_14	Optical_Wire
Wire_14b	Optical_Wire
Wire_15	Optical_Wire
Wire_15	Optical_Wire

Wire_15a	Optical_Wire
Wire_15a	Optical_Wire
Wire_1b	Optical_Wire
Wire_2	Optical_Wire
Wire_2b	Optical_Wire
Wire_3	Optical_Wire
Wire_3b	Optical_Wire
Wire_4	Optical_Wire
Wire_4b	Optical_Wire
Wire_5	Optical_Wire
Wire_5b	Optical_Wire
Wire_6	Optical_Wire
Wire_6b	Optical_Wire
Wire_7	Optical_Wire
Wire_7b	Optical_Wire
Wire_8	Optical_Wire
Wire_8b	Optical_Wire
Wire_9	Optical_Wire
Wire_9b	Optical_Wire

9.4.3. Model design: services associated to entities

The following table shows the TLC services provided by the specific entities that make up the network infrastructure for the Unified Scenario 4.

Table 39 Services for Use Case 4	
Entity Name	Services
ANTENNA_1	Antenna_Slice_5G
ANTENNA_2	Antenna_Slice_5G
FG1500_1	URL Filtering
FG1500_1	Centralised Antivirus

FG1500_1	IDS and IPS
FG1500_1	DLP
FG1500_1	E-mail filtering
FG1500_1	Layer 4 Firewall
ISP_1	internet_access - ISP
Streamer_1	HE-BTV 1
Streamer_2	HE-BTV 1
Streamer_3	HE-BTV 1
Streamer_4	HE-BTV 1

10. USE CASE 5.1: PROTECTION OF CLOUD STORAGE SERVICES HEALTHCARE SYSTEM (TIM TESTBED)

10.1. Unified Reference Scenario 5

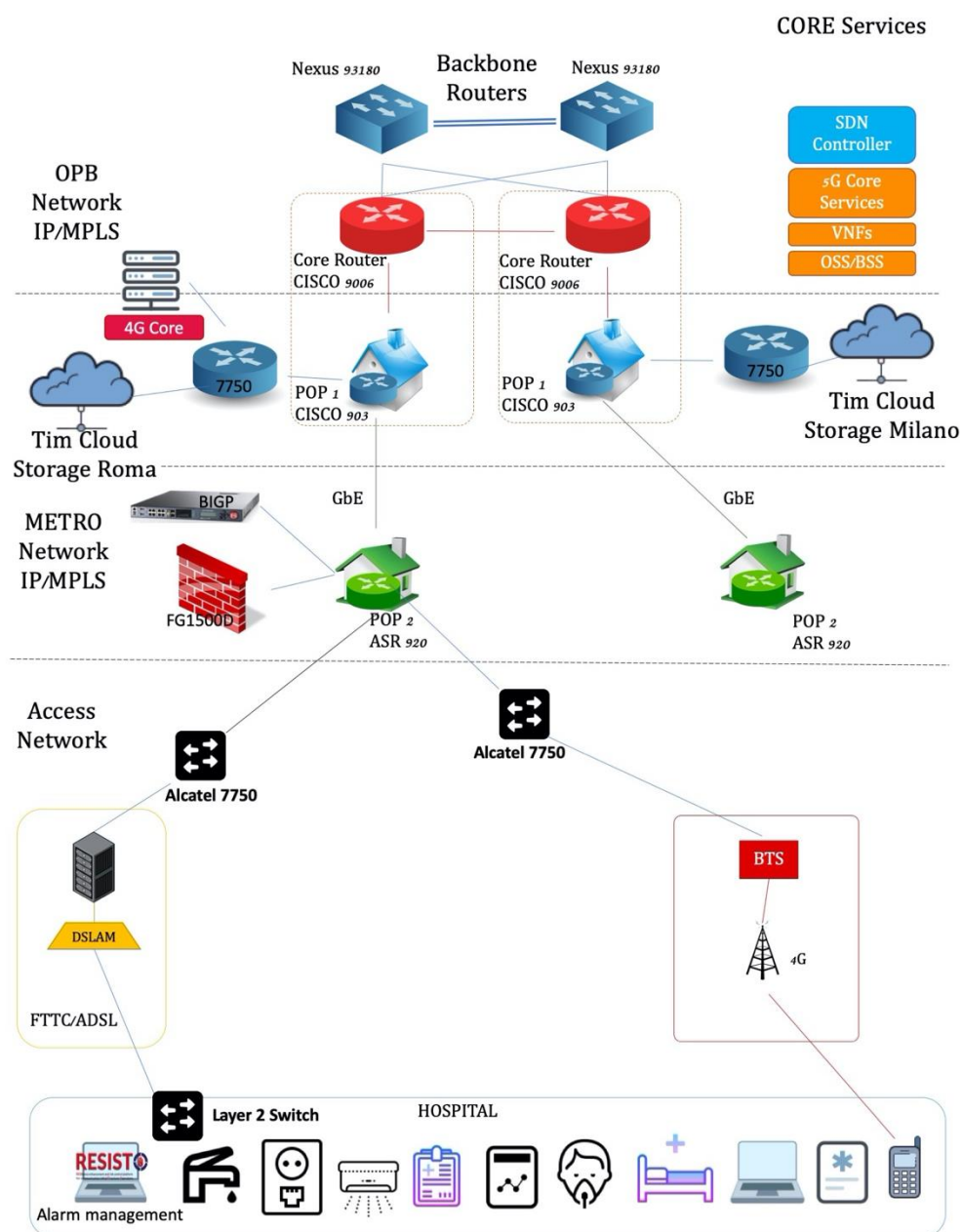


Figure 44 Unified Scenario 5: Use Case 5.1 – TIM Testbed

Health systems are one of the most interesting targets for cyberattacks, as electronic health records (EHR) and all the information regarding patients are very sensitive. Hospitals are increasingly dependent on their ICT systems: the use of connected medical devices and networked systems for normal medical activity expose those systems to both cyber and physical attacks, where the purpose is to disrupt the service or steal sensitive information that could be used for other types of attacks.

Even if other critical infrastructures suffer cyber-attacks, the healthcare industry is particular because the damage caused by an attack can have a direct impact on patients' lives.

To assess the resilience of secure storage support for Telco's infrastructure, the network infrastructure in Figure 44 is designed, including Cloud Storage in Figure 45.

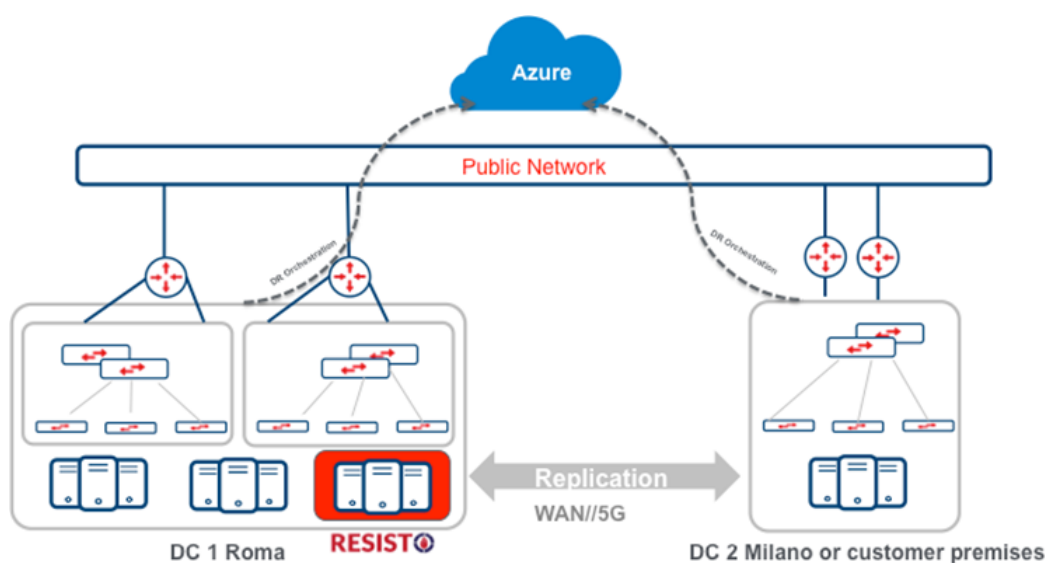


Figure 45 Tim Cloud storage critical infrastructure Healthcare Scenario

Table 40 shows the network elements, organized in core, distribution and access levels.

Table 40 TLC Network Elements for Reference Unified Scenario 5					
TLC Network Elements	Network	Services	Testbed Components		
			Component	Name	Description
CORE network			Nexus 93180 Cisco 9006		
METRO nodes/ POP level 1		Cloud Storage Roma –Milano	Cisco 903		
METRO network					
POP level 2			ASR 920		
Access Network			Alcatel 7750		
Access Node			DSLAM, BTS		
Premises node			Hospital		
End Users			Medical Rooms, Operating Rooms, Medical Devices		

10.2. Threats and Impacts on CISIApro

Table 41 describes cyber and physical threats and shows impacts on CISIApro, taking into consideration Table 14, where state variables are defined.

Table 41 Cyber and Physical security events for the Unified Scenario 5			
Type	Threat	Description	Impacts on CISIApro
Physical	Unauthorized access to physical system	An unauthorized cybercriminal accesses a protected area (Datacenter)	<i>Unauthorized_access</i>
Physical	Power outage		<i>Power_Fault</i>
Physical	Temperature out of range		<i>Temperature_Fault</i>
Cyber	Change of system configuration	A cybercriminal starts a program from a privilege folder or temporary folder of system to change system configuration	<i>Config_Change</i>
Cyber	Tampering of sensitive information	Large amount of data has been extracted from the storage system, that indicates a possible data exfiltration	<i>Data_Corruption</i>
Cyber	Denial of service	DoS attacks are performed by sending huge amount of data toward a specific server, overwhelming its resources till it is not able to provide any services	<i>Service_Fault</i>
Cyber	Malware	Malware is able to infect and consequently block the normal behaviours of electronic medical devices	

10.3. Impacts on the Unified Scenario

According to Use Case 5.1 described in deliverable D2.8, impacts that can be derived for the Unified Scenario 5 are reported in Table 42.

Table 42 Impacts on the Unified Scenario 5	
Type	Description
Technical	Breach of access
Economic	The threats affect the business operation since an incident can generate reputational, financial and stakeholders' impacts.
Societal	Damage to files and personal data

10.4. CISIApro implementation

This paragraph shows the model implemented in CisiaPro and the entities that make up the telecommunication network with the related services provided.

To simulate the events described in the Healthcare Use Case, in addition to the telecommunications network, a hospital ward is designed, which has been described in detail in 5.3.1.

Figure 47 illustrates how the hospital ward was created in CisiaPro.

10.4.1. Description of CisiaPro model

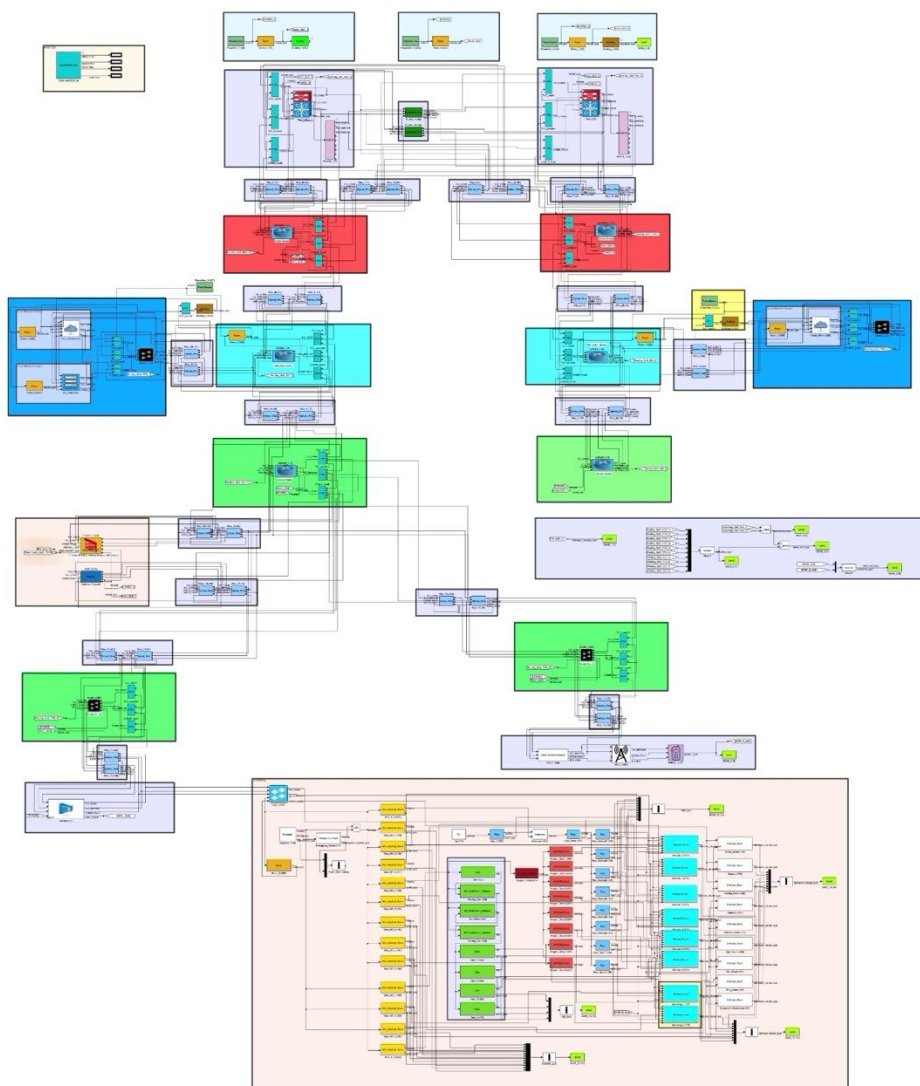


Figure 46 Unified Scenario 5 CisiaPro Model top view

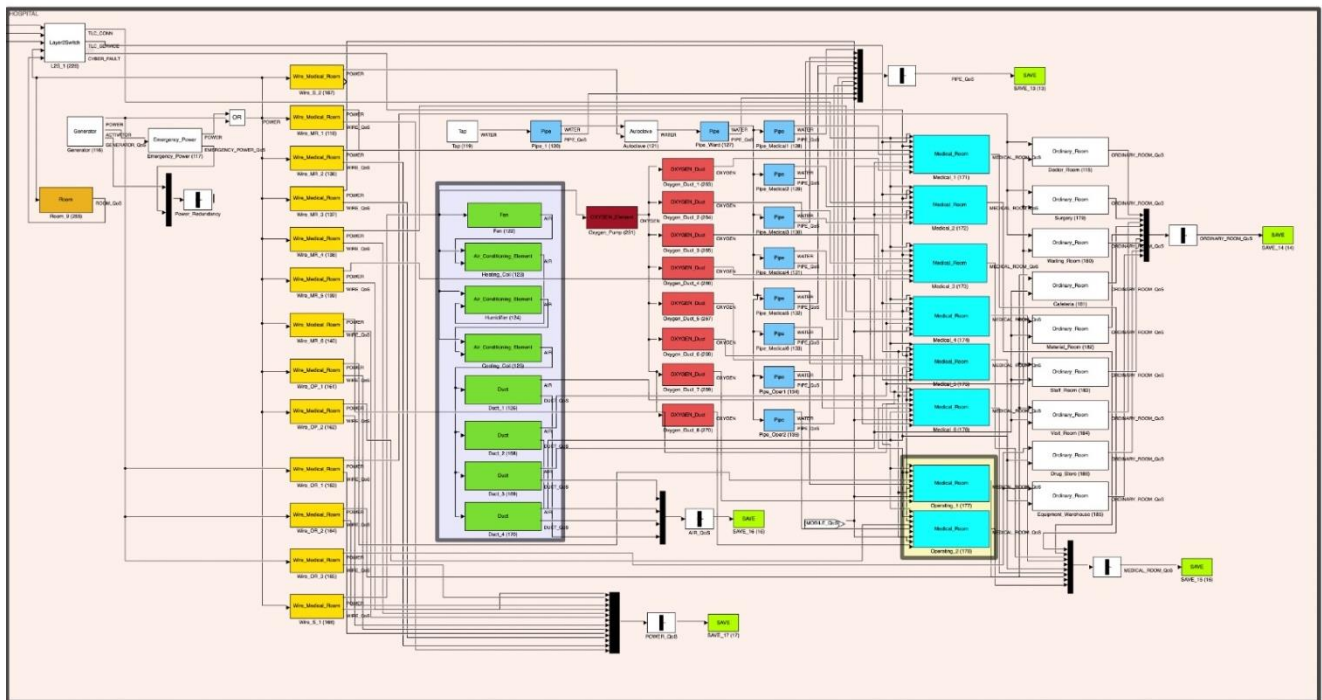


Figure 47 Hospital Ward CISIAPro Model

10.4.2. Model design: entities for Unified Scenario 5

The entities that characterize the model depicted in Figure 46 are listed below:

Entity Name	Entity Type
5G_Core	App_Server
ANT_1	BTS_ANTENNA
ASR9006_1	CISCO_router
ASR9006_2	CISCO_router
ASR903_1	CISCO_router
ASR903_2	CISCO_router
ASR920_1	CISCO_router
ASR920_2	CISCO_router

Alcatel_1	Alcatel7750
Alcatel_2	Alcatel7750
Alcatel_3	Alcatel7750
Alcatel_4	Alcatel7750
Autoclave	Autoclave
BIGP_2	F5BIGP
BTS_1	BaseTransceiverStation
Building_1	Building
Building_1	Building
Building_3	Building
Building_5	Building
Cafeteria	Ordinary_Room
Cloud_Milano	CloudServer
Cloud_Roma	CloudServer
Cooling_Coil	Air_Conditioning_Element
Doctor_Room	Ordinary_Room
Drug_Store	Ordinary_Room
Duct_1	Duct
Duct_2	Duct
Duct_3	Duct
Duct_4	Duct
Emergency_Power	Emergency_Power
Equipment_Warehouse	Ordinary_Room
FG1500_2	FortiGate1500D
Fan	Fan
Generator	Generator
Heating_Coil	Air_Conditioning_Element
Humidifier	Air_Conditioning_Element
L2S_1	Layer2Switch

MA5603	DSLAM
Material_Room	Ordinary_Room
Medical_1	Medical_Room
Medical_2	Medical_Room
Medical_3	Medical_Room
Medical_4	Medical_Room
Medical_5	Medical_Room
Medical_6	Medical_Room
Mobile_1	MobileUnit
Nex_1	Nexus93180Switch
Nex_2	Nexus93180Switch
Operating_1	Medical_Room
Operating_2	Medical_Room
Oxygen_Duct_1	OXYGEN_Duct
Oxygen_Duct_2	OXYGEN_Duct
Oxygen_Duct_3	OXYGEN_Duct
Oxygen_Duct_4	OXYGEN_Duct
Oxygen_Duct_5	OXYGEN_Duct
Oxygen_Duct_6	OXYGEN_Duct
Oxygen_Duct_7	OXYGEN_Duct
Oxygen_Duct_8	OXYGEN_Duct
Oxygen_Pump	OXYGEN_Element
Pipe_1	Pipe
Pipe_Medical1	Pipe
Pipe_Medical2	Pipe
Pipe_Medical3	Pipe
Pipe_Medical4	Pipe
Pipe_Medical5	Pipe
Pipe_Medical6	Pipe

Pipe_Oper1	Pipe
Pipe_Oper2	Pipe
Pipe_Ward	Pipe
PowerGen_1	PowerSource
PowerGen_2	PowerSource
PowerGen_3	PowerSource
PowerGen_5	PowerSource
PowerGen_6	PowerSource
ROUTE_1	ROUTE
ROUTE_2	ROUTE
R_Wire_1	Redundant_Wire
R_Wire_1b	Redundant_Wire
Room_1	Room
Room_2	Room
Room_3	Room
Room_4	Room
Room_5	Room
Room_6	Room
Room_7	Room
Room_8	Room
Room_9	Room
Staff_Room	Ordinary_Room
Surgery	Ordinary_Room
Tap	Tap
Visit_Room	Ordinary_Room
Waiting_Room	Ordinary_Room
Wire_1	Optical_Wire
Wire_10	Optical_Wire
Wire_10b	Optical_Wire

Wire_12	Optical_Wire
Wire_12b	Optical_Wire
Wire_14	Optical_Wire
Wire_14b	Optical_Wire
Wire_15	Optical_Wire
Wire_15	Optical_Wire
Wire_15a	Optical_Wire
Wire_15a	Optical_Wire
Wire_16	Optical_Wire
Wire_16a	Optical_Wire
Wire_1b	Optical_Wire
Wire_2	Optical_Wire
Wire_2b	Optical_Wire
Wire_3	Optical_Wire
Wire_3b	Optical_Wire
Wire_4	Optical_Wire
Wire_4b	Optical_Wire
Wire_5	Optical_Wire
Wire_5b	Optical_Wire
Wire_6	Optical_Wire
Wire_6b	Optical_Wire
Wire_7	Optical_Wire
Wire_7	Optical_Wire
Wire_7b	Optical_Wire
Wire_7b	Optical_Wire
Wire_8	Optical_Wire
Wire_8b	Optical_Wire
Wire_9	Optical_Wire
Wire_9b	Optical_Wire

Wire_MR_1	Wire_Medical_Room
Wire_MR_2	Wire_Medical_Room
Wire_MR_3	Wire_Medical_Room
Wire_MR_4	Wire_Medical_Room
Wire_MR_5	Wire_Medical_Room
Wire_MR_6	Wire_Medical_Room
Wire_OP_1	Wire_Medical_Room
Wire_OP_2	Wire_Medical_Room
Wire_OR_1	Wire_Medical_Room
Wire_OR_2	Wire_Medical_Room
Wire_OR_3	Wire_Medical_Room
Wire_S_1	Wire_Medical_Room
Wire_S_2	Wire_Medical_Room

10.4.3. Model design: services associated to entities

The following Table 44 explains the TLC services provided by the entities outlined in the CISIApro model, relating to Unified Scenario 5.

Table 44 Services for Use Case 5.1	
Entity Name	Services
5G_Core	5G_core
BIGP_2	Web Application Firewall
BIGP_2	Enhanced application layer enrichment and protection
Cloud_Milano	Cloud Storage Milano
Cloud_Roma	Cloud Storage Roma
FG1500_2	URL Filtering
FG1500_2	Centralised Antivirus

FG1500_2	IDS and IPS
FG1500_2	DLP
FG1500_2	E-mail filtering
FG1500_2	Layer 4 Firewall

11. USE CASE 5.2: PROTECTION OF CLOUD STORAGE SERVICES – 5G SMART MANUFACTURING (TIM TESTBED)

11.1. Unified Reference Scenario 6

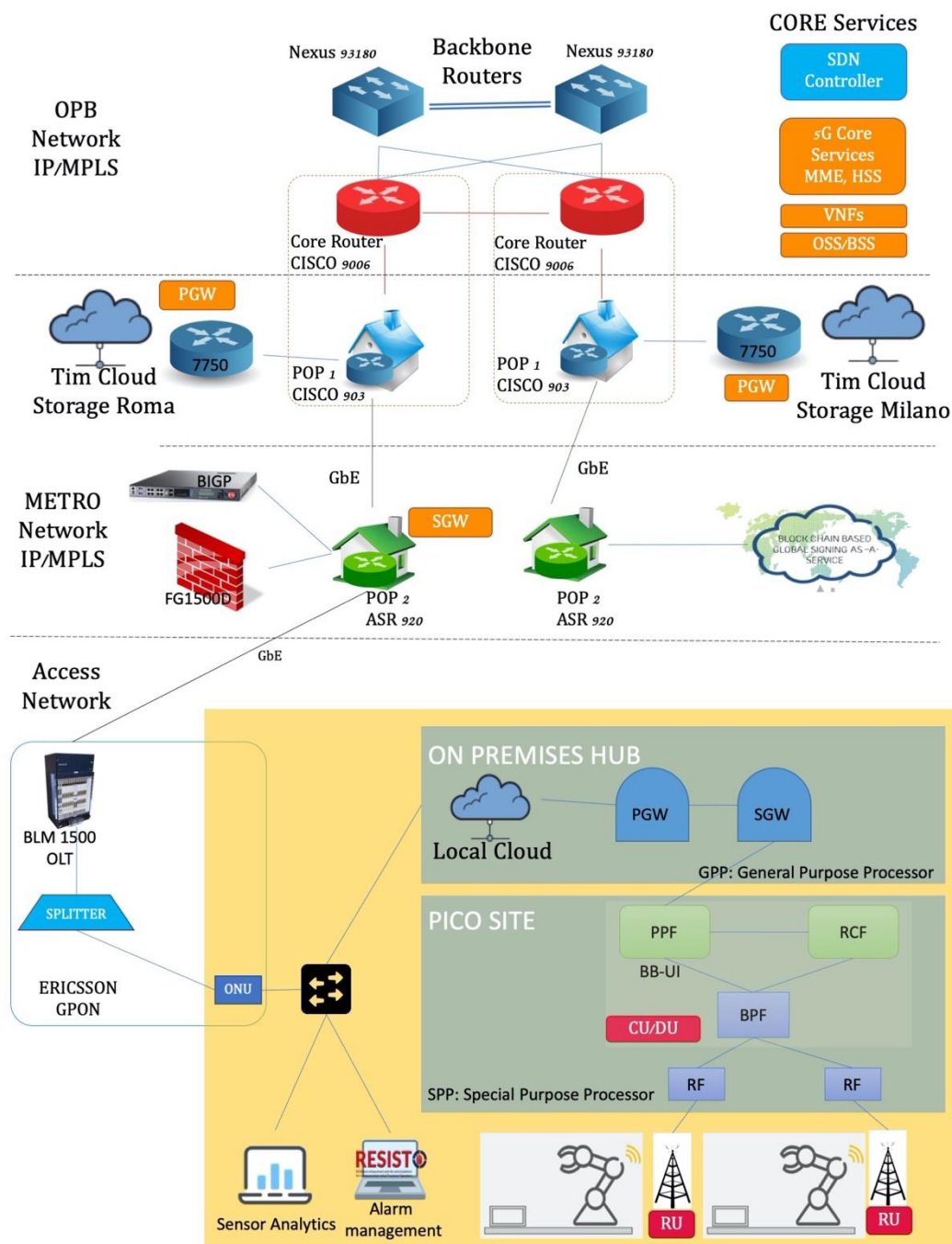


Figure 48 Unified Scenario 6: Use Case 5.2 – TIM Testbed

Smart factories and warehouses bring a new and complex set of requirements: indeed, as the number of remote-control and autonomous robots and automated guided vehicles (AGVs) on the factory floor increase, manufacturers are demanding reliability and predictable latency for quick reaction times. So, connectivity becomes essential of the smart factory.

The 5G network is able to provide the requested wireless connectivity that enables mobility for connected devices, agility in operations and an ever-increasing level of device density. In this case, it is possible to implement the concept of virtual robot control, where various parts of a robot's motion control calculation can be outsourced to a cloud (or edge cloud) system instead of locating them in the robot itself. To this extent the protection against cyber-attacks of the nodes where the control modules are located is of fundamental importance.

The Unified Scenario 6 in Figure 48 is implemented on the basis of TIM's testbed Lab, which is responsible for providing Cloud and Storage for testing services and to detect some threat cyber and physical.

As you can see from the following figure, there is a Block Chain based safety module, capable of monitoring the status of the configuration data or SW.

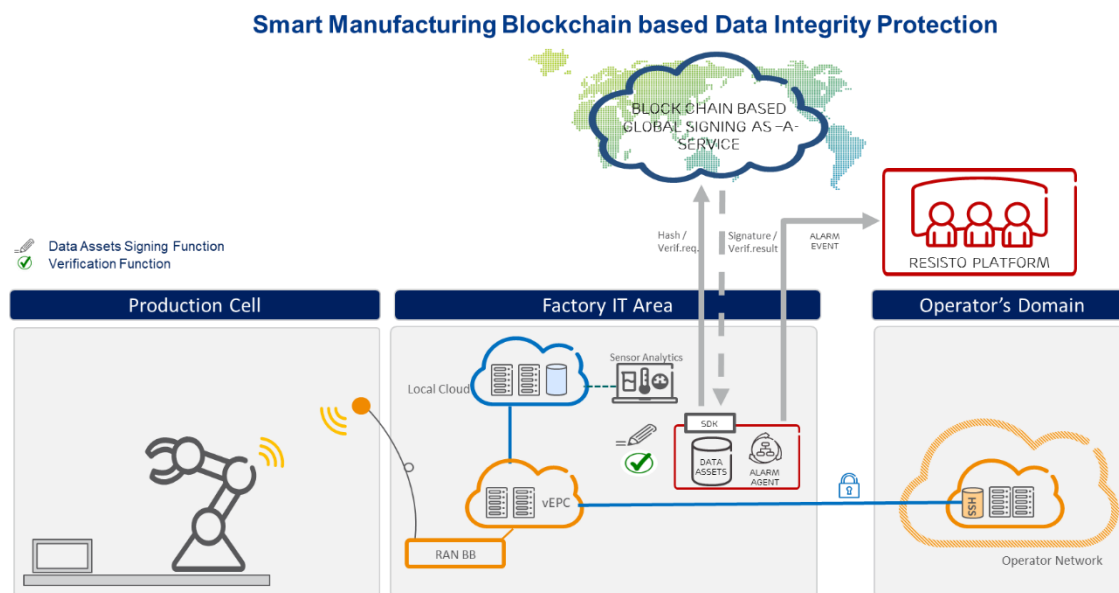


Figure 49 Critical infrastructure Smart Manufacturing Scenario

Network components that make up the TLC architecture in Figure 48 are specified in detail in Table 45.

Table 45 TLC Network Elements for Reference Scenario 6					
TLC Network Elements	Network	Services	Testbed Components		
			Component	Name	Description
CORE network			Nexus 93180 Cisco 9006		
METRO nodes/ POP level 1		Cloud Storage Roma –Milano	Cisco 903		
METRO network		Block Chain based Global Signing AS-A-SERVICE	BIGP FG1500D		
POP level 2			ASR 920		
Access Network			BLM 1500 OLT		
Access Node			SPLITTER		
Premises node			Factory IT Area (local cloud, RAN BB, VEPC, Sensor Analytics, Alarm generator)		
End Users			Robot Control, CNC control, AGV control, IoT sensors control (temperature, light, CO2, humidity)		

11.2. Threats and Impacts on CISI Apro Services

Table 46 describes cyber and physical threats and shows impacts on CISI Apro, taking into consideration Table 14, where state variables are defined.

Table 46 Cyber and Physical security events for the Unified Scenario 6			
Type	Threat	Description	Impacts on CISI Apro
Cyber	Data Tampering attack	An unauthorized person accesses to the end-user local cloud where the robot control SW is stored	SW_Change
Cyber	Man in the middle attack	An unauthorized person accesses to one or more of the nodes of the 5G network used to connect the robots to the remote-control system. If the configuration data of the nodes are modified the link among the remote robots and the control unit can be lost, causing the lock of the factory activities	Config_Change

11.3. Impacts on the Unified Scenario

According to Use Case 5.2 described in deliverable D2.8, impacts that can be derived for the Unified Scenario 6 are reported in Table 47.

Table 47 Impacts on the Unified Scenario 6	
Type	Description
Technical	Breach of access
Economic	The threats affect the business operation since an incident can generate reputational, financial and stakeholders' impacts.
Societal	Damage to files and personal data

11.4. CISI Apro implementation

The Unified Scenario 6, created to simulate TIM Sub Use Case 2, is modelled in CISI Apro as shown in Figure 50. This model represents the network infrastructure that provides connectivity to robots, AGVs and IoT sensors control of the Smart Factory.

11.4.1. Description of CISI Apro model

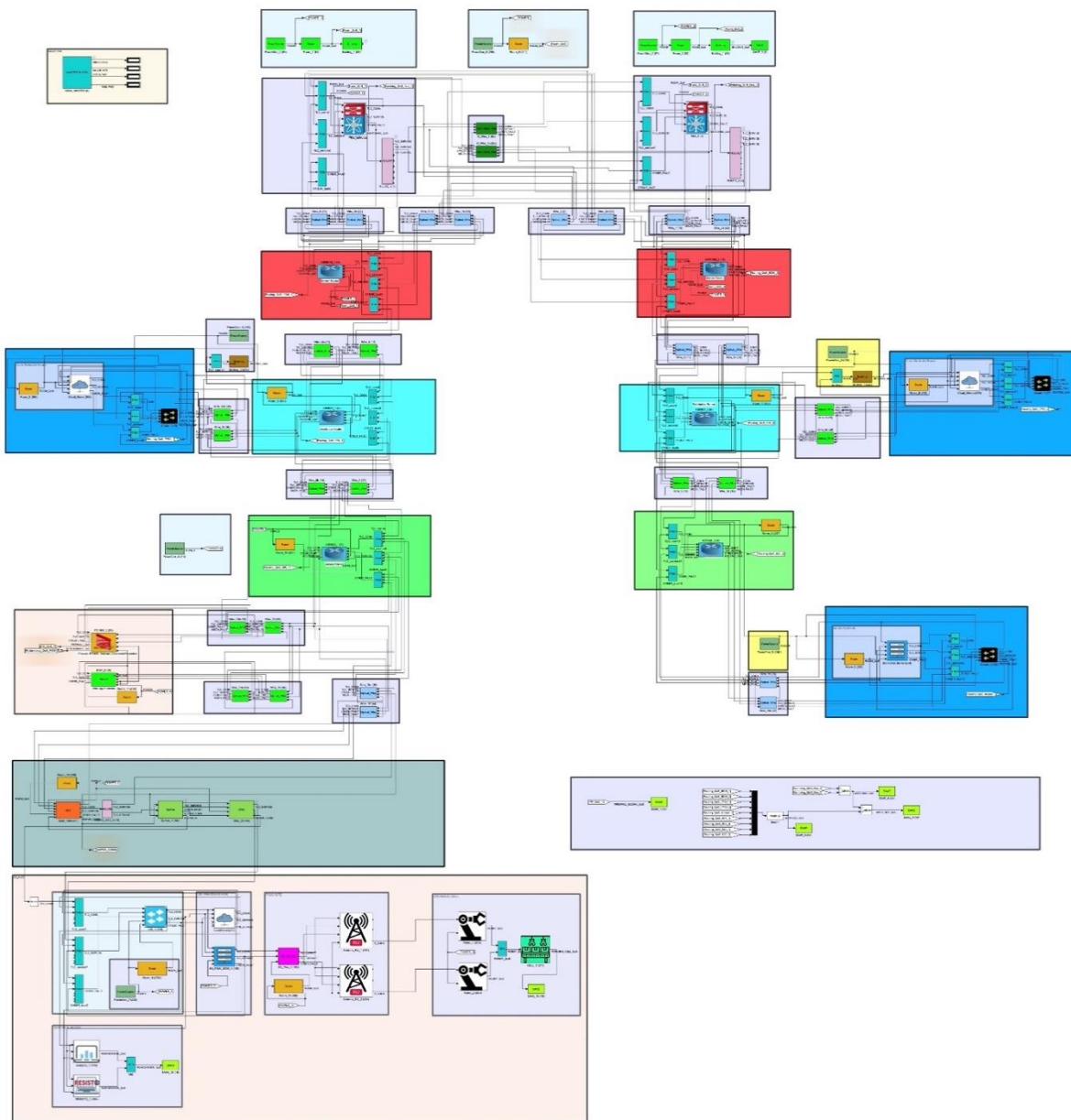


Figure 50 Unified Scenario 6 CISI Apro Model top view

The Smart Factory, described in detail in 5.3.2, is designed in CISApro Model as shown in Figure 51.

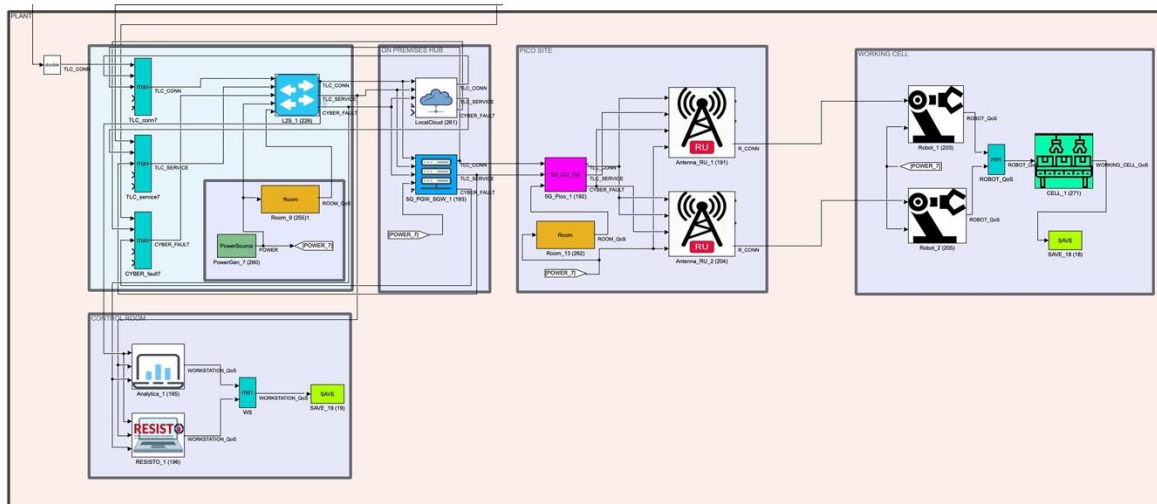


Figure 51 Smart Factory in CISIApro Model

11.4.2. Model design: entities for Unified Scenario 6

All the entities explained in the diagram in Figure 50 are listed in the following table, in which also the type of entity is specified.

Table 48 Entities for Unified Scenario 6

Entity Name	Entity Type
5G_PGW_SGW_1	App_Server
5G_Pico_1	5G_CU_DU
ASR9006_1	CISCO_router
ASR9006_2	CISCO_router
ASR903_1	CISCO_router
ASR903_2	CISCO_router
ASR920_1	CISCO_router
ASR920_2	CISCO_router
Alcatel_1	Alcatel7750

Alcatel_1	Alcatel7750
Alcatel_2	Alcatel7750
Analytics_1	Analytics_1
Antenna_RU_1	RU_ANTENNA
Antenna_RU_2	RU_ANTENNA
BIGP_2	F5BIGP
BLM_1500	OLT
BlockChainServer	App_Server
Building_1	Building
Building_1	Building
Building_3	Building
Building_5	Building
CELL_1	Working_Cell
Cloud_Milano	CloudServer
Cloud_Roma	CloudServer
FG1500_2	FortiGate1500D
L2S_1	Layer2Switch
LocalCloud	CloudServer
Nex_1	Nexus93180Switch
Nex_2	Nexus93180Switch.
ONU_3	ONU
PowerGen_1	PowerSource
PowerGen_2	PowerSource
PowerGen_3	PowerSource
PowerGen_4	PowerSource
PowerGen_5	PowerSource
PowerGen_5	PowerSource
PowerGen_6	PowerSource
PowerGen_7	PowerSource

RESISTO_1	RESISTO_1
ROUTE_1	ROUTE
ROUTE_2	ROUTE
ROUTE_OTE_9	ROUTE
R_Wire_1	Redundant_Wire
R_Wire_1b	Redundant_Wire
Robot_1	Robot
Robot_2	Robot
Room_1	Room
Room_10	Room
Room_11	Room
Room_12	Room
Room_13	Room
Room_2	Room
Room_3	Room
Room_4	Room
Room_5	Room
Room_6	Room
Room_7	Room
Room_8	Room
Room_9	Room
Room_9	Room
Splitter_1	Splitter
Wire_1	Optical_Wire
Wire_10	Optical_Wire
Wire_10b	Optical_Wire
Wire_11	Optical_Wire
Wire_11b	Optical_Wire
Wire_12	Optical_Wire

Wire_12b	Optical_Wire
Wire_14	Optical_Wire
Wire_14b	Optical_Wire
Wire_15	Optical_Wire
Wire_15a	Optical_Wire
Wire_1b	Optical_Wire
Wire_2	Optical_Wire
Wire_2b	Optical_Wire
Wire_3	Optical_Wire
Wire_3b	Optical_Wire
Wire_4	Optical_Wire
Wire_4b	Optical_Wire
Wire_5	Optical_Wire
Wire_5b	Optical_Wire
Wire_6	Optical_Wire
Wire_6b	Optical_Wire
Wire_7	Optical_Wire
Wire_7b	Optical_Wire
Wire_8	Optical_Wire
Wire_8b	Optical_Wire
Wire_9	Optical_Wire
Wire_9b	Optical_Wire

11.4.3. Model design: services associated to entities

The following Table 29 shows the TLC services provided by the entities outlined in the CISIApro model, relating to Unified Scenario 6.

Table 49 Services for Use Case 5.2	
Entity Name	Services
5G_PGW_SGW_1	5G_core
5G_Pico_1	CU-DU
BIGP_2	Web Application Firewall
BIGP_2	Enhanced application layer enrichment and protection
BlockChainServer	Blockchain
Cloud_Milano	Cloud Storage Milano
Cloud_Roma	Cloud Storage Roma
FG1500_2	URL Filtering
FG1500_2	Centralised Antivirus
FG1500_2	IDS and IPS
FG1500_2	DLP
FG1500_2	E-mail filtering
FG1500_2	Layer 4 Firewall
LocalCloud	Cloud Storage

12. USE CASE 7: MARITIME SAFETY AND EMERGENCY CASE (RTV TESTBED)

12.1. Unified Reference Scenario 7

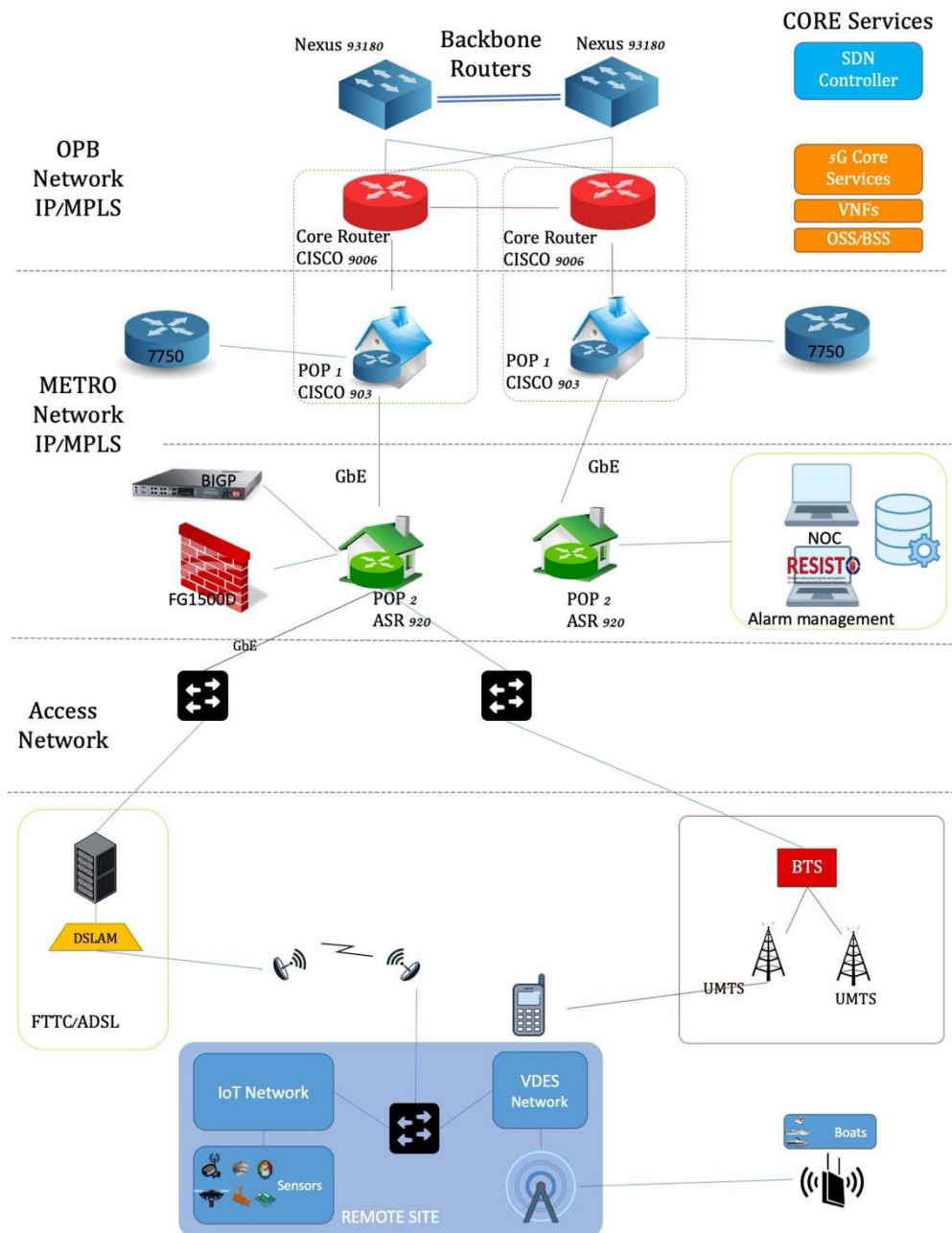


Figure 52 Unified Scenario 7: Use Case 7 – RTV Testbed

The Unified Scenario 7 in Figure 52 is used to simulate Use Case 7, whose goal is to analyze and protect maritime and emergency communications from cyber and physical threats.

To model Maritime Scenario, described in detail in paragraph 5.3.4, refer to the following Figure 53.

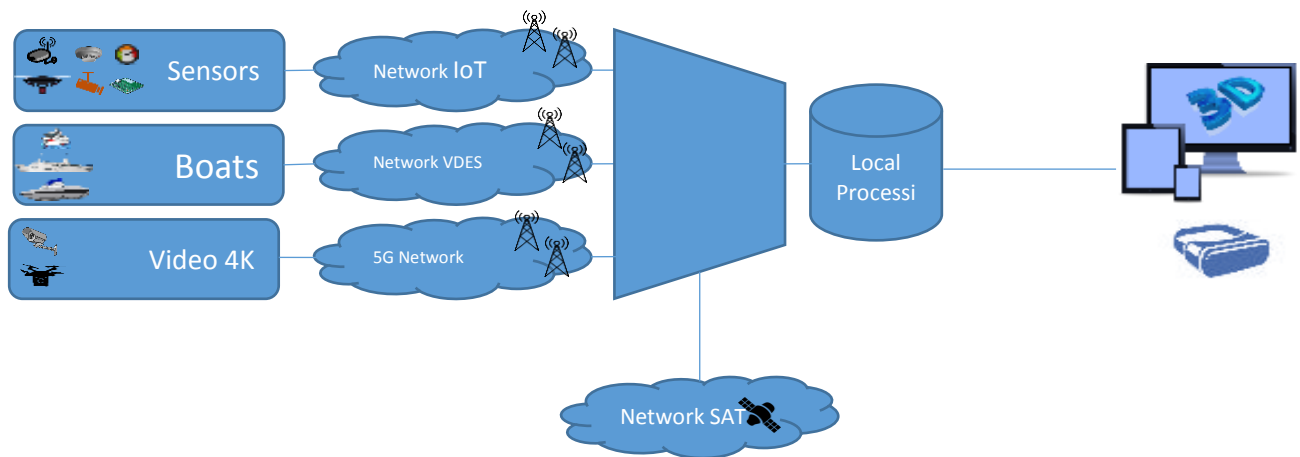


Figure 53 Topology of Emergency service provision

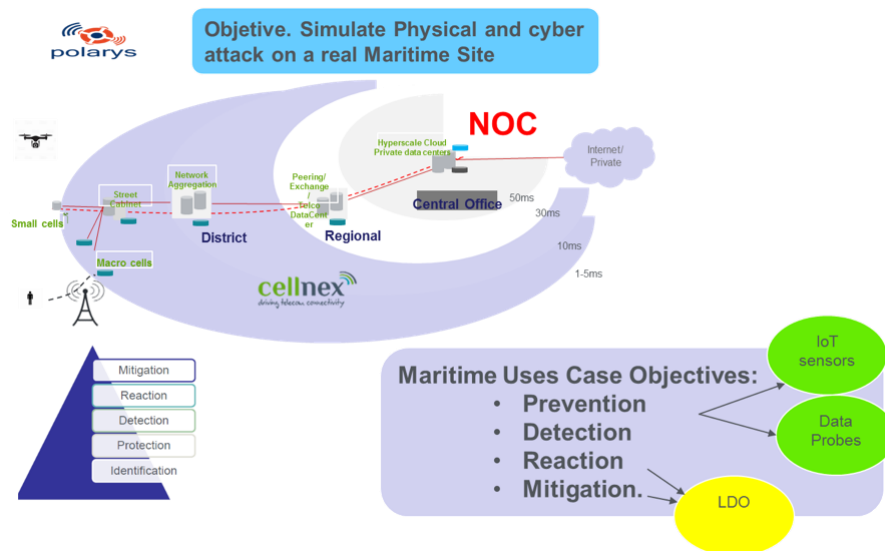


Figure 54: Use case 7 Topology of Maritime Use Cases

The telecommunications network elements that characterize the Unified Scenario 7 in Figure 52 are organized in the following table according to the level they define.

Table 50 TLC Network Elements for Reference Scenario 7					
TLC Network Elements	Network	Services	Testbed Components		
			Component	Name	Description
CORE network			Nexus 93180 Cisco 9006		
METRO nodes/ POP level 1			Cisco 903		
METRO network	MPLS		BIGP FG1500D		
POP level 2			ASR 920		
Access Network	Passive Optical Network		OLT		
Access Node			DSLAM, BTS		
Premises node		RU	ONU, Antenna		
End Users			Port Authority		

12.2. Threats and Impacts on CISI Apro

Table 51 Cyber and Physical security events for the Unified Scenario 7			
Type	Threat	Description	Impacts on CISI Apro
Physical	Unauthorized access	An unauthorized person gains entry into a protected building	Unauthorized_access
Cyber		An attack is executed by a third party targeting the provider's network	

12.3. Impact on the Unified Scenario

Table 52 Impact on the Unified Scenario 7	
Type	Description

12.4. CISIApro implementation

Starting from Figure 52, showing the Unified Scenario 7, the telecommunications network is modelled in CISIApro as illustrated in Figure 55. The components illustrated and the services provided by the TLC network are described in detail below.

12.4.1. Description of CISIApro model

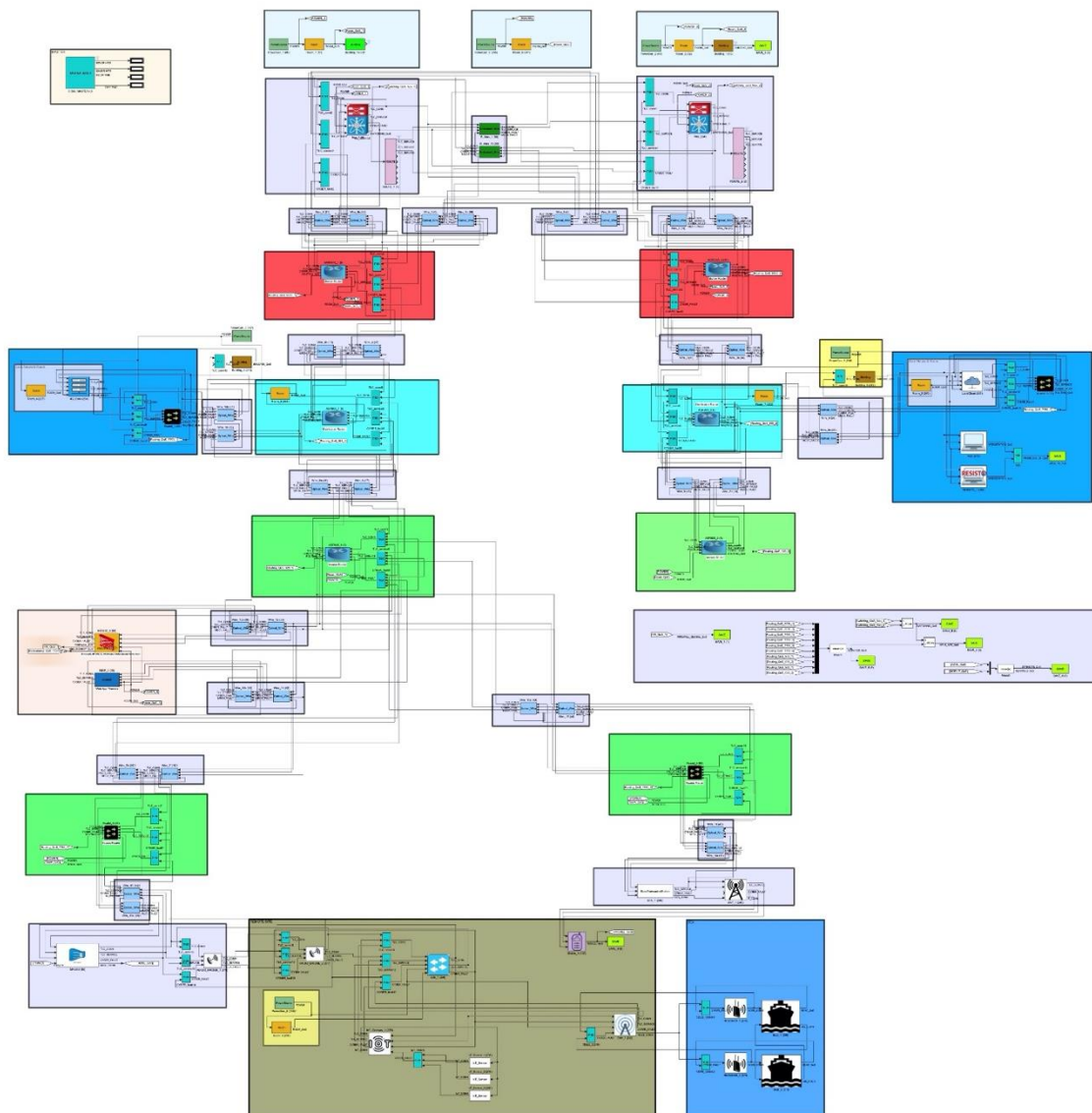


Figure 55 Unified Scenario 7 CISIApro Model top view

To access the protection of critical assets that are located in rural areas where the response time is low due to the distance and some time to the kind of accessibility, in CISIApro the Maritime Environment is designed as shown in Figure 56.

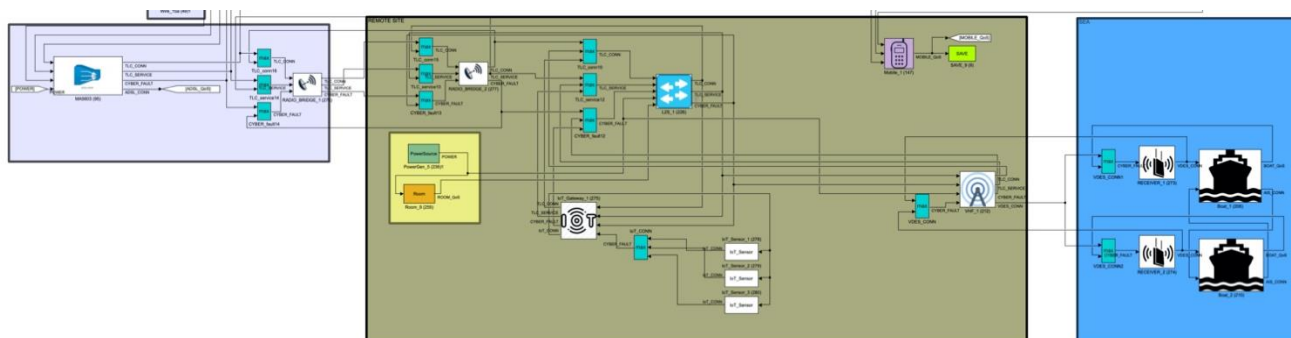


Figure 56 Maritime Environment in CISIApro Model

12.4.2. Model design: entities for Unified Scenario 7

All the components in the infrastructure in Figure 55 that could suffer cyber-physical attacks are listed in the following table.

Table 53 Entities for Unified Scenario 7	
Entity Name	Entity Type
4G_Core	App_Server
ANT_1	BTS_ANTENNA
ASR9006_1	CISCO_router
ASR9006_2	CISCO_router
ASR903_1	CISCO_router
ASR903_2	CISCO_router
ASR920_1	CISCO_router
ASR920_2	CISCO_router
Alcatel_1	Alcatel7750
Alcatel_2	Alcatel7750

Alcatel_3	Alcatel7750
Alcatel_4	Alcatel7750
BIGP_2	F5BIGP
BTS_1	BaseTransceiverStation
Boat_1	Boat
Boat_2	Boat
Building_1	Building
Building_1	Building
Building_3	Building
Building_5	Building
FG1500_2	FortiGate1500D
IoT_Gateway_1	IoT_Gateway
IoT_Sensor_1	IoT_Sensor
IoT_Sensor_2	IoT_Sensor
IoT_Sensor_3	IoT_Sensor
L2S_1	Layer2Switch
LocalCloud	CloudServer
MA5603	DSLAM
Mobile_1	MobileUnit
NOC	Workstation
Nex_1	Nexus93180Switch
Nex_2	Nexus93180Switch
PowerGen_1	PowerSource
PowerGen_2	PowerSource
PowerGen_3	PowerSource
PowerGen_5	PowerSource
PowerGen_5	PowerSource
PowerGen_6	PowerSource
RADIO_BRIDGE_1	Radio_Bridge

RADIO_BRIDGE_2	Radio_Bridge
RECEIVER_1	VDES_RECEIVER
RECEIVER_2	VDES_RECEIVER
RESISTO_1	RESISTO_1
ROUTE_1	ROUTE
ROUTE_2	ROUTE
R_Wire_1	Redundant_Wire
R_Wire_1b	Redundant_Wire
Room_1	Room
Room_2	Room
Room_4	Room
Room_5	Room
Room_6	Room
Room_7	Room
Room_8	Room
Room_9	Room
VHF_1	VDES_ANTENNA
Wire_1	Optical_Wire
Wire_10	Optical_Wire
Wire_10b	Optical_Wire
Wire_12	Optical_Wire
Wire_12b	Optical_Wire
Wire_14	Optical_Wire
Wire_14b	Optical_Wire
Wire_15	Optical_Wire
Wire_15	Optical_Wire
Wire_15a	Optical_Wire
Wire_15a	Optical_Wire
Wire_16	Optical_Wire

Wire_16a	Optical_Wire
Wire_1b	Optical_Wire
Wire_2	Optical_Wire
Wire_2b	Optical_Wire
Wire_3	Optical_Wire
Wire_3b	Optical_Wire
Wire_4	Optical_Wire
Wire_4b	Optical_Wire
Wire_5	Optical_Wire
Wire_5b	Optical_Wire
Wire_6	Optical_Wire
Wire_6b	Optical_Wire
Wire_7	Optical_Wire
Wire_7b	Optical_Wire
Wire_7b	Optical_Wire
Wire_8	Optical_Wire
Wire_8b	Optical_Wire
Wire_9	Optical_Wire
Wire_9b	Optical_Wire

12.4.3. Model design: services associated to entities

The following table shows the TLC services provided by the specific entities that make up the network infrastructure for the Unified Scenario 7.

Table 54 Services for Use Case 7	
Entity Name	Services
4G_Core	4G_core
BIGP_2	Web Application Firewall

BIGP_2	Enhanced application layer enrichment and protection
FG1500_2	URL Filtering
FG1500_2	Centralised Antivirus
FG1500_2	IDS and IPS
FG1500_2	DLP
FG1500_2	E-mail filtering
FG1500_2	Layer 4 Firewall
LocalCloud	Cloud Storage

13. SUMMARY AND CONCLUSIONS

The purpose of this document is to describe the models created with CISIApro 2.0 to simulate the different use cases presented in Deliverable 2.8.

Each unified scenario created allows to evaluate the exposure to risks and the impact that possible cyber-physical threats can have on the same systems.

CISIApro 2.0 is in fact an agent-based simulator aiming at assessing the consequences of adverse events in an interdependent scenario. CISIApro 2.0 has two distinct phases: the first is the modelling activities and the second is the real-time simulator that evaluates the consequences of the adverse events connected to heterogeneous data sources. The output of CISIApro 2.0 is exploited in the decision-making process, to improve the operator situation awareness and to make better decisions knowing which are the consequences of actual events.

14. REFERENCES

Apart from the references already denoted within the txt, the following ones were also considered:

ID	REFERENCE
[1]	RESISTO - Grant Agreement. Project Starting Date: May, 1st 2018, Innovation action Number 786409 RESISTO, and following amendments, Ref. Ares(2019)3472075-28/05/2019
[2]	Ph.D. Thesis Cosimo Palazzo 2019 - Modelling Risk in Highly Interdependent Systems
[3]	DHS (Department of Homeland Security), National Infrastructure Protection Plan: 2006, 2006
[4]	Directive, N. I. S. "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union." OJ L 194, no. 19.7 (2016): 2016.
[5]	O'Rourke, Thomas D. "Critical infrastructure, interdependencies, and resilience." BRIDGE-Washington-National Academy of Engineering- 37, no. 1 (2007): 22.
[6]	Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. "Identifying, understanding, and analyzing critical infrastructure interdependencies." IEEE control systems magazine 21, no. 6 (2001): 11-25.
[7]	Bruneau, Michel, and Andrei Reinhorn. "Exploring the concept of seismic resilience for acute care facilities." Earthquake Spectra 23, no. 1 (2007): 41-62.
[8]	Bruneau, Michel, Stephanie E. Chang, Ronald T. Eguchi, George C. Lee, Thomas D. O'Rourke, Andrei M. Reinhorn, Masanobu Shinozuka, Kathleen Tierney, William A. Wallace, and Detlof Von Winterfeldt. "A framework to quantitatively assess and enhance the seismic resilience of communities." Earthquake spectra 19, no. 4 (2003): 733-752.
[9]	Risk Steering Committee. "DHS Risk Lexicon: 2010 Edition (Washington, DC: Department of Homeland Security, September 2010), 26." As of December 29 (2013).
[10]	Petit, F. D. P., G. W. Bassett, R. Black, W. A. Buehring, M. J. Collins, D. C. Dickinson, R. E. Fisher et al. Resilience measurement index: An indicator of critical infrastructure resilience. No. ANL/DIS-13-01. Argonne National Lab.(ANL), Argonne, IL (United States), 2013.
[11]	Haimes, Yacov Y., and Pu Jiang. "Leontief-based model of risk in complex interconnected infrastructures." Journal of Infrastructure systems 7, no. 1 (2001): 1-12.
[12]	Gopalakrishnan, Kasthurirangan, and Srinivas Peeta, eds. Sustainable and resilient critical infrastructure systems: simulation, modeling, and intelligent engineering. Springer Science & Business Media, 2010.

ID	REFERENCE
[13]	Digioia, Giusj, Chiara Foglietta, Stefano Panzieri, and Alessandro Falleni. "Mixed holistic reductionistic approach for impact assessment of cyber-attacks." In 2012 European Intelligence and Security Informatics Conference, pp. 123-130. IEEE, 2012.
[14]	RESISTO Consortium, "D3.1 Risk and resilience management process for cyber-physical threats of telecom CI"
[15]	CISI Apro 2.0, http://cisiapro.dia.uniroma3.it/
[16]	RESISTO Consortium, "D2.4"