

**RESISTO:**

## **D6.3\_HMI DEFINITION AND PLATFORM INTEGRATION**



# RESISTO

## D6.3 – HMI DEFINITION AND PLATFORM INTEGRATION

<b>Document Manager:</b>	Emanuele AONZO	LDO	Editor
--------------------------	----------------	-----	--------

<b>Project Title:</b>	RESilience enhancement and risk control platform for communication infraSTructure Operators
<b>Project Acronym:</b>	RESISTO
<b>Contract Number:</b>	786409
<b>Project Coordinator:</b>	LEONARDO
<b>WP Leader:</b>	LDO

<b>Document ID N°:</b>	ID: RESISTO_D6.3_200603_01	<b>Version:</b>	1.0
<b>Deliverable:</b>	D6.3	<b>Date:</b>	03/06/2020
		<b>Status:</b>	APPROVED

<b>Document classification</b>	<b>Public</b>
--------------------------------	---------------

Approval Status	
<b>Prepared by:</b>	Emanuele AONZO (LDO)
<b>Approved by: (WP Leader)</b>	Alberto NERI (LDO)
<b>Approved by: (Coordinator)</b>	Bruno SACCOMANNO (LDO)
<b>Advisory Board Validation (Advisory Board Coordinator)</b>	N.A.
<b>Security Approval (Security Advisory Board Leader)</b>	Paolo DI MICHELE (LDO)

## CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Emanuele AONZO	LDO	System Engineer
Chiara FOGLIETTA	RM3	Scientific Researcher
Massimo CRETAIO	RM3	Scientific Researcher
Michael SKITSAS	ADI	System Engineer
Jose Manuel SANCHEZ Javier VALERA	INT	System Engineer

## 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	12/03/2020	All	All	Draft ToC
0.2	13/05/2020	All	All	Release for SAB Assessment
1.0	03/06/2020	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 (GE) – 16154 – Italy

Tel.: +39 348 6505565

E-Mail: bruno.saccomanno@leonardocompany.com

## RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

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

## EXECUTIVE SUMMARY

This document describes the RESISTO HMI and the complete integration of the platform. RESISTO HMI is a web based component. It is made up of a base component that performs a series of joint operations and hosts the other specific components of the project and use cases. This HMI is able to display the data relating to the alarm situations managed by the system and to assist the operator in his functions of alarm management and monitoring of the situation in real time. The integration of the RESISTO platform with all its components is also described.

## CONTENTS

<b>ABBREVIATIONS .....</b>	<b>10</b>
<b>1. INTRODUCTION .....</b>	<b>11</b>
1.1. Deliverable Structure.....	11
<b>2. RESISTO HMI .....</b>	<b>12</b>
2.1. Introduction .....	12
2.2. SC2 Web Viewer overview .....	12
2.2.1. Resources.....	16
2.2.2. Layout management .....	22
2.2.3. Visualization workspace.....	23
2.2.4. Alarms Management and workflow .....	27
2.2.4.1. Workflow management.....	29
2.2.4.2. Alarm report .....	30
2.2.4.3. Alarms on GIS.....	31
2.2.4.4. Alarm status and detail .....	34
2.3. HMI components overview.....	40
2.4. RISK Predictor HMI.....	44
2.5. Network Orchestration HMI.....	48
2.5.1. Interaction with ETSI OSM.....	52
2.5.2. Interaction with Sonata Tango 5G .....	56
2.5.3. Interaction with Openstack.....	58
2.6. Audio and Video Detector HMI .....	60
2.7. RADIOFILTER and RANMONITOR HMI .....	61
2.8. HMI Adaptation .....	64
<b>3. PLATFORM INTEGRATION .....</b>	<b>66</b>
3.1. Introduction .....	66
3.2. Environment design .....	66
3.3. Evaluation of computing power.....	68
3.4. Integration work.....	68
<b>4. CONCLUSION .....</b>	<b>70</b>

## List of Figures

Figure 1 – Web Viewer workstation - video management configuration.....	13
Figure 2 – Home Screen .....	14
Figure 3 – Status bar .....	15
Figure 4 – Notification .....	16
Figure 5 – Resource tree .....	17
Figure 6 – Device Navigation Tree .....	17
Figure 7 – Search Options Resources.....	18
Figure 8 – Administration: set “Show on Gis” to true.....	18
Figure 9 – Visualization on GIS map.....	19
Figure 10- Resources: Right Click Selection .....	20
Figure 11 - Resources: Properties .....	20
Figure 12 – WebPages Properties.....	21
Figure 13– Properties for a Web Page Resource.....	21
Figure 14 – Docking a panel.....	22
Figure 15 – Layout Management.....	22
Figure 16– Layout Management.....	23
Figure 17 - Area of management of video streams.....	24
Figure 18 – Toolbar for layout customization .....	24
Figure 19 – Panels .....	24
Figure 20 - Video Layouts Configuration .....	25
Figure 21–Layout modification .....	25
Figure 22 –toggle mark.....	26
Figure 23 – Assign a name to a panel .....	26
Figure 24– Alarm Management .....	27
Figure 25 – Alarm Management: alarm arise .....	28
Figure 26 – Alarm Management: manage an alarm .....	28
Figure 27 – Workflow current Task.....	29
Figure 28 – Workflow task completed .....	29
Figure 29 – Alarm Report .....	30
Figure 30 – Attach a file to a report .....	31
Figure 31–Gis cartography.....	31
Figure 32 - base cartography .....	32
Figure 33 – Details on Alarm .....	32
Figure 34 - Device on map.....	33
Figure 35 – Alarms on the map.....	34
Figure 36 - Device .....	35
Figure 37 – Alarm Details .....	36
Figure 38 – Alarm Toolbar .....	37
Figure 39 – Assign Alarm to another operator.....	37
Figure 40– Synoptic Alarm .....	38
Figure 41 – Synoptic Alarm .....	38
Figure 42 – Synoptic Alarm Filter .....	38
Figure 43 – Details Selected Alarm.....	39
Figure 44 – Alarm Related Events.....	39
Figure 45 – Alarm Related Events for a Tamper Alarm .....	40
Figure 46 – three screen HMI example .....	41
Figure 47 – Detail of Screen 1 .....	42



Figure 48 – Detail of Screen 2 .....	42
Figure 49 – Alarm tray .....	43
Figure 50 – Alternatives for Screen 3 .....	43
Figure 51 – Risk Predictor main dashboard .....	44
Figure 52 – Risk Predictor main dashboard with left sidebar closed .....	45
Figure 53 – Classic map of case study .....	46
Figure 54 – Risk map of case study .....	46
Figure 55 – Building map of case study .....	47
Figure 56 – Risk Predictor page with change in the topology .....	47
Figure 57 – Risk Predictor page with zoom in the map topology .....	48
Figure 58 - RESISTO Network Services Orchestrator overview .....	49
Figure 59 - Orchestrator HMI login .....	50
Figure 60 - Orchestrator Node-red flows .....	50
Figure 61 - Orchestrator HMI main screen .....	51
Figure 62 – Network service defined on OSM .....	51
Figure 63 – Network slice template defined on OSM .....	52
Figure 64 – Orchestrator instantiate network slice .....	52
Figure 65 – Orchestrator verify Network Slice instantiate on Openstack (1) .....	53
Figure 66 – Orchestrator verify Network Slice instantiate on OSM (1) .....	54
Figure 67 – Orchestrator verify Network Slice instantiate on Openstack (2) .....	54
Figure 68 – Orchestrator verify Network Slice instantiate on Openstack (3) .....	55
Figure 69 – Orchestrator verify Network Slice instantiate on OSM (2) .....	55
Figure 70 – Orchestrator verify Network Slice instantiate on Orchestrator HMI .....	56
Figure 71 – Orchestrator Sonata Network Services from Orchestrator HMI .....	56
Figure 72 – Orchestrator Sonata Network Services from Sonata HMI .....	57
Figure 73 – Orchestrator operator Accept/Reject request from NBI .....	57
Figure 74 – Orchestrator response to NBI request .....	58
Figure 75 – Orchestrator tenant Openstack tenant configuration .....	59
Figure 76 – Orchestrator Openstack minimal configuration .....	59
Figure 77 – Annotated detected persons .....	60
Figure 78 – Video stream configuration .....	61
Figure 79 – Map view of camera detections and alerts .....	61
Figure 80 – RADIOFILTER HMI (1) .....	62
Figure 81 – RADIOFILTER HMI (2) .....	62
Figure 82 – RANMONITOR HMI (1) .....	63
Figure 83 – RANMONITOR HMI (2) .....	64
Figure 84 – Template for HMI Adaptation requirements per use case .....	65
Figure 85 – Integration Environment .....	67
Figure 86 – Template for HMI Adaptation requirements per use case .....	68

## ABBREVIATIONS

<b>5G</b>	5th generation mobile wireless standards
<b>API</b>	Application Programming Interface
<b>BI</b>	Business Intelligence
<b>ETSI</b>	European Telecommunications Standards Institute
<b>EWCF</b>	Emergency Warning Communication Function
<b>GIS</b>	Geographic Information System
<b>IaaS</b>	Infrastructure as a Service
<b>HMI</b>	Human Machine Interface
<b>MANO</b>	Management and Orchestration
<b>NBI</b>	North Bound Interface
<b>OSM</b>	Open Source MANO
<b>VIM</b>	Virtualized Infrastructure Manager
<b>VPN</b>	Virtual Private Network
<b>WP</b>	Work Package

## 1. INTRODUCTION

In this document the theme of RESISTO HMI will be treated. HMI is a very important component because it is in direct contact with the human being and represents a significant added value for the operator but at the same time must be usable and immediately understandable, complete in information but immediate and easy to read. This HMI has been designed to be modular and flexible so as to be able to adapt effectively to the different situations to be faced and managed, therefore it presents a common basis for general-purpose functions and specific modules that make it customized for the specific actions to be performed on a system against an attack.

Furthermore, this document also deals with the system integration of RESISTO.

This activity has been tackled with a view to optimizing resources and maximum sharing to guarantee broad access and functionality to the various partners distributed in Europe. A cloud-based infrastructure has been set up to facilitate the activity of all partners from their offices in order to speed up the activities. This platform is also designed to facilitate the subsequent validation phase at least for some of the proposed use cases.

### 1.1. Deliverable Structure

The deliverable D6.3 is the report of the WP6 related to the activities on Human Machine Interface (HMI) definition and platform Integration of RESISTO project.

The deliverable comprises 4 sections:

- *Section 1*: introductory overview;
- *Section 2* presents the RESISTO HMI and all the specific components
- *Section 3* presents the Platform Integration Activity
- *Section 4*: conclusion of the work

## 2. RESISTO HMI

### 2.1. Introduction

This chapter describes the main HMI of RESISTO. The HMI is based on the SC2 web Viewer this component manages the basic functionalities of the platform which are:

- Login and credential management
- User profiling
- Layout management
- multiscreen management
- Alarm management
- Workflow management

From a graphical point of view, the web interface is presented as a cockpit for the management of anomalous situations and a DSS that allows to provide the operator with all the information necessary to manage a specific class of anomalies.

The aim of the solution is the simultaneous and logical display of many useful information for the user and to give him the possibility to correctly manage the entire alarm life cycle in the most immediate way possible. The operator interface has been designed to offer all the features so that they are visible and usable by giving immediate feedback to the user both visual and audible (for example sirens and clearly visible icons) that notify that an event has occurred to be managed with the due timeliness. The possibility of using the multiscreen guarantees the user greater visibility and usability of the graphical interface.

### 2.2. SC2 Web Viewer overview

SC2 application is a security management system that, through the integration of different hardware and software modules, aims to establish a monitoring application effective and complete for the detection of anomalous situations and alarms management; then increases control and improves situation awareness by:

- collecting data from disparate security devices or systems;
- analyzing and correlating data, events and alarms, to identify real situations and their priority;
- presenting relevant situation information in a quick and clear format for an operator;
- Providing Standard Operating Procedures (SOPs) for situation management, a step-by-step guide through instructions based on best practices and policies.

The system has a Client–Server architecture. The Server is made up of the following components:

- A. Server (based on the Mule Enterprise Service Bus): a suite of SW components to centralize the management of configured devices (such as: cameras, video recorders, environmental sensors, access control sensors, intrusion detection system etc.), process received events and generate alarms towards connected Clients;
- B. Database: all configuration data, received data from the field (events) and the alarms generated by the server are historicized on an instance of Mongo DB;
- C. Messaging Middleware: an instance of Apache Active MQ handles, in a secure and reliable way, all messages (events and alarms) between components;

The components listed above can be distributed on different elaboration unit with the possibility to scale from a single server to a large-scale distributed system.

Two Client applications are used for interfacing to the system:

- **Web Viewer** Client (Operator Client) provides to the operators the functionality of monitoring video streams, pointing moving cameras, alarms management,
- **Administration** Client (Administrative Client) allows the configuration of the system in terms of devices, users profiles and capabilities, alarm management rules, displaying and recording of video streams;

This paragraph covers the Web Viewer Client application.

Live Web Viewer SC2 Client is in full web technology. Depending on the security application, the operator station can vary from one monitor configuration to multiple display configurations. A recommended configuration utilizes three monitor to offer the operator a wider effective working area, ideal to take advantage of the resources and functionalities of the application.



Figure 1 – Web Viewer workstation - video management configuration

The Web Viewer software have a main working window, from which the operator can open additional windows to display a larger number of video streams, maps or other useful information of sites under surveillance.

The Web Viewer Client allows the operator to perform the following main actions:

- Alarm Management by workflows
- Diagnostics of the system components, services and sensors;
- Monitoring of real time video streams and manage PTZ cameras
- View and report the occurred alarms

Operator can enter the user name and password in the **User** and **Password** fields, and click on [Confirm] to logon; if the login operation is successful, the user is connected and the home screen appears. This login work as a single sign on mechanism so each RESISTO HMI components hosted into the SC2 Web Viewer client can be accessed with this login operation. Operator can select the language from the list of supported languages to automatically translate all entries of the application interface into the selected language. For RESISTO purpose the language used is English.

After the login procedure the home screen appears similar to the following image:

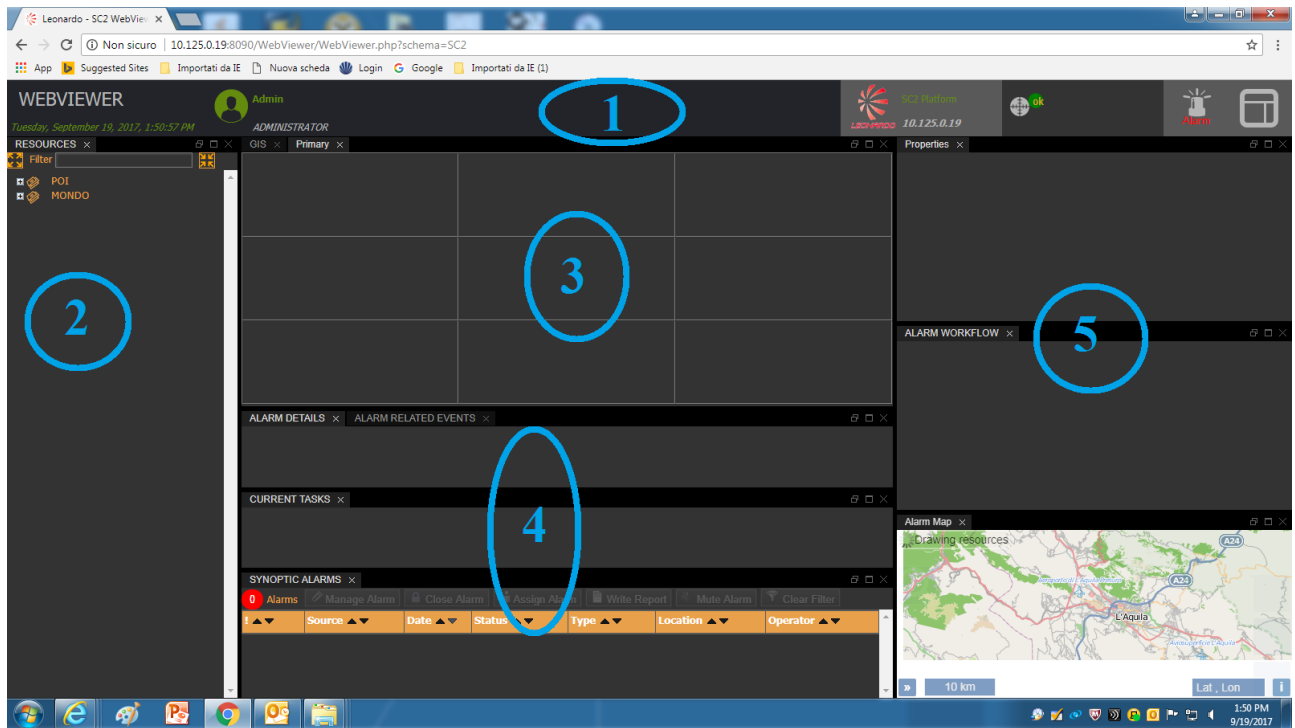


Figure 2 – Home Screen

The window is divided into several functional areas, described in the following paragraphs, corresponding to:

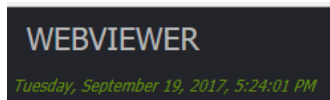
- 1) **User Status Bar**, showing system status, at the top;
- 2) **Configured Devices** navigation tree and contacts;
- 3) **Workspace** for Web application hosting and video streams management (if available), at the center. Web application visualization can be arranged on other monitors in a multi display configuration;
- 4) **Alarm Management** area, at the bottom;
- 5) **Alarm Workflow** area and **process status**.

The user status bar is shown below (**Figure 3**):

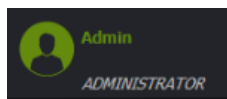




**Figure 3 – Status bar**



- the currently day week, date and time (in green color) and the name of the application (in white color);






- Name of the currently logged user (in green color) and his role (in white color), this icon is a button and by placing the mouse pointer over this icon, the logout button will appear; click the left mouse button to execute the logout operation;



- IP of the connected Server, this icon is a button and by pressing it will appear a window, shown in the following picture, containing the information about the Web Viewer application



- Diagnostic of the Server components shows subsystems status, depending on installed components. In good working systems the subsystem icon appears green otherwise, if at least one component of the subsystem is faulty; the icon becomes red and shows the number of faulty subsystem components. If the icon is absent, the component is not part of the installed system. The mouse positioning on the red icon can be used to show the name of the faulty components of the subsystem:

-  "Communication Service" subsystem status;
-  "System" system core services status;
-  The state of communication with the "GIS Cartographic System".








-  **notification:** indicates with a red dot and a number inside, for example , the number of upload files now available from the notification system because the uploading process has been completed correctly.



Figure 4 – Notification

-  **Security Level**: indicates the security level that has been set for alarm management;
-  Alarm and Layout Management, these icons are two buttons and, by pressing them, perform the following features:

- the **Alarm** button  will display the window which allows to send a geo-referenced manual alarm, will be explained
- **Layout Management** button  will display the window which allows to create, delete, select and manage layouts
- **Components** button  will display the window which allows to restore the current layout.

### 2.2.1. Resources

The Resources section is a Device Navigation Tree which contains the list of configured views. Views are containers used to organize Sites, Cameras and other supported devices and services on the basis of logical criteria such as geographical distribution, functional operation, etc. At each view is associated a Device Navigation Tree. The view is visible to the operator only if its user profile is enabled to access it.



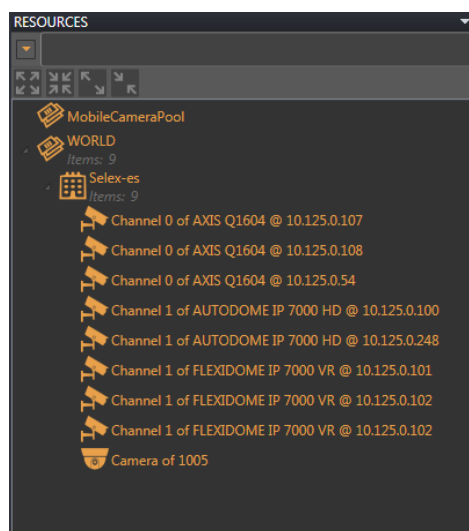


Figure 5 – Resource tree

When a PTZ camera is selected and the PTZ control is enabled will appear the PTZ dashboard under the panel.

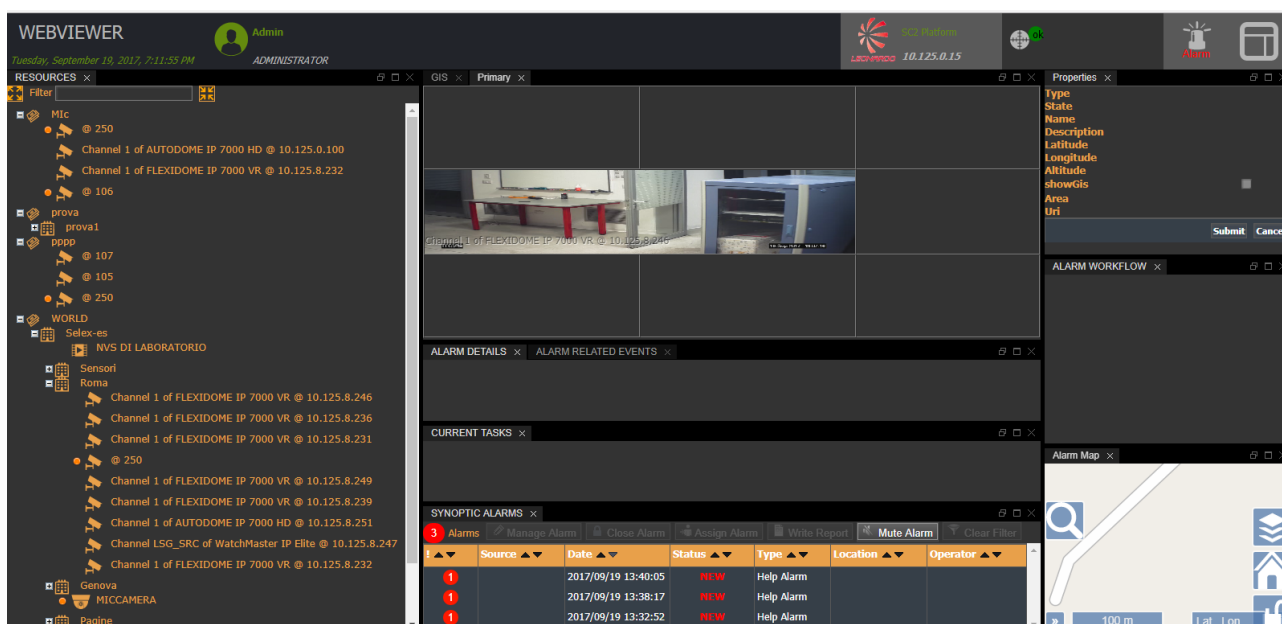


Figure 6 – Device Navigation Tree

On top of the window containing the tree of resources is an editing field to enter the string you want to search among the nodes and leaves of the tree of resources.



**Figure 7 – Search Options Resources**

Under the search field are present the following buttons:

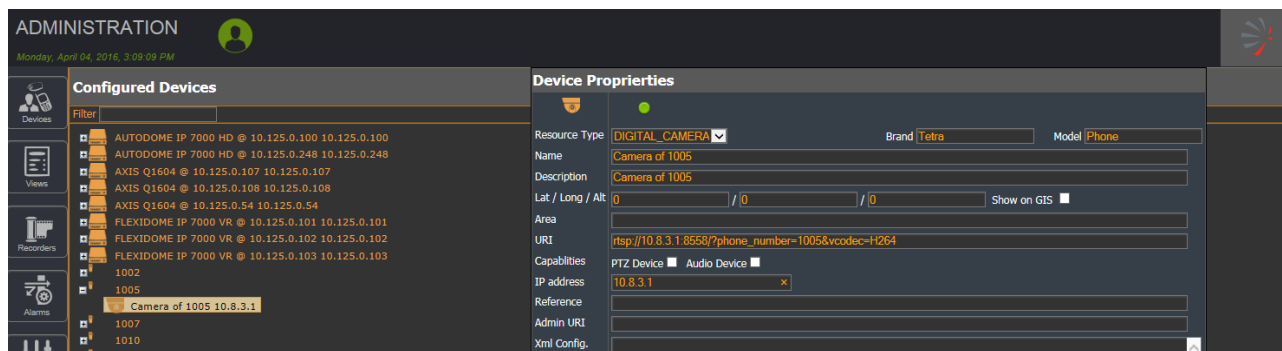


Expands the entire tree of resources,



Collapses the entire tree,

If during configuration of a resource in the Administration Interface, you select the "Show on Gis" option, the configured resource, will be automatically displayed in the map by the Web Viewer in the geographic area in which is located.



**Figure 8 – Administration: set “Show on Gis” to true**

After you configure a resource, the map will contain within a distinct geographic area, the icons that represent a resource or an alert, as shown in the following figure.

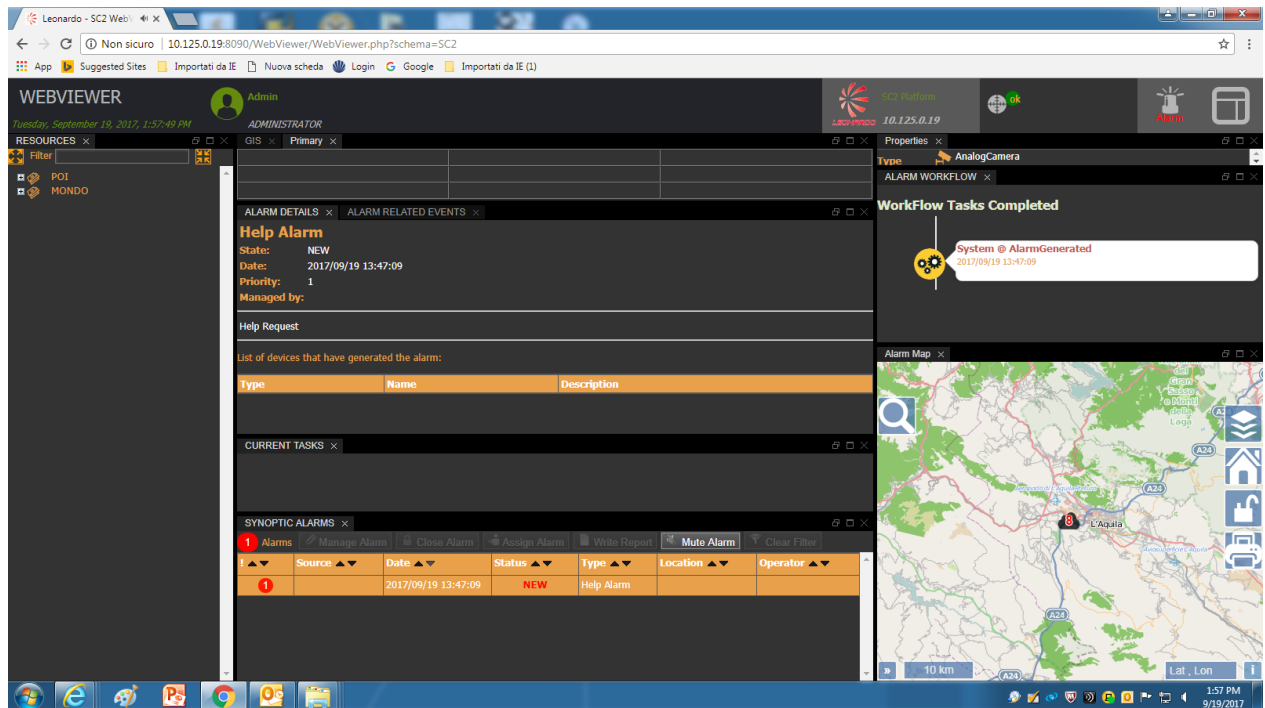


Figure 9 – Visualization on GIS map

The resource tree can contain different types of resources, and each of them provides different types of tools for the operator to perform different types of actions depending on the specificity of the object that is part of the system.

The next few paragraphs will explain in more detail how these graphic interface masks change depending on the type of item that was selected from the resource tree.

**NOTE:** Some resource types can be created and configured through the Web Viewer display interface only if the operator role that has accessed the system has enabled the "CAN\_MANAGE\_DGNA" entry among its functionalities: this enablement can only run through the SC2 Administrator client by accessing, through the "Settings" section, the "Functionality" table.

By selecting a resource from the resource tree with the Right mouse button, depending from the resource type you can have three options:

- Properties
- GoTo by means of this commands the map will show the selected resource
- Layer +/- by means of this commands the layer of the resource is showed or not on the map



Figure 10- Resources: Right Click Selection

"PROPERTIES" panel will show all properties that characterize the selected device.

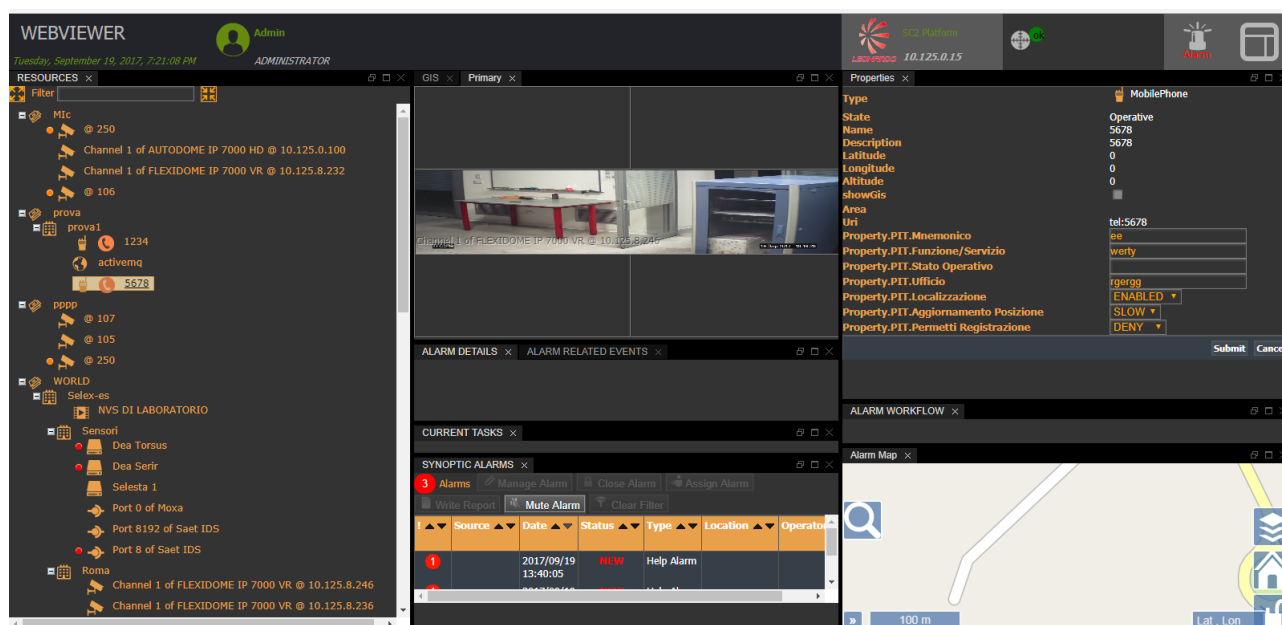
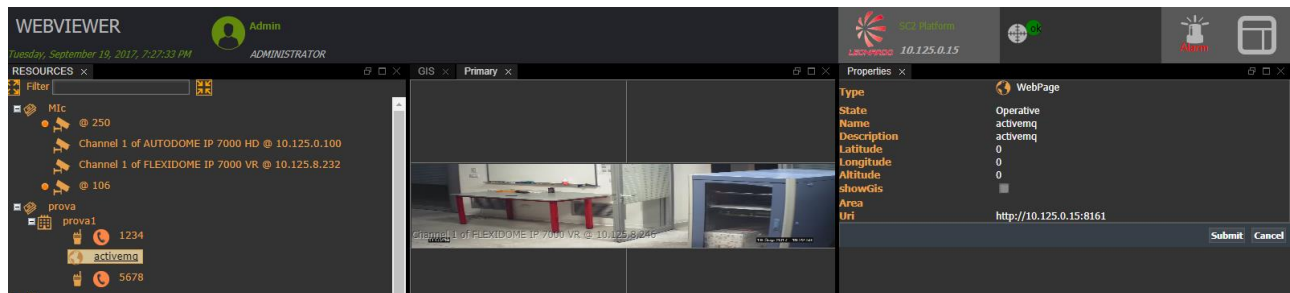



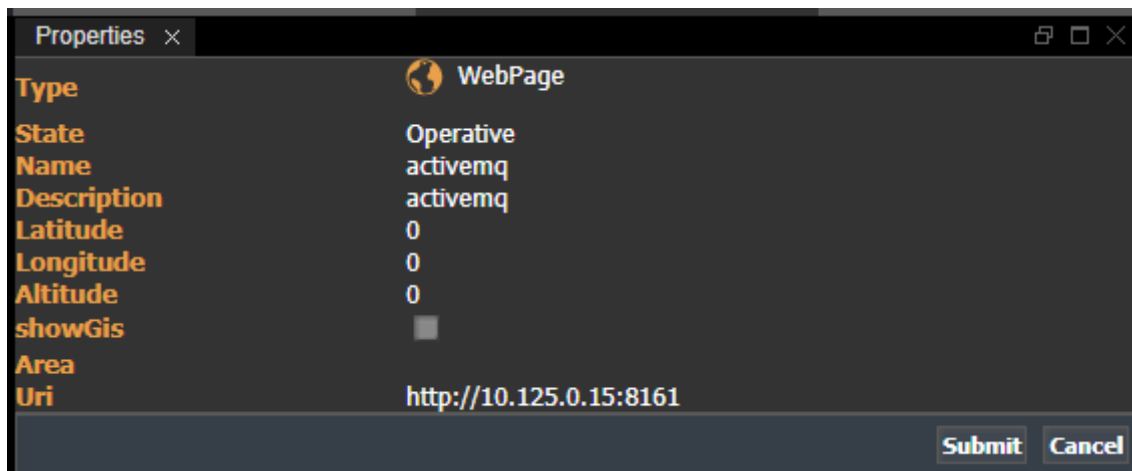
Figure 11 - Resources: Properties

The "**PROPERTIES**" panel lists the properties of the resource and allows you to edit these data simply by editing them if write enabled. Once changed, the system detects a change of value and proposes to the operator to make the change via the [Submit] button which will appear inside the box at the bottom right.



**Figure 12 – WebPages Properties**

Selecting from the resource tree from the "Webpage" node,  the tabs will show as shown in the following figure.



**Figure 13– Properties for a Web Page Resource**

This kind of resource is used by RESISTO to host other web application into the SC2 web Veiewer HMI.

You can move the panels from their default position, simply by selecting it with the mouse and dragging it to appear on the screen like dashed line, shown in the figure below, containing the possible position that can be assigned to the panel you want to move.

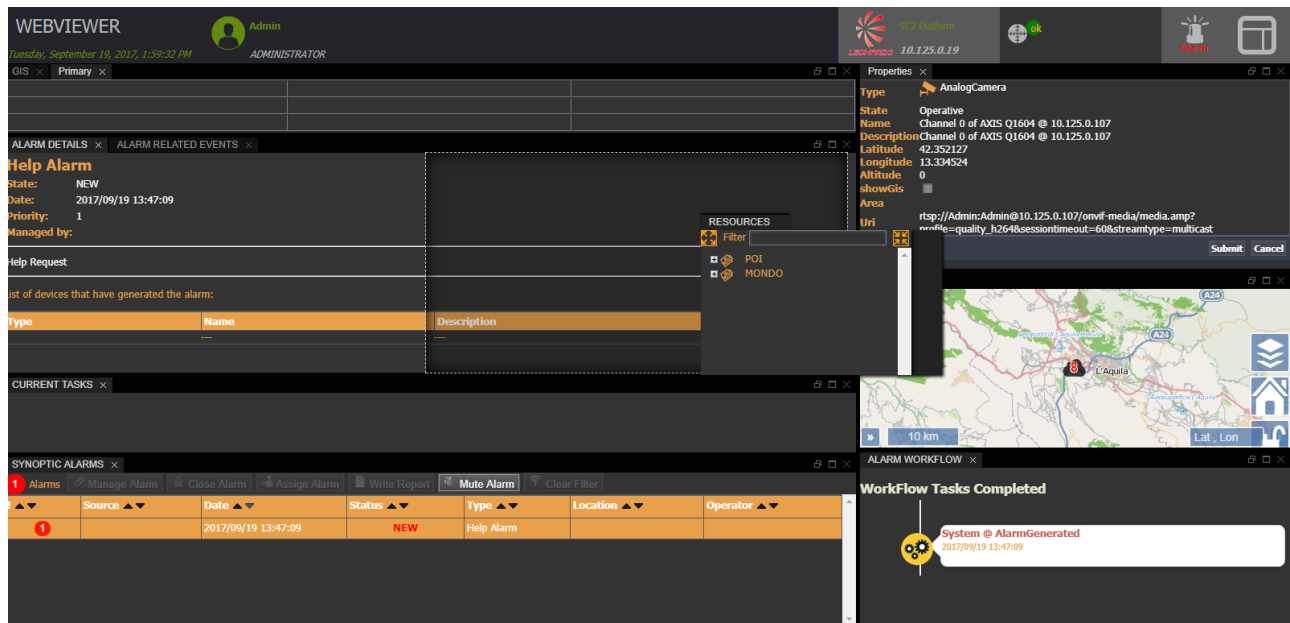


Figure 14 – Docking a panel

To do this you must move the panel with the mouse pointer and point it inside one of the small squares drawn with the dashed line on the interface.

## 2.2.2. Layout management



The **[Layout Management]** button will display the window, shown in the following figure, which allows creating, deleting, selecting and managing layouts.

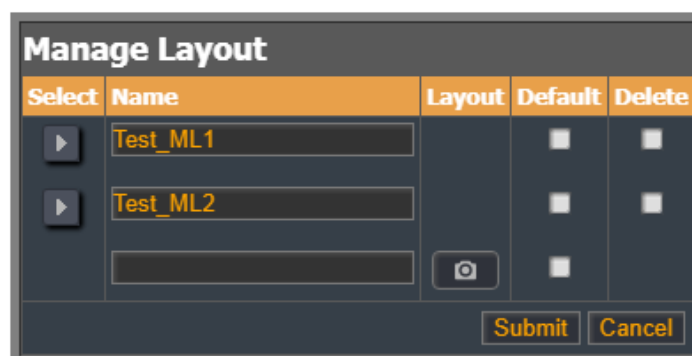




Figure 15 – Layout Management

To create a new layout, move all the different parts of the application's graphical interface as desired and press the button Manage Layout, shown in the previous figure, write the name that you want to assign to that layout within the Name field and then press the button :


the application will take a picture of its current layout and associate it with the specified name; the layout will be immediately memorized. Also the map configuration in terms of layer showed is saved.

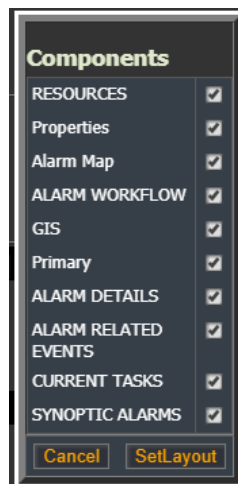
To clear a layout, you need to select it by pressing the corresponding check box on the Delete column and then pressing the Submit button.

To set a layout as Default (it will open automatically to the operator login) you have to select it with the corresponding check box on column Default.



To select a layout and visualize it immediately, you have to press the button : the graphical interface of the application will change immediately.

The save operation is used to associate the current layout with the connected user by setting it as its default template. At the next user access, Web Viewer will load saved settings by submitting to the operator the same interface.

 The [**Components**] button will display the window, shown in the following figure, which allows to managing layouts. The "Components" window is used to restore the presence of the panels that have been incorrectly closed.



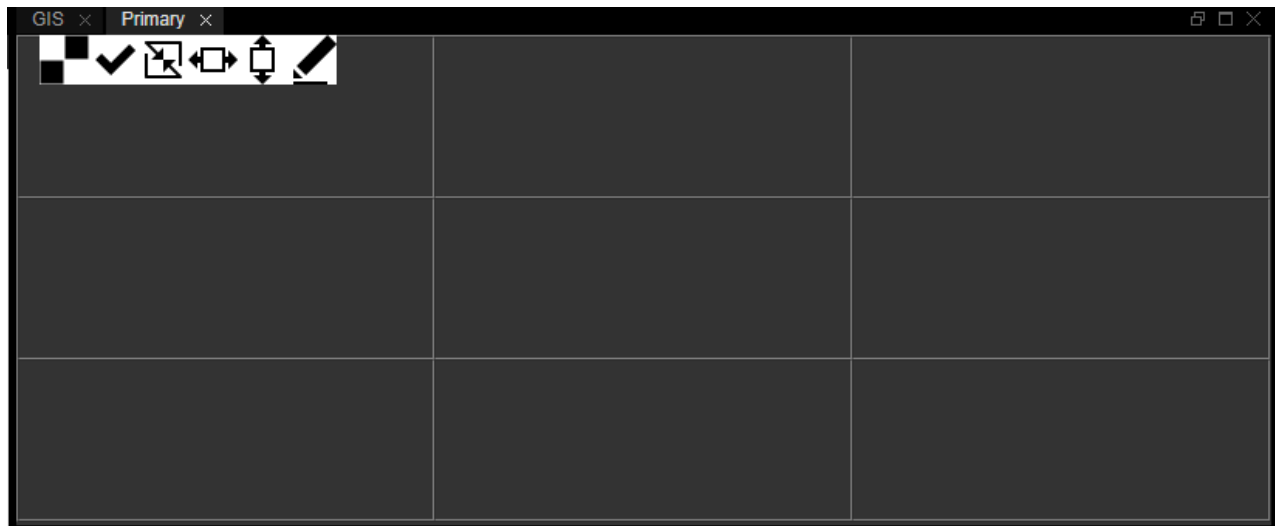
**Figure 16– Layout Management**

After setting the panels to the check box next to each, press the button  to confirm the setting, otherwise leave the choice by pressing the button .

### 2.2.3. Visualization workspace

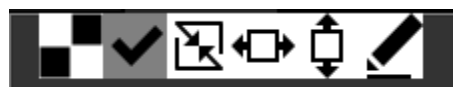
The central visualization area can be organized with tabs, each configurable to show different combinations of cameras, maps and devices allowing users to customize the working area according

to their preferences. In a multi monitor configuration it is possible to use different visualization windows each with different tabs. The active tab name is displayed with a different color. Each panel typically hosts video streams for visualization but can be used to display services associated to other devices (maps service, web pages, etc.).



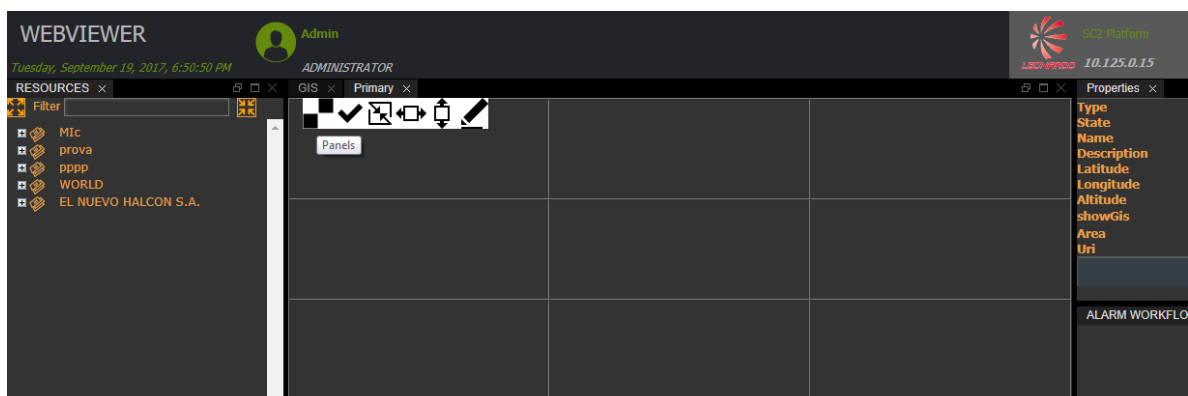
**Figure 17 - Area of management of video streams**

The toolbar at the top left allows you to change the layout of the current tab. It is possible to aggregate or to split a panel:




**Figure 18 – Toolbar for layout customization**

Placing the mouse pointer over the panel matrix header opens a drop-down menu containing a list of preconfigured layouts used to organize the Workspace area. The layout selected with the left mouse button is inserted as a new tab in the current workspace.



**Figure 19 – Panels**



**Matrix** is the whole array of display panels. Press the button **[Panels]**  to open the lists of type of video layouts configuration, as shown in the following picture.

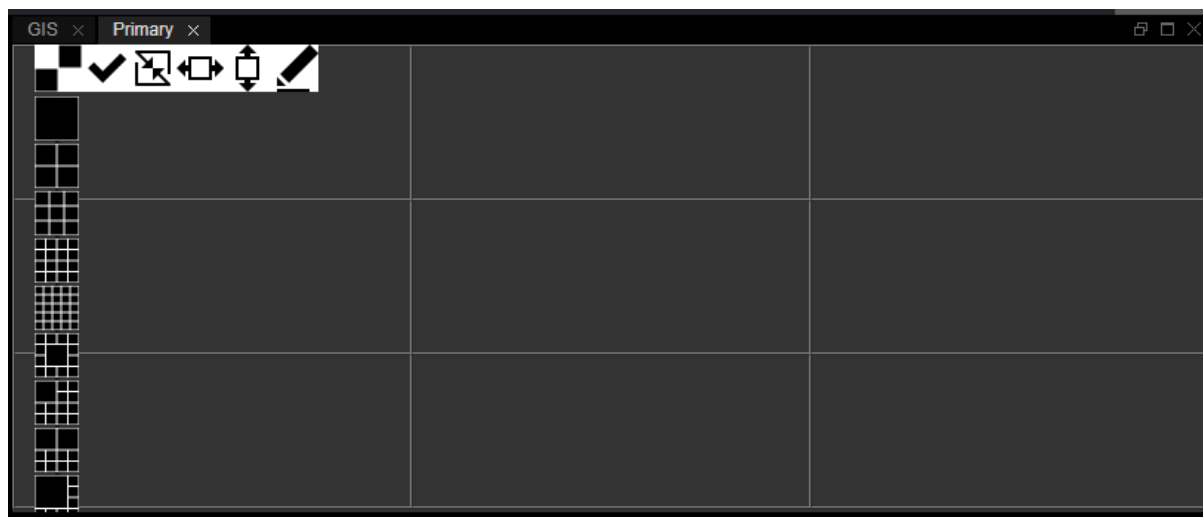


Figure 20 - Video Layouts Configuration

Selecting  (Edit Panel Layout)  activates the arrangements for changing the layout; the area turns gray; selecting a rectangle, it is highlighted in red.

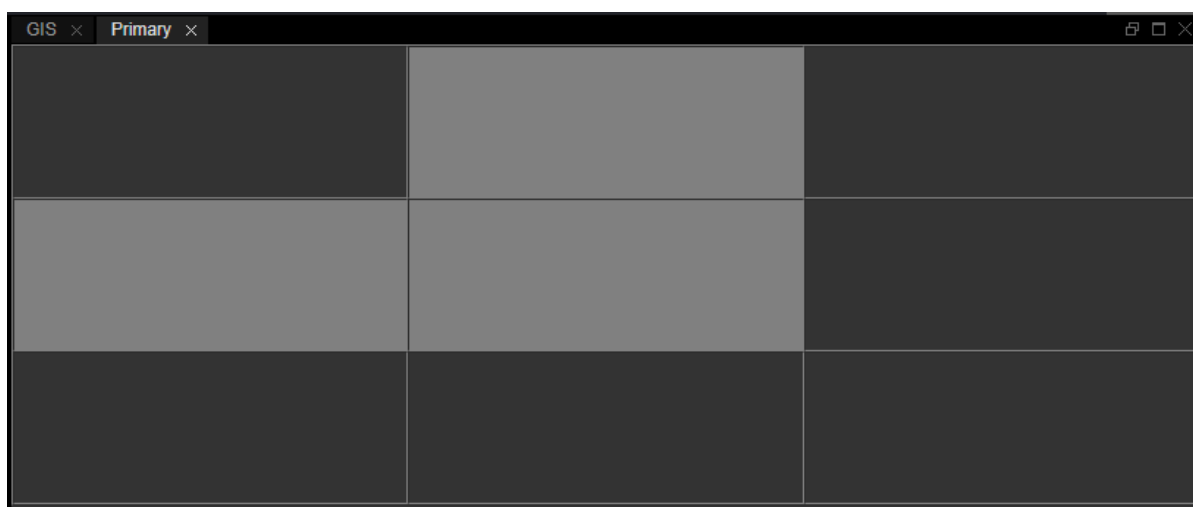



Figure 21–Layout modification

Holding down the mouse left button, it is possible to join the selected rectangle with the adjacent rectangle to create a wider panel. The action is done by pressing the button .

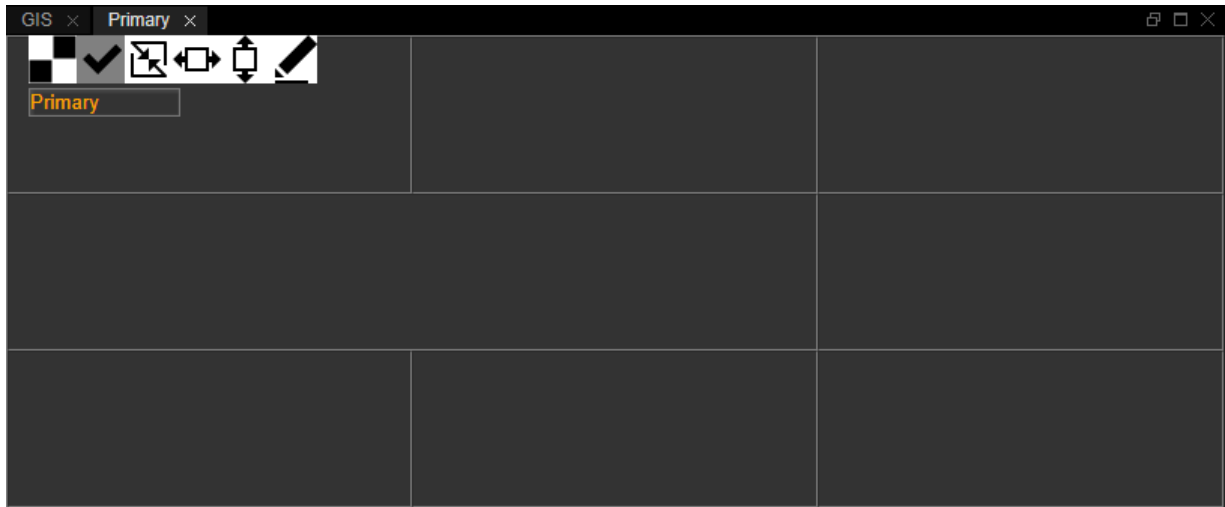



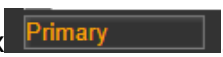


Figure 22 –toggle mark

Similarly, by pressing the button  the selected panel is split horizontal, while pressing the button  the selected panel is split vertical, whenever possible into the composing rectangles.

By pressing the button  it's possible to editing into the box , it is possible to assign a name to the panel.

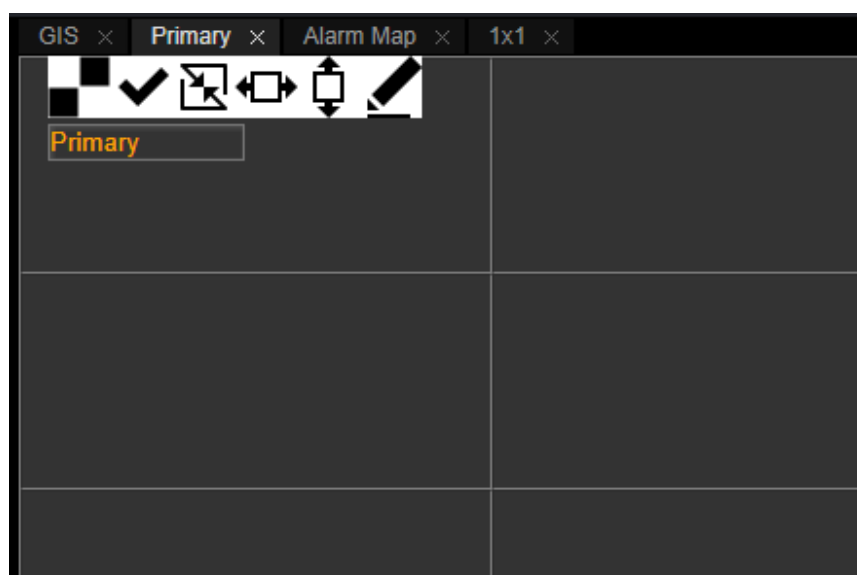
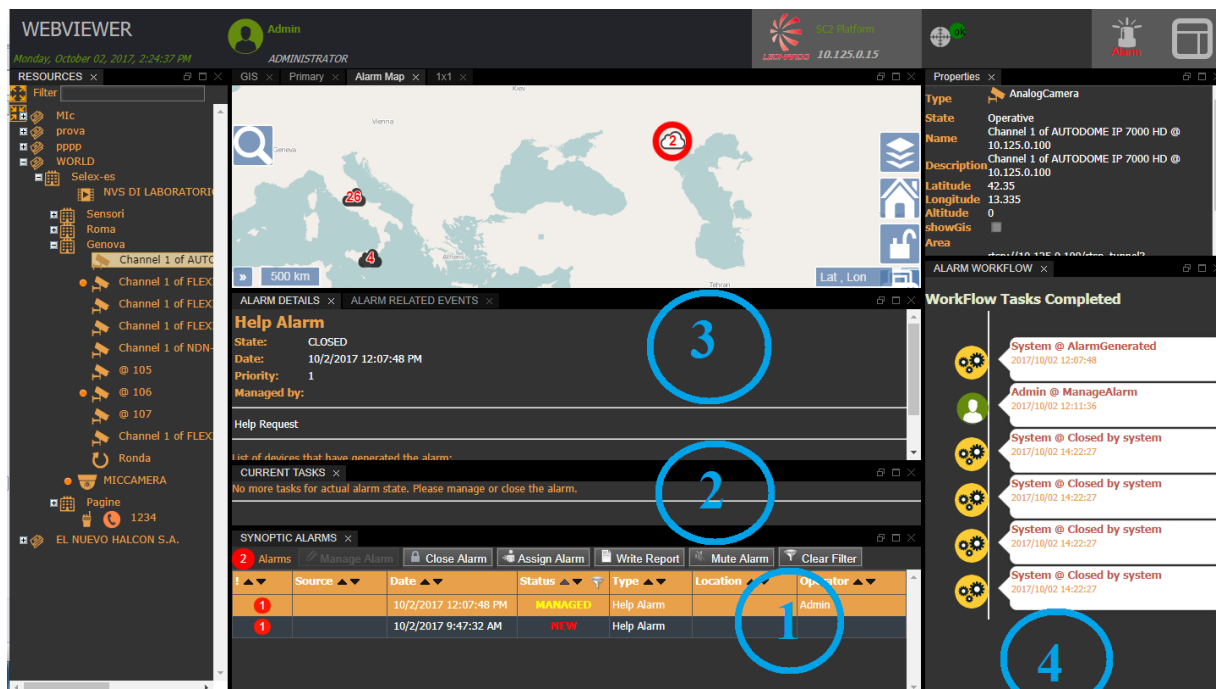


Figure 23 – Assign a name to a panel

## 2.2.4. Alarms Management and workflow

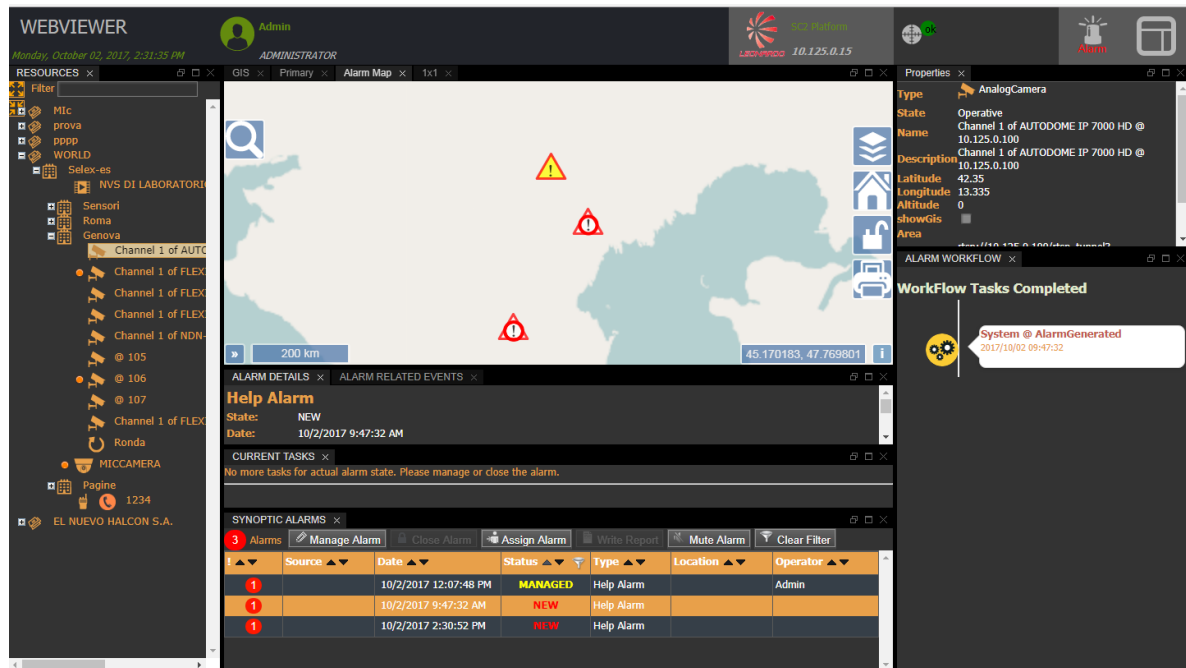
The alarms management area is divided in sections, as shown in the following picture.



**Figure 24– Alarm Management**

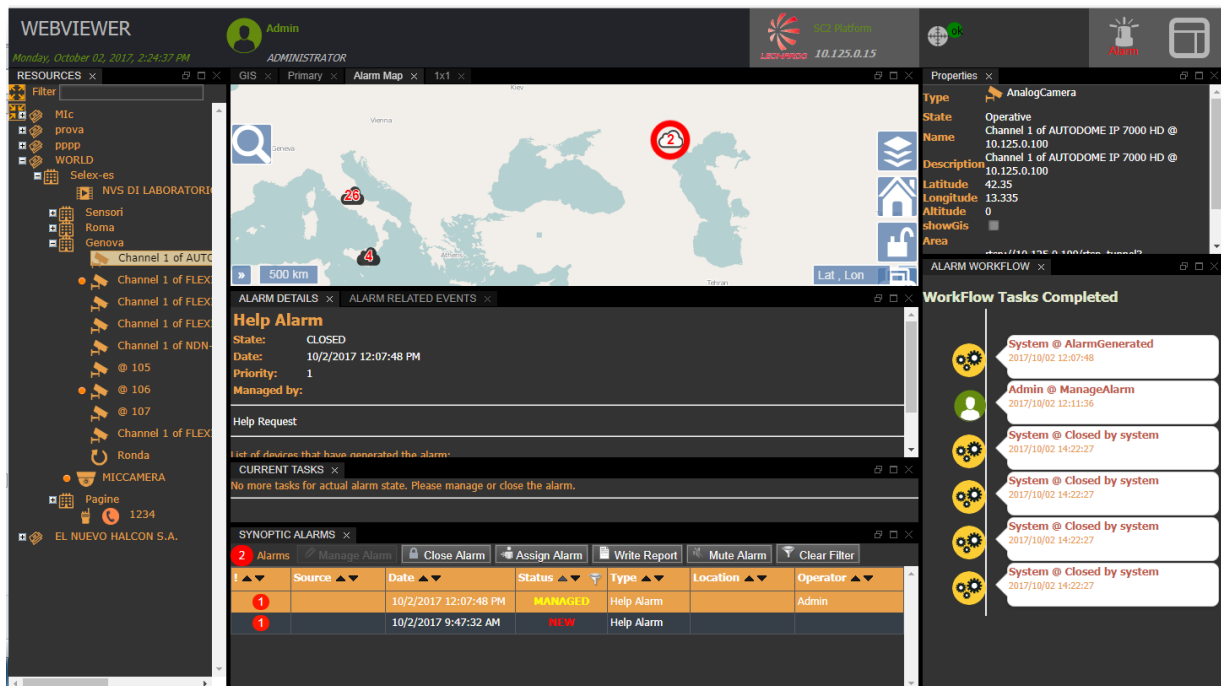
1. synoptic table of alarms
2. current operations on alarms
3. tab to display the details associated with the selected alarm and related events
4. process status and performed operations on alarms

The system signals the occurrence of an alarm by means of an icon on the map, in the moment the alarm arises, and a new line in the "Synoptic Alarms" table is compiled with all the information relating to the alarm, as shown in the following picture.



**Figure 25 – Alarm Management: alarm arise**

When managing an alarm, the interface will populate all the information that the system generates with alarm management, as shown in the following picture.



**Figure 26 – Alarm Management: manage an alarm**

#### 2.2.4.1. Workflow management

In case a workflow is associated to a managed alarm the operator is guided to follow the Operating Standard Procedures defined in the workflow by performing the operations proposed in the "Current Tasks".

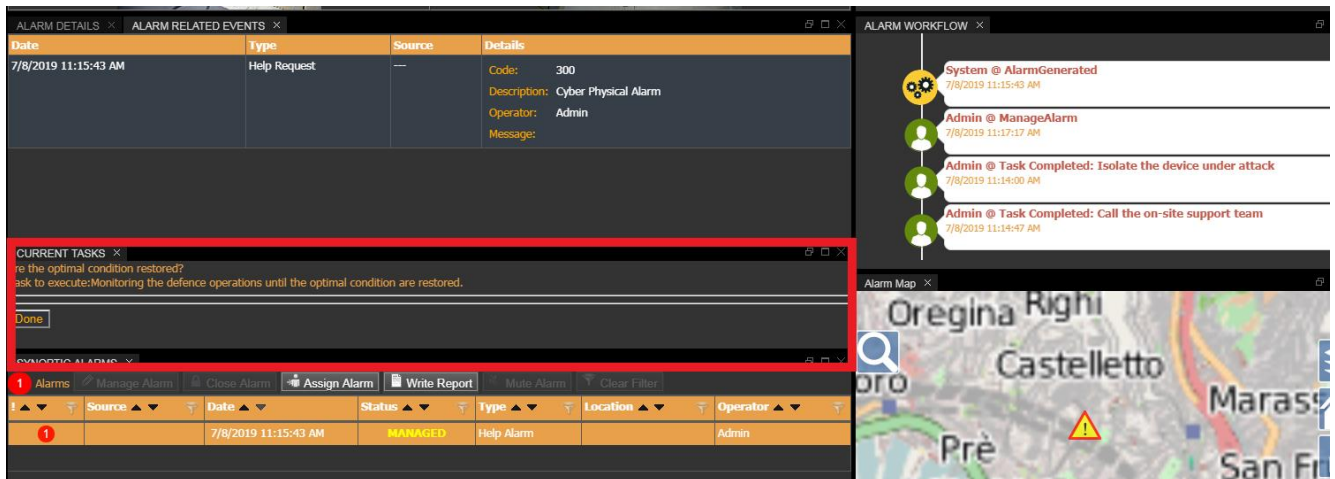


Figure 27 – Workflow current Task

The task already completed can be viewed into the Workflow task completed section that lists all the task already completed for the workflow associated to the alarm currently managed. See following picture:

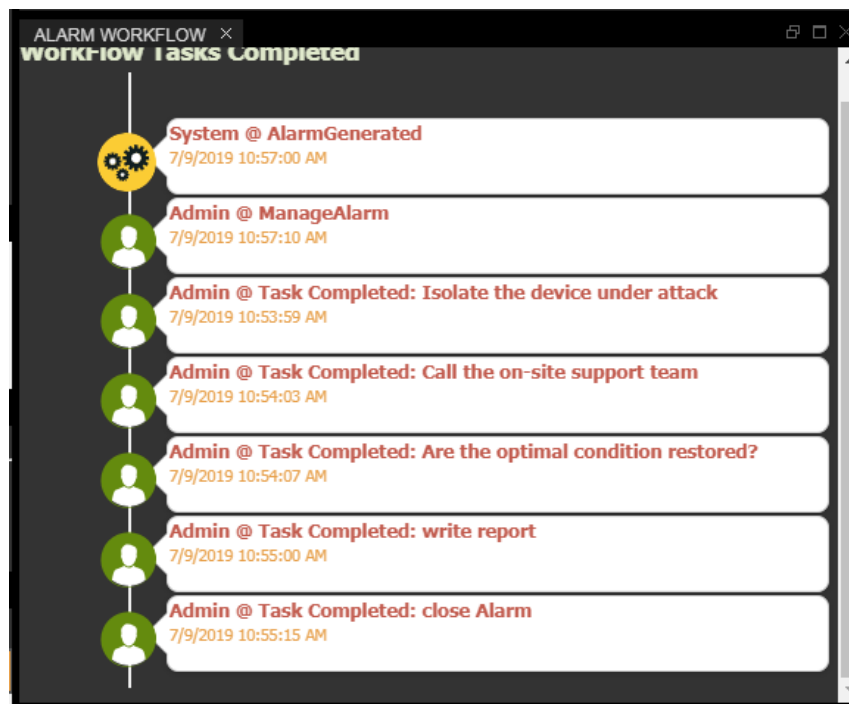


Figure 28 – Workflow task completed

The workflow is represented graphically according to the step currently executed.


The operations are displayed in different colors depending on their type:

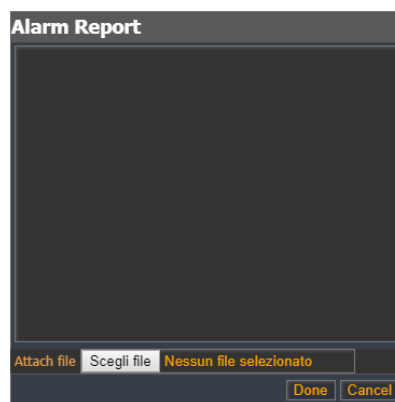
- User Task: operations performed by the operator
- Service Task: automated tasks
- Current Task: current operation
- Completed Task: completed operations.

When all the workflow tasks of an alarm are completed the user can close the alarm.

#### 2.2.4.2. Alarm report


On a managed alarm it is possible to associate a Report.

Select a Managed Alarm from the list and press the button  the mask will open, shown in the following figure.



**Figure 29 – Alarm Report**

The mask contains the alarm report text box in which it is possible to edit notes. Once the alarm is closed, reports can be shown by using the Administration Client to query the Alarm Archive.

It has to be noticed that the maximum number of simultaneously managed alarms is limited to ten for each operator. You can also attach a file to the report you are writing through the relevant button : you will open a window to navigate between local disk files and select the file to attach, as shown in the following picture.

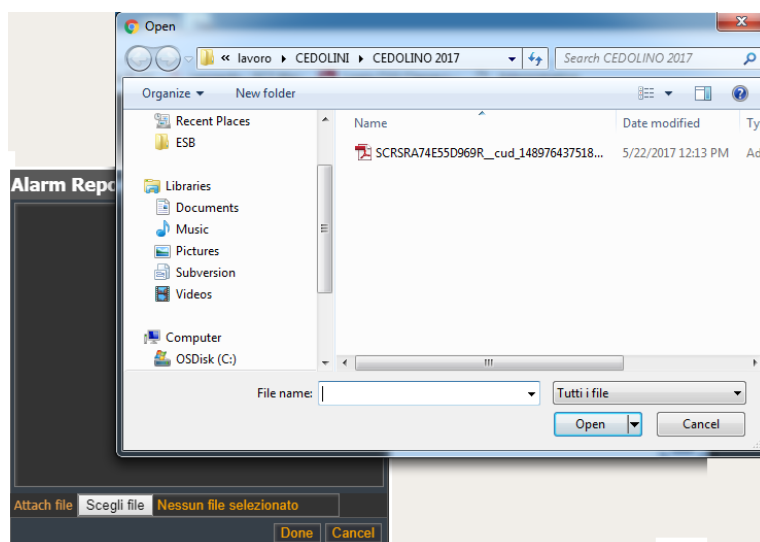


Figure 30 – Attach a file to a report

## 2.2.4.3. Alarms on GIS

If the GIS Service is configured, the Web Viewer shows automatically a panel (see Figure 20) containing the cartography in which it's possible to locate the resources of type Mobile Terminal (if configured in the system).

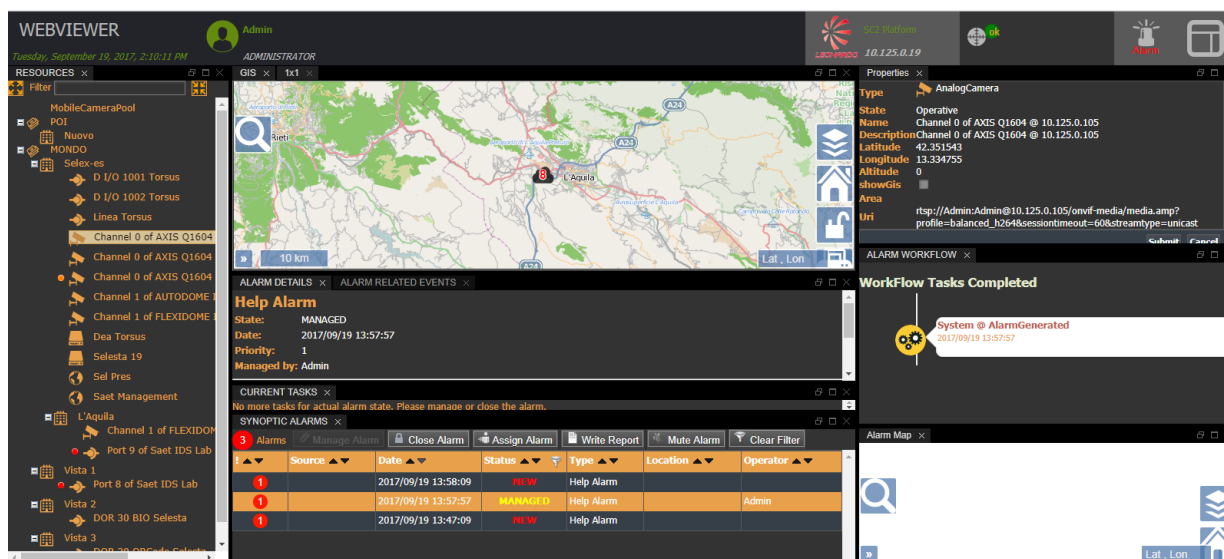
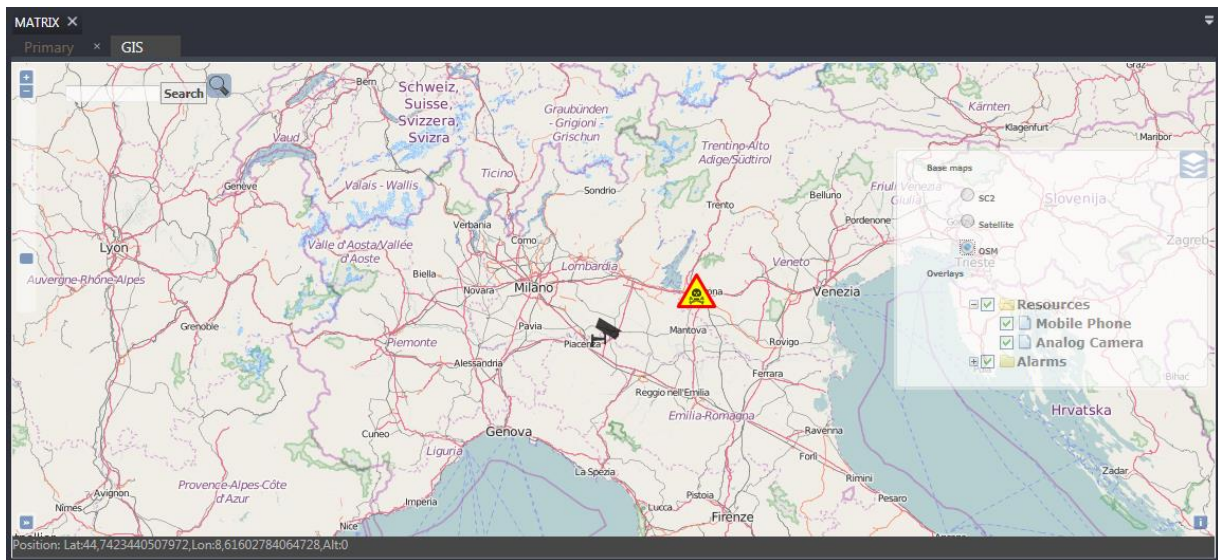


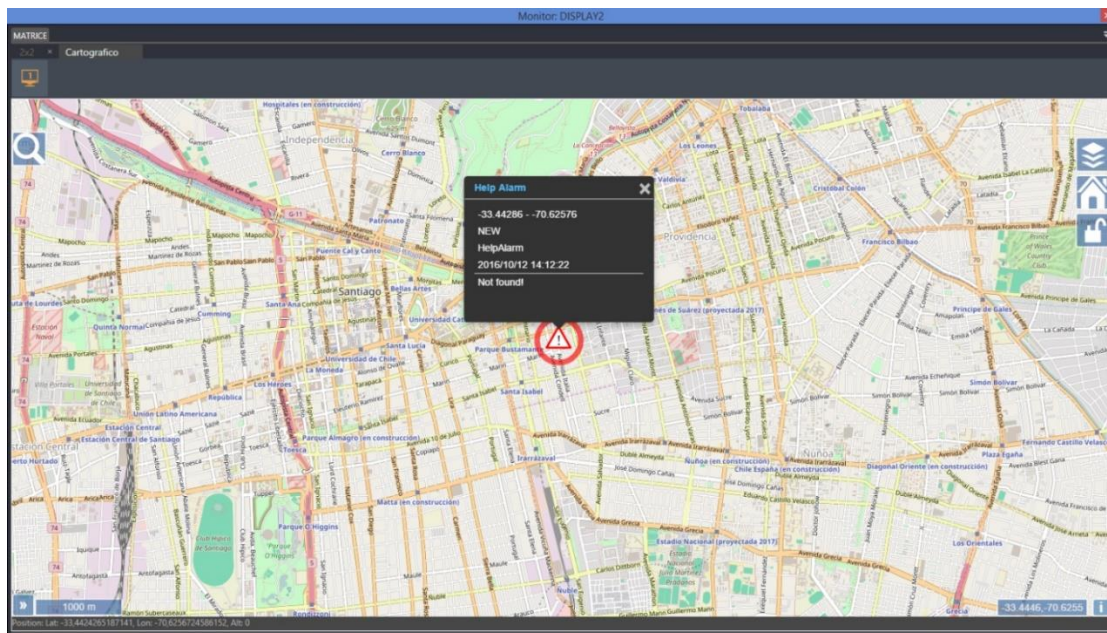
Figure 31–Gis cartography





**Figure 32 - base cartography**

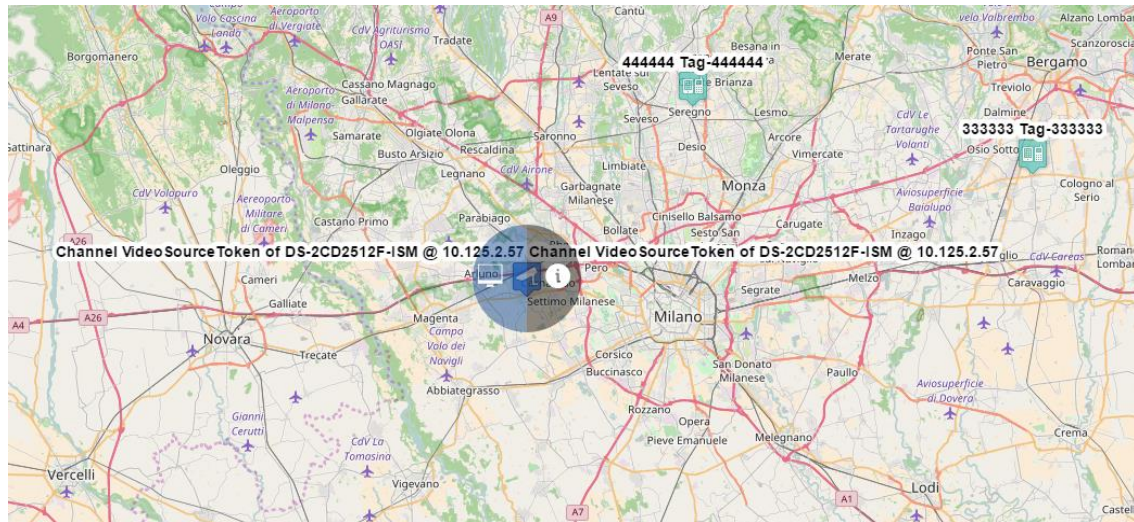
If you select an alarm on the map, you will see a small window containing a summary of the information regarding the alarm.



**Figure 33 – Details on Alarm**

Depending on the type of device will be displayed on the map information, icons and different colors, as shown in the following figure.





**Figure 34 - Device on map**

The map shows all the resources connected to the system and all alarms that have been generated. Depending on the type of alarm you will see a different icon.

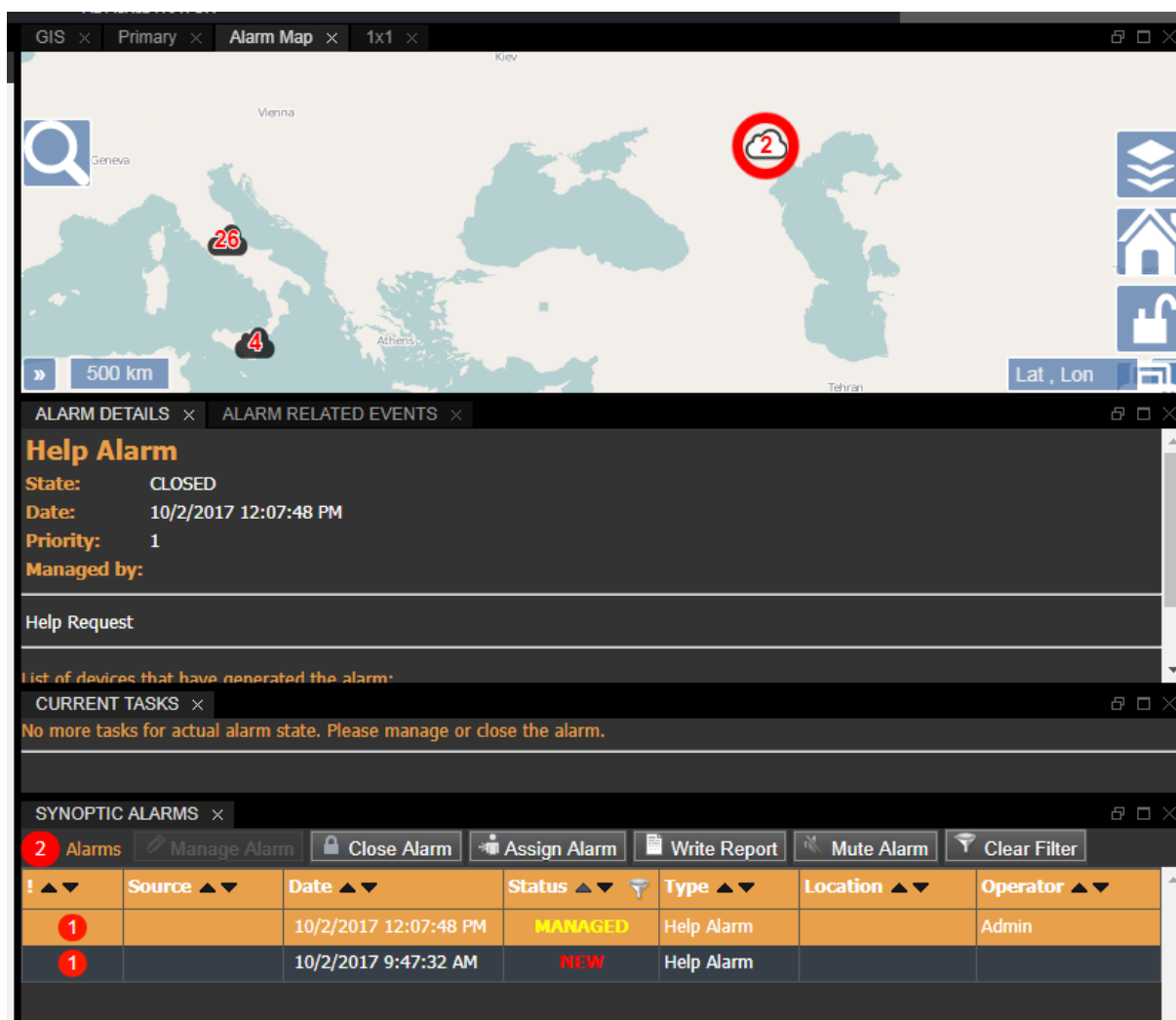



Figure 35 – Alarms on the map

#### 2.2.4.4. Alarm status and detail

The bottom of the icon that indicates the alarm (for example, for this  is yellow) indicates the alarm status:

- white = new,
- yellow = managed.

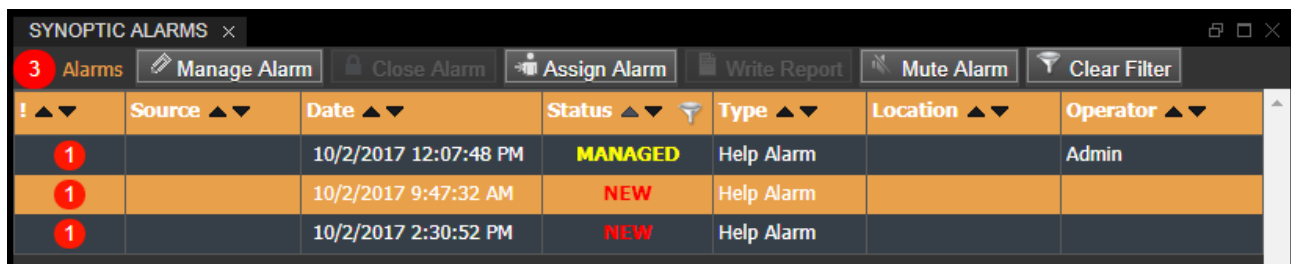
When the alarm disappears from the map means that it was closed.

The symbol within the icon indicates the alarm type and the color of the edge of the sign indicating the alarm priority, which will go from bright red, to the highest priority, the darker red for the lowest priority.

The Synoptic Table shows alarms in the new state (unmanaged) and in Managed state (currently managed). The alarms are displayed at the onset. When the Client starts, the Synoptic Table is populated with all the alarms that were New or Managed in the previous session, as well as with the alarms occurred during the period of inactivity of the Client.

New alarms are automatically closed by the system if they were older than a period configurable by the system administrator. Automatically closed alarms are still present in the Alarm Archive.

The feasibility and possibility to manage a determined type of alarm depends on users' role and privileges.



SYNOPTIC ALARMS						
<span>3 Alarms</span> <span>Manage Alarm</span> <span>Close Alarm</span> <span>Assign Alarm</span> <span>Write Report</span> <span>Mute Alarm</span> <span>Clear Filter</span>						
	Source	Date	Status	Type	Location	Operator
1		10/2/2017 12:07:48 PM	MANAGED	Help Alarm		Admin
1		10/2/2017 9:47:32 AM	NEW	Help Alarm		
1		10/2/2017 2:30:52 PM	NEW	Help Alarm		

Figure 36 - Device

The following figure shows how the system exposes for each alarm, the position on the map and a summary of information on the map.

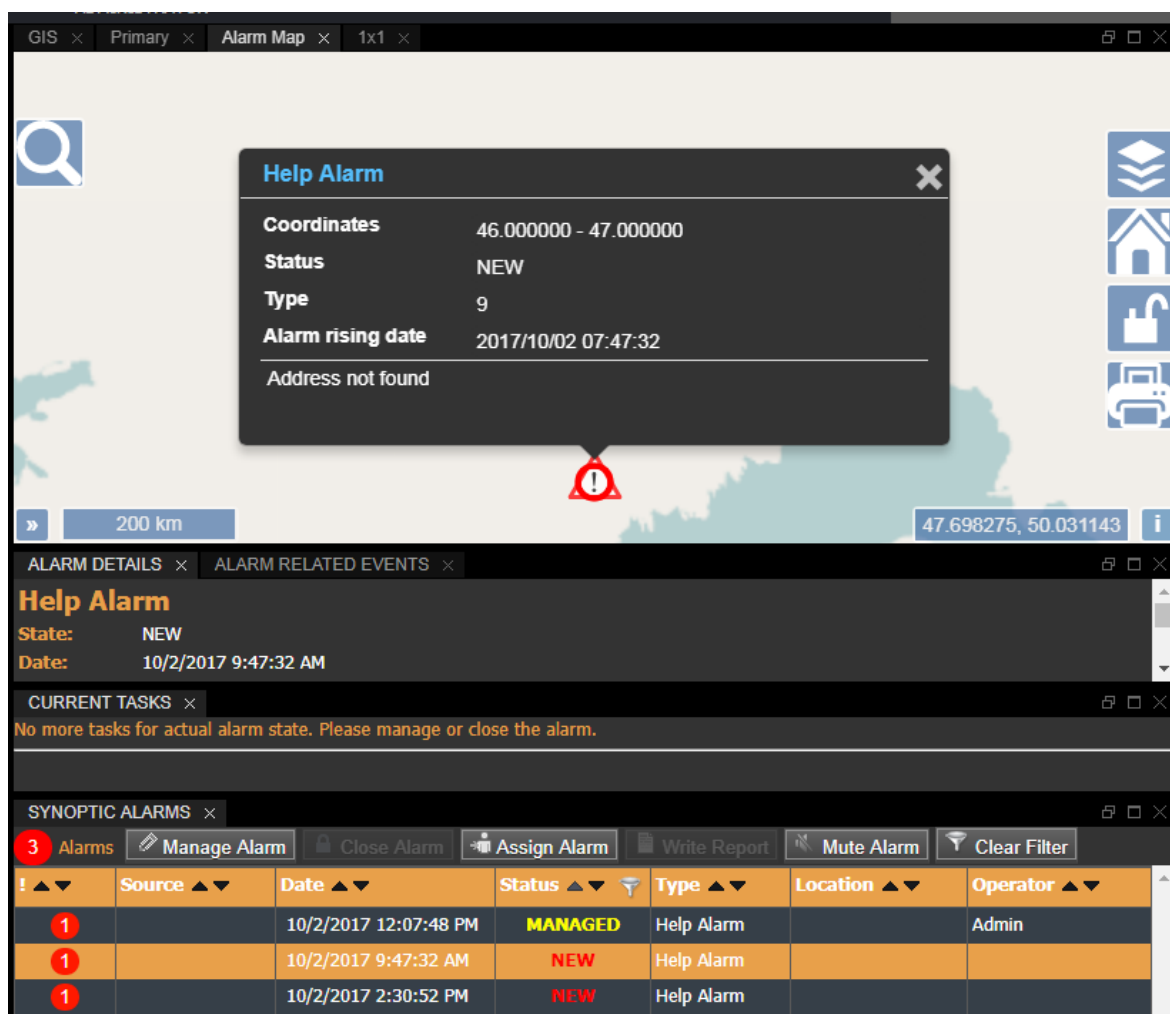
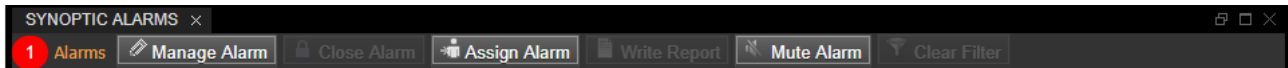


Figure 37 – Alarm Details

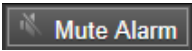
For each alarm the following information's are reported:

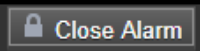
- Alarm priority from "1" (high) to "10"(low) and each priority is associated with a color 1, 2, 5, ..., 9, 10.
- The source of the alarm
- Date/Time of Alarm generation
- Status (New or Managed) the icon color is associated to the state of the alarm ( NEW = new alarm, MANAGED = managed)
- The Type of the alarm
- The location of the source
- Operator: for MANAGED alarms, the user who managed them.


Within the "Synoptic Alarms" tab, there are listed buttons that call the alarm management operations explained above.




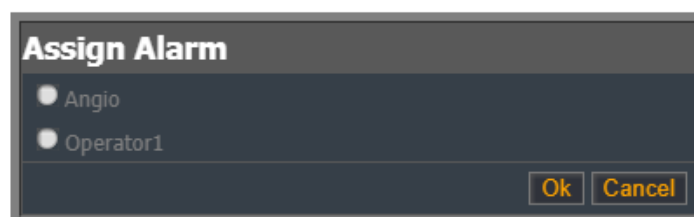
**Figure 38 – Alarm Toolbar**

When the alarm sound is enabled, it is possible to turn it off using the button  and inhibits the sound signal.

At the end of the alarm management, it is possible to close it by selecting the alarm with the left mouse button and choose "Close Alarm" : the alarm will be archived, placed in "Closed" state and will disappear from the "Synoptic Alarm" table.

Select an alarm from the table and press the button,  to starts executing the workflow to manage the alarm.

Select the alarm from the table and  to assign the alarm to another operator currently logged on another client machine: The mask, shown in the following figure, will appear which will allow you to select one of the listed operators.



**Figure 39 – Assign Alarm to another operator**

Selecting an alarm if the event happened in a zone with one or more cameras associated, the related live video streams are opened in a new tab of the workspace. If available, the map displaying the alarm position is shown as well. It has to be noticed that the maximum number of simultaneously opened tabs can be limited by the administrator.

The tab "Details Selected Alarm" shows the information associated to the currently selected alarm.

This mask separates diagnostic interrupts, less serious, from the list of alarms will therefore see two tabs each containing one of these two sets, respectively.


SYNOPTIC ALARMS x

1 Alarms Manage Alarm Close Alarm Assign Alarm Write Report Mute Alarm Clear Filter

! ▲▼	Source ▲▼	Date ▲▼	Status ▲▼	Type ▲▼	Location ▲▼	Operator ▲▼
1	Port 8 of Saet IDS	10/5/2017 9:48:18 AM	NEW	Tamper IDS Alarm	Saet Input 8	

Figure 40– Synoptic Alarm

On each tab, you can choose to see all the alarms in the list or only those in Status = "New" by performing the check on the corresponding item.

The filter is activated when I place the mouse pointer on the right edge of the column header, a funnel  will appear, as shown in the picture below.

SYNOPTIC ALARMS x

2 Alarms Manage Alarm Close Alarm Assign Alarm Write Report Mute Alarm Clear Filter

! ▲▼	Source ▲▼	Date ▲▼	Status ▲▼	Type ▲▼	Location ▲▼	Operator ▲▼
1		10/2/2017 12:07:48 PM	MANAGED	Help Alarm		Admin
1		10/2/2017 9:47:32 AM	NEW	Help Alarm		

Figure 41 – Synoptic Alarm

Pressing the funnel with the left mouse button, a drop-down menu will appear that allows you to select which filter to add to the " Alarms ", the selection is done by clicking on the box beside the item you want to select, then press the ok button.

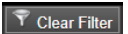
SYNOPTIC ALARMS x

2 Alarms Manage Alarm Close Alarm Assign Alarm Write Report Mute Alarm Clear Filter

! ▲▼	Source ▲▼	Date ▲▼		Type ▲▼	Location ▲▼	Operator ▲▼
1		10/2/2017 12:07:48 PM	<input checked="" type="checkbox"/> All	Help Alarm		Admin
1		10/2/2017 9:47:32 AM	<input checked="" type="checkbox"/> MANAGED	Help Alarm		
			<input checked="" type="checkbox"/> NEW			

ok

Figure 42 – Synoptic Alarm Filter

If you have applied a filter to the list of alarms in the table you can cancel it using the button .

Selecting a row from the synoptic alarms table will display in the "Alarm Details" panel all the information regarding the selected alarm, as shown in the following image.

**Alarm Details**

**Tamper IDS Alarm**

State: NEW  
Date: 10/5/2017 9:48:18 AM  
Priority: 1  
Managed by:

Tamper IDS Event

List of devices that have generated the alarm:

Type	Name	Description
	Port 8 of Saet IDS	Port 8 of Saet IDS

**SYNOPTIC ALARMS**

2 Alarms | Manage Alarm | Close Alarm | Assign Alarm | Write Report | Mute Alarm

Clear Filter

!	Source	Date	Status	Type	Location	Operator
1	Port 8 of Saet IDS	10/5/2017 9:48:18 AM	NEW	Tamper IDS Alarm	Saet Input 8	
1		10/5/2017 6:02:09	NEW	Help Alarm		

Figure 43 – Details Selected Alarm

By selecting the tab "Alarm Related Events", the events that triggered the alarm are shown.

**Alarm Related Events**

Date	Type	Source	Details
10/5/2017 9:48:18 AM	Tamper IDS Event	Port 8 of Saet IDS	

**SYNOPTIC ALARMS**

2 Alarms | Manage Alarm | Close Alarm | Assign Alarm | Write Report | Mute Alarm

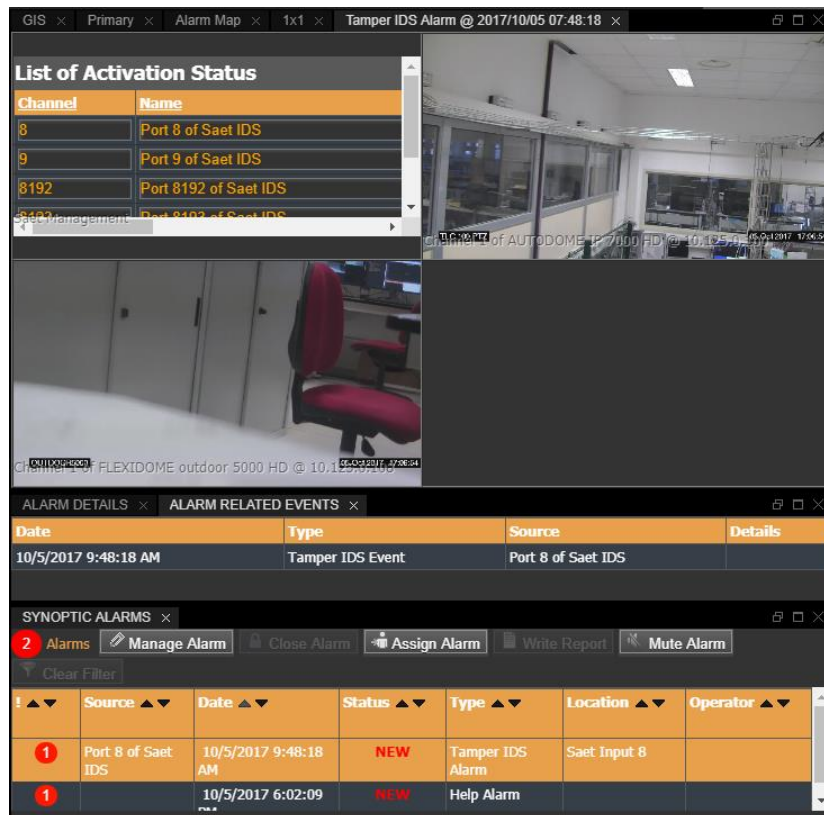
Clear Filter

!	Source	Date	Status	Type	Location	Operator
1	Port 8 of Saet IDS	10/5/2017 9:48:18 AM	NEW	Tamper IDS Alarm	Saet Input 8	
1		10/5/2017 6:02:09	NEW	Help Alarm		

Figure 44 – Alarm Related Events



Depending on the type of alarm selected, the appearance of this tab may change to present very different information between one type of alarm and another.



**Figure 45 – Alarm Related Events for a Tamper Alarm**

For most alarm types managed by the system, the "alarm related events" tab will contain a list of events and their description, while for particular types of alarms this tab will be the content of a much more complex information matrix. In the following paragraphs we will explain in detail these special cases of alarm types.

## 2.3.HMI components overview

The previous chapter SC2 describes which the basic component of the RESISTO HMI is. This chapter describes the composition of the RESISTO HMI based on the needs of the various use cases proposed. The configuration of the HMI is very flexible and therefore allows you to adapt to different needs depending on specific requirements.

The HMI can be multi-screen to ensure better visibility of all components. RESISTO is considered a three-screen configuration.

Each screen will be appropriately configured for operator functionality. These functionalities are different according to the use case treated and therefore a series of layouts will be suitably defined. Each layout is designed to optimize the vision and usability of the applications displayed and hosted in the HMI base SC2 Web Viewer (see the next figure).



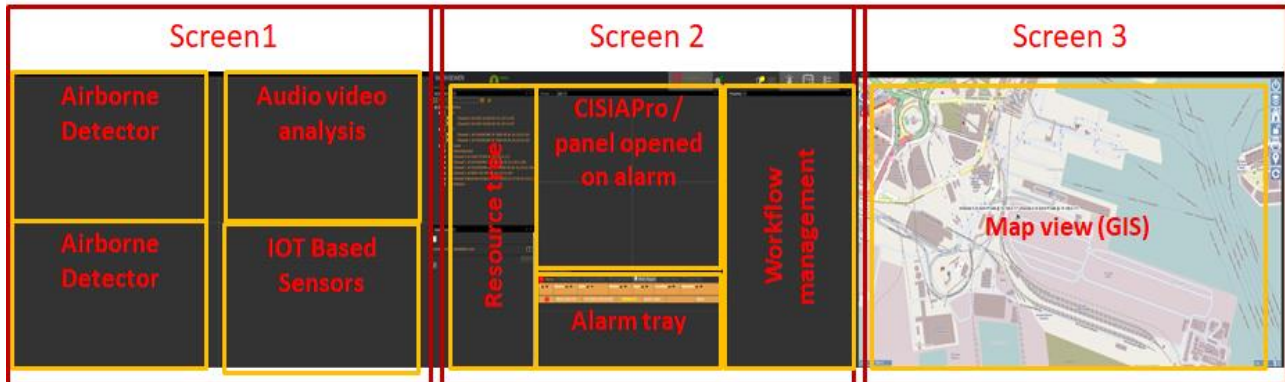


Figure 46 – three screen HMI example

RESISTO HMI will be based on 3 monitors with these purpose:

- **Screen 1:** It hosts vertical RESISTO web applications like integrated subsystems HMIs or camera it is possible to hosts more application using “multi panel” view.
- **Screen 2:** it hosts the base SC2 resource and alarm management modules:
  - Resource tree view
  - Alarm tray: it shows the currently opened alarms
  - Workflow management of the alarms: workflow diagram, action tasks and user interactive window.
  - At the center of page can be viewed a web app for example Risk Predictor (CISIAPro) or, in another panel, web pages opened when an alarm rise.
- **Screen 3:** it hosts the GIS based application to show georeferenced resources and alarms

HMI can personalize the panel and use multiple panel to show information that can't be seen into a single monitor. More panel can be added in needed

Visualization Layout are fully configurable and can be saved and restored

The Layouts can be customized for each user.

SC2 is fully dockable so every component can be shown/hidden and moved into every screen and every position of the screen.

Each panel is configured as a set of tiles that can be 1x1, 2x2,..., 5x5 and other configurations like in figure on the right, a different customized layout can be made by merging cells of a panel.



Figure 47 – Detail of Screen 1

Screen 1 is dedicated to vertical subsystem of RESISTO that exposes his own web HMI that will be hosted into SC2. It can be a four tiles panel with an application per tile.



Figure 48 – Detail of Screen 2

**Screen 2:** is dedicated to SC2 cockpit component:

- Resource tree
- Alarm tray
- Workflow management

Page opened on alarm click: for example alarm detail description, video stream, picture or data, information for the operator in order to mitigate the incident.

The entire HMI can be dockable so it is possible to move every component in any position of the screens and also eliminate one or more components.

Detail of alarm list:

8 Alarms		Manage Alarm	Close Alarm	Assign Alarm	Write Report	Mute Alarm	Clear Filter
▲ ▼ 🔍	Source ▲ ▼ 🔍	Date ▲ ▼	Status ▲ ▼ 🔍	Type ▲ ▼ 🔍	Location ▲ ▼ 🔍	Operator ▲ ▼	
3	Moxa 2214 CH0	10/23/2018 3:45:45 PM	NEW	Moxa Alarm	Zona2		
3	Moxa 2214 CH0	10/23/2018 3:10:26 PM	NEW	Moxa Alarm	Zona2		
3	Moxa 2214 CH0	10/23/2018 3:05:32 PM	NEW	Moxa Alarm	Zona2		
3	Moxa 2214 CH0	10/23/2018 3:03:34 PM	NEW	Moxa Alarm	Zona2		
3	Moxa 2214 CH0	10/23/2018 2:53:30 PM	NEW	Moxa Alarm	Zona2		
3	Moxa 2210 CH0	10/23/2018 2:52:06 PM	NEW	Moxa Alarm	Zona1		
1		10/23/2018 2:16:21 PM	NEW	Help Alarm			

Figure 49 – Alarm tray

The alarm opened visualized with a source, timestamp, alarm status (NEW, MANAGED), type of the alarm, location. It is possible to perform operations on the alarms for example to manage the alarm and perform the workflow, to assign the alarm to another operator, close the alarm only if the workflow of management is completed.

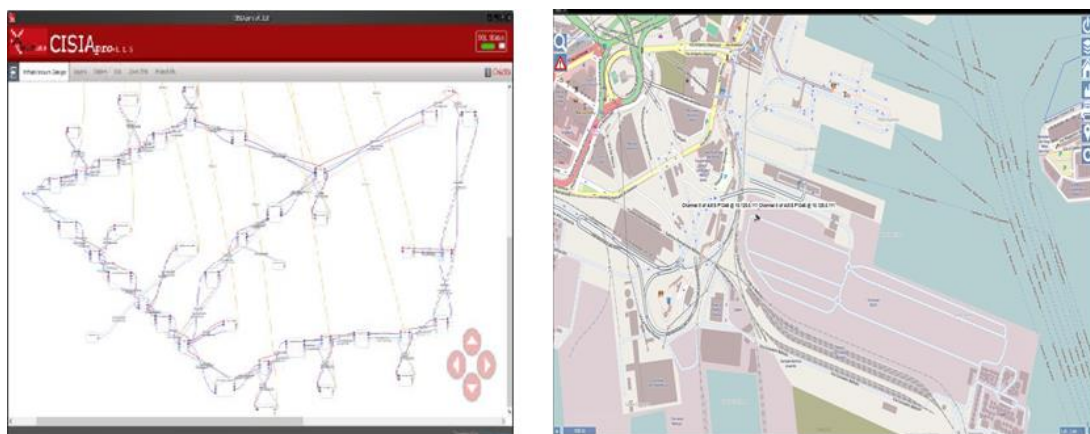


Figure 50 – Alternatives for Screen 3

In another context **Screen 3** can host Risk Predictor (CISIAPro) dashboard (panel 1) and RESISTO GIS (Panel 2). The applications will be shown into two panels to alternate visualization. In alternative the applications can be hosted into a 2 tiles panel.

For showing of other RESISTO application there are these options:

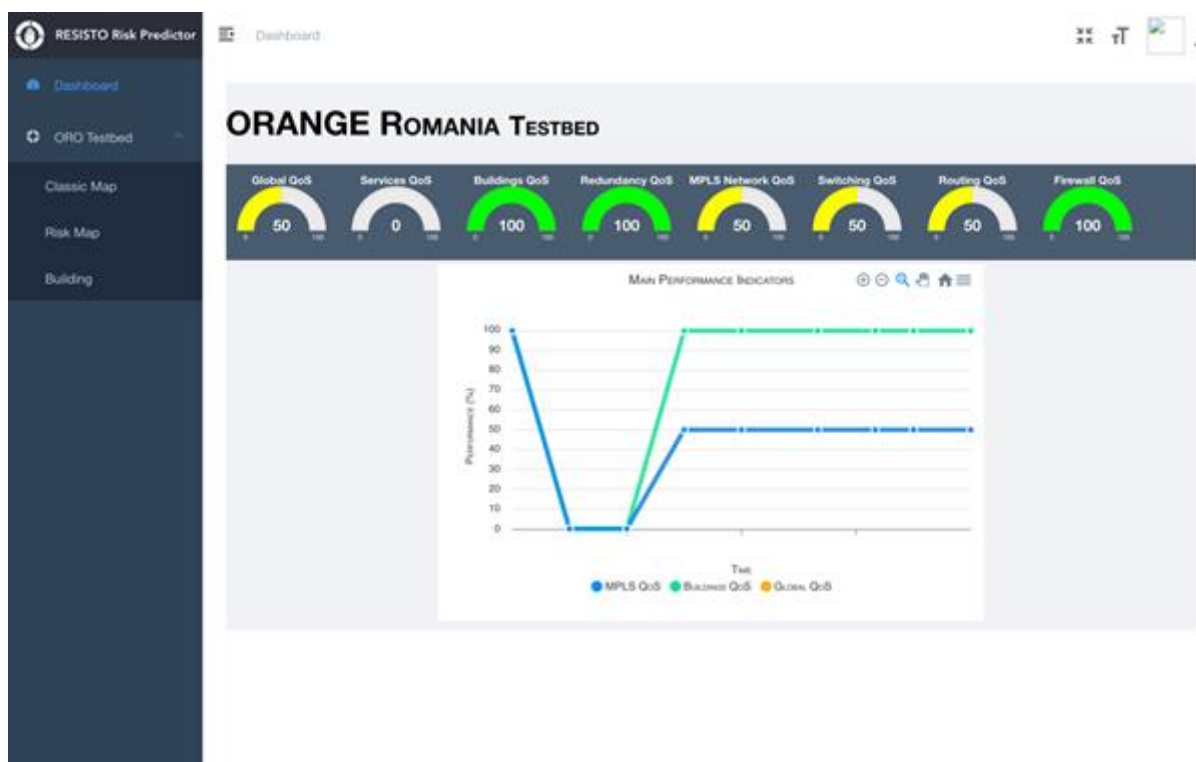
- Separation of a screen in more zones (e.g. Separate the third screen into 2 tiles or more tiles)
- Configuring different user layouts to view only a subset of application allowed for each user.
- Adding more panels superimposed into the screens.

For use cases where the use of a network orchestrator is foreseen, a space will be reserved in the HMI for the control interface of this component and for an application that allows the operator to always have the network situation under control monitored. This is also to highlight the actions carried out on the managed infrastructure and to view the effect of these actions in near real time.

## 2.4. RISK Predictor HMI

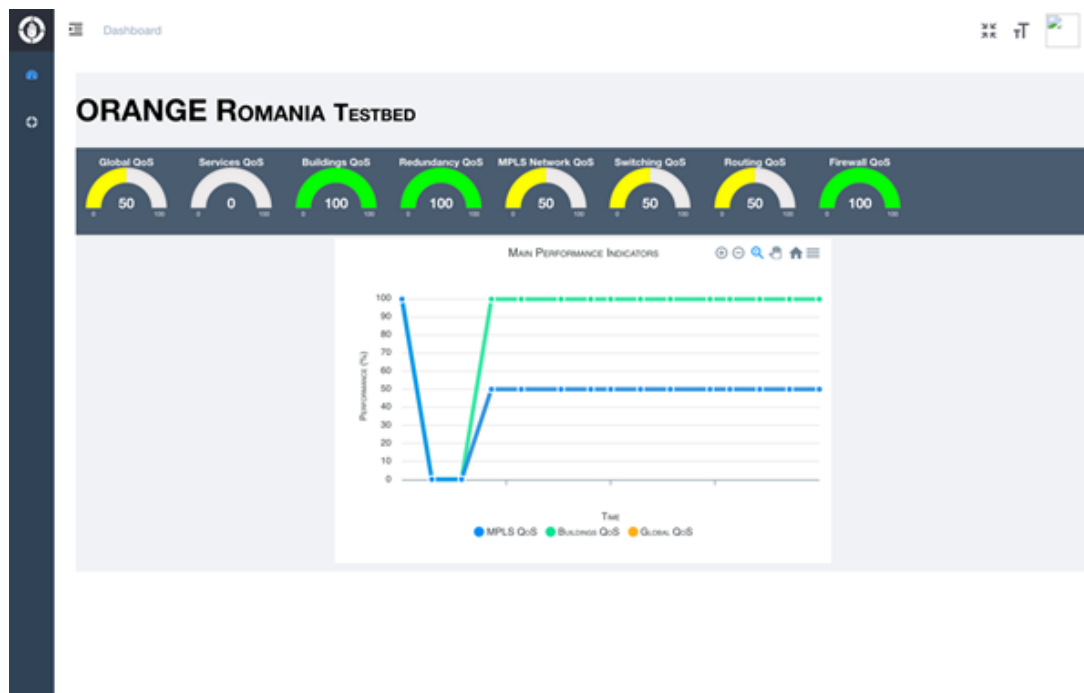
The Risk Predictor HMI wants to display the results of the simulator on assessing consequences of adverse events. Usually the aim is to have the same interface as the operator with additional information to improve the operator' situation awareness.

The Risk Predictor has a web page based on JavaScript framework. The Risk Predictor has a main dashboard containing the synoptic view of all the testbed as described in **Figure 51**, containing all the testbed with main indicators. AT the moment we provide only one case study.



**Figure 51 – Risk Predictor main dashboard**

All the pages have a left sidebar that can be partially closed, as in **Figure 52**, where only some icons are visible.



**Figure 52 – Risk Predictor main dashboard with left sidebar closed**

Each case study has at least three pages: a map without colours, a map with risk colours and a page for buildings or physical locations of the devices. All the pages contain the left sidebar that can be eventually closed.

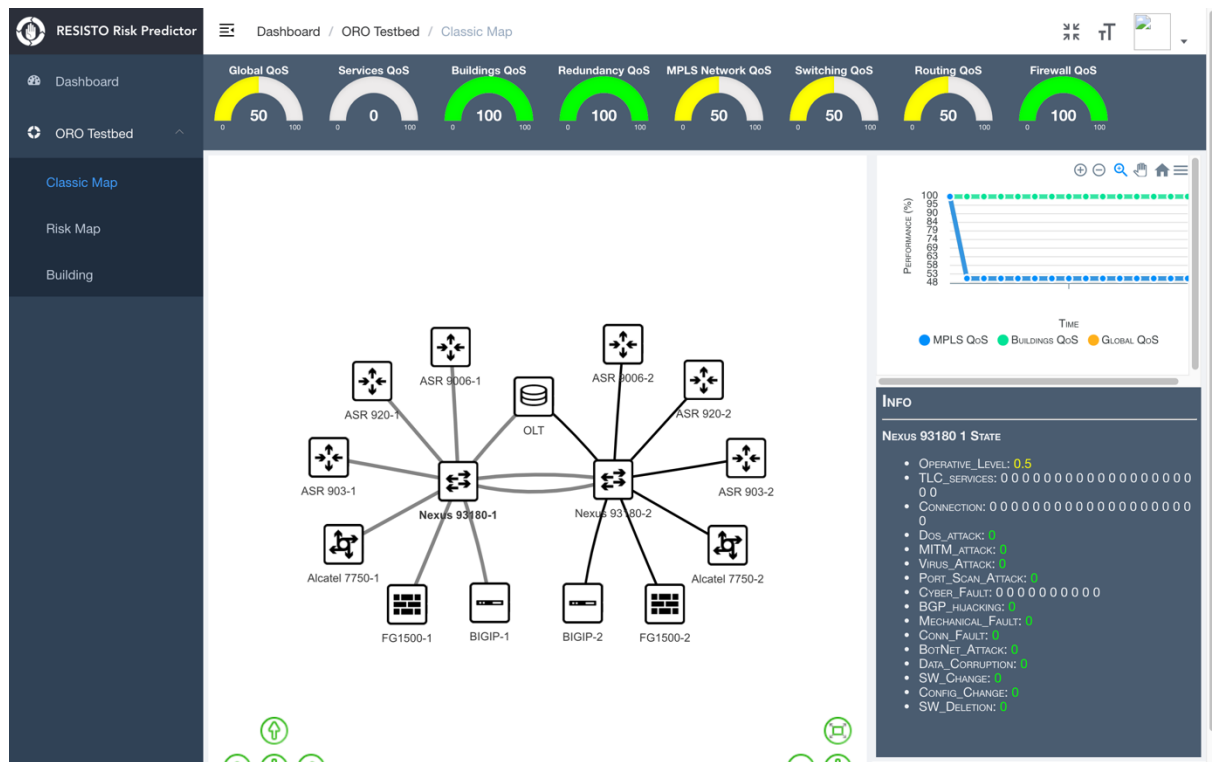
For the pages of the case study, we have three main sections: the header, the right sidebar and the centre.

The header contains the gauges for the main indicators which are evaluating using the Risk Predictor, as demonstrated in **Figure 53**, **Figure 54**, **Figure 55**. In this case, we have global QoS (Quality of Service), services QoS, Buildings QoS, MPLS Network QoS, Switching QoS, Routing QoS, Firewall QoS.

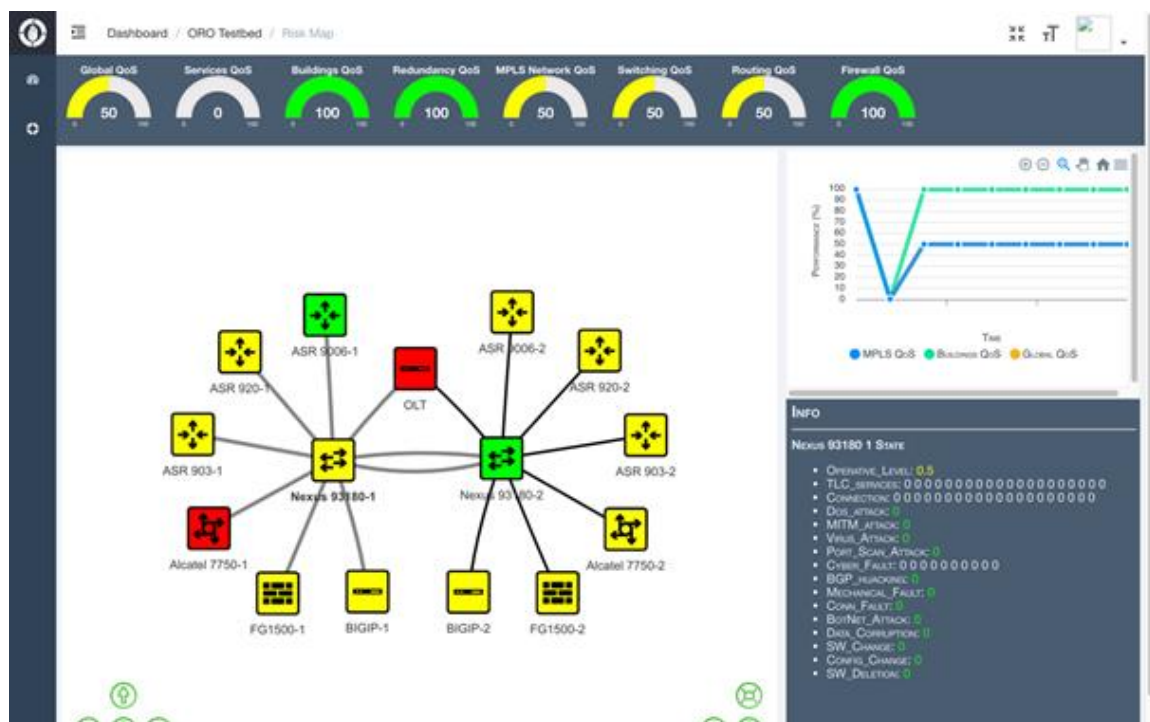
The right sidebar contains two parts. In the upper side we have the real time graphics of three main indicators: global, MPLS, and buildings QoS. Those three values can help us to assess the resilience of the infrastructure. In the below side of the sidebar we have the information related to the device we click in the map, with all the variables that are present in the Risk Predictor simulator. The aim is to better understand what is happening in the network and its consequences.

The central side of the page changes: in

, we have the topology of the actual case study without colours, in **Figure 53**, we have the same topology with the risk colours and in we have the buildings representation. The risk map is depending on the last output of the Risk Predictor (i.e., CISIApro 2.0) execution: the colours represent the forthcoming ability of this device to provide its job. In **Figure 55** we have the picture of the server rooms with the icons related to possible physical damages such as fire, water flooding, cooling fault or power fault. We also consider the unauthorized access problems.



**Figure 53 – Classic map of case study**



**Figure 54 – Risk map of case study**



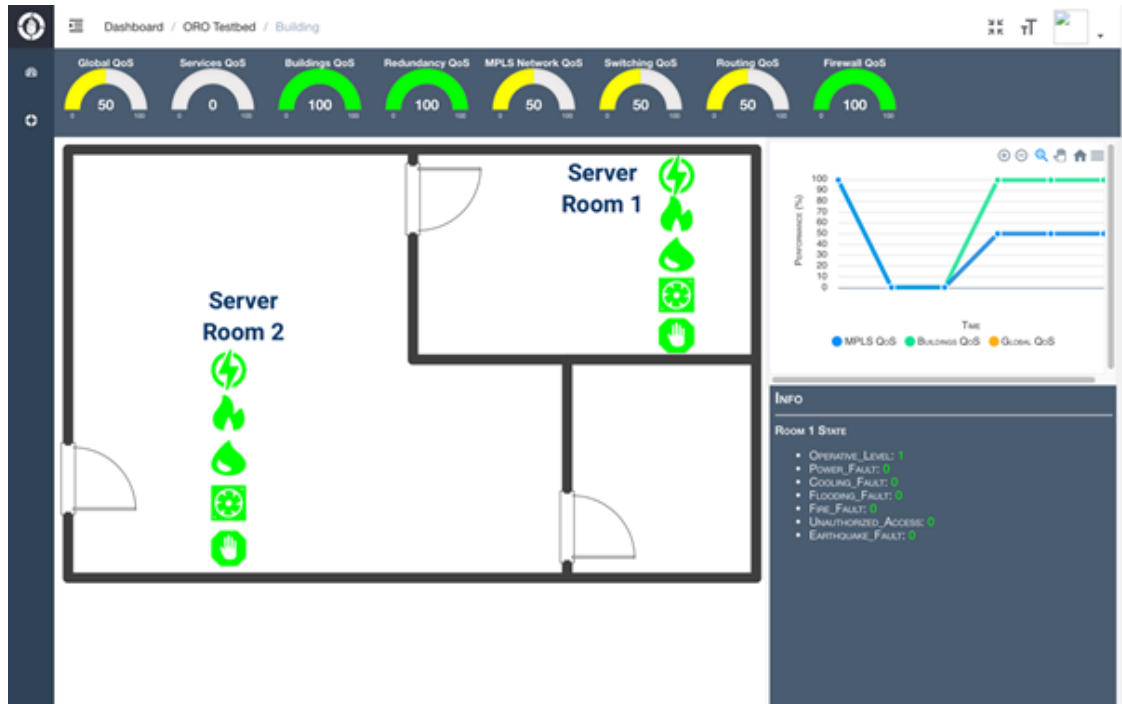


Figure 55 – Building map of case study

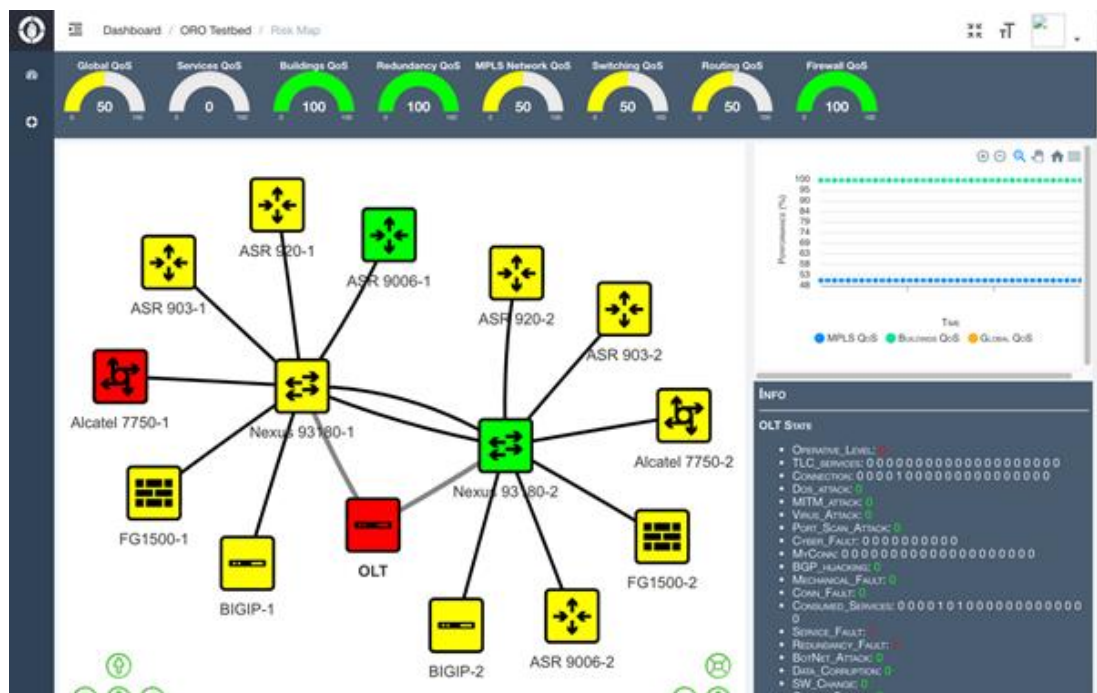


Figure 56 – Risk Predictor page with change in the topology



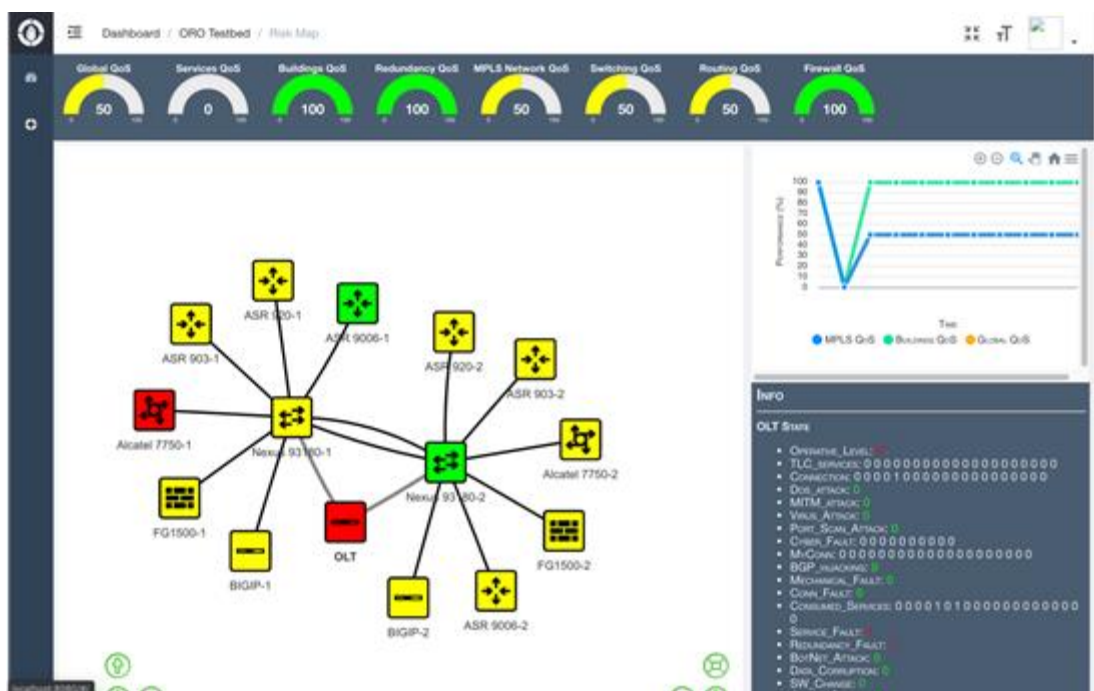
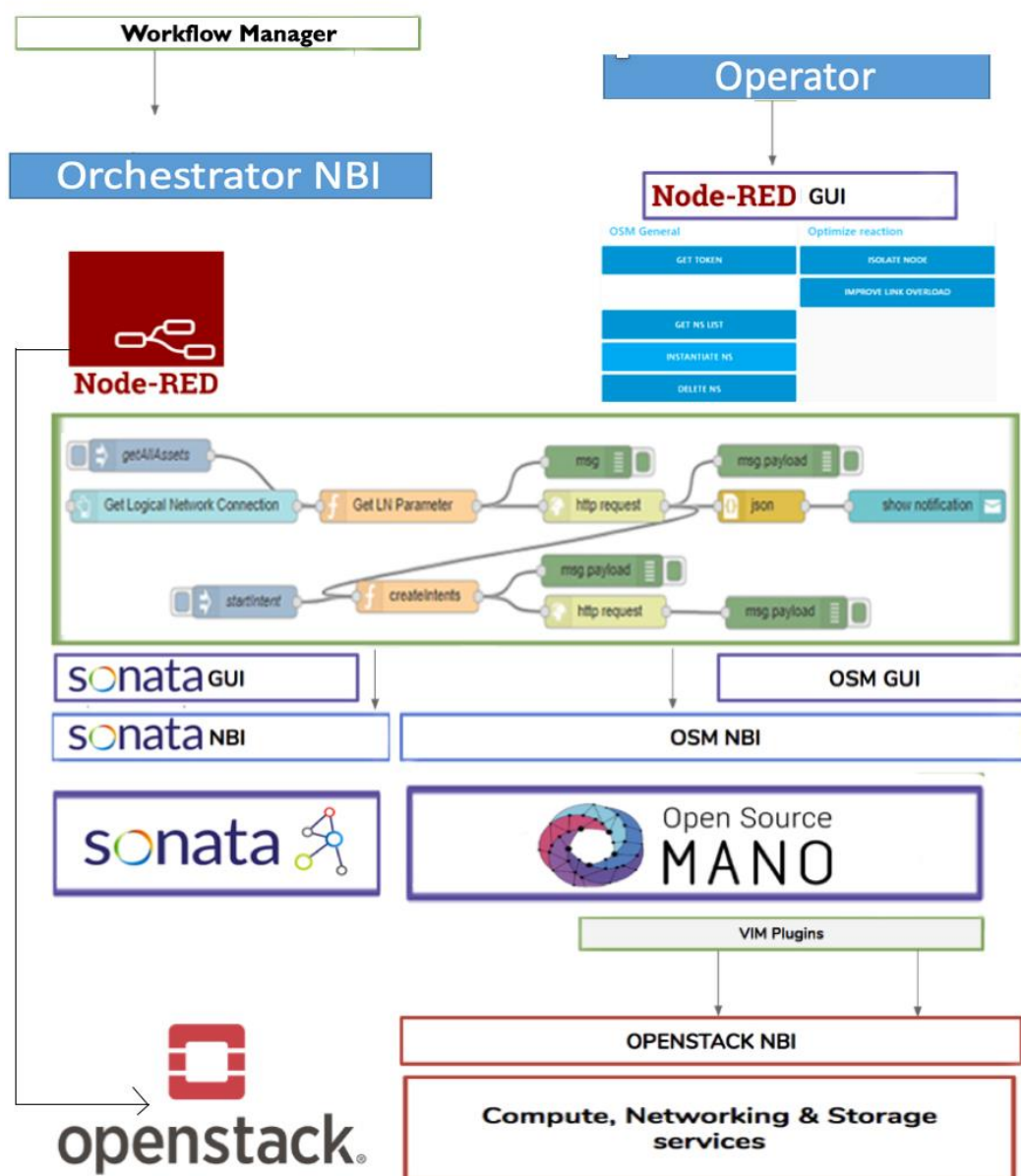


Figure 57 – Risk Predictor page with zoom in the map topology

The position of the devices in the map can be changed. The map topology can be enlarged, as in Figure 57, or can be reduced. The entire map can be moved in every direction.

## 2.5. Network Orchestration HMI

This chapter describes the Network Services Orchestration of RESISTO.

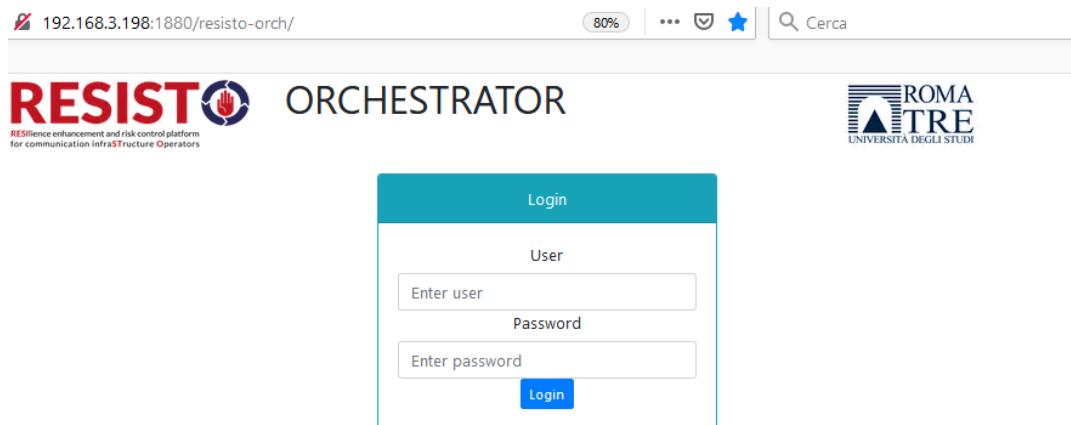


**Figure 58 - RESISTO Network Services Orchestrator overview**

RESISTO Network Services Orchestration application manage the lifecycle of Network Service and/or Network Slice through a high-level HMI that hide to operator the complexity of underlying network structure. The action available on the HMI can be also invoked through NBI, a subset of ETSI OSM's NBI compliant to ETSI NFV SOL005.

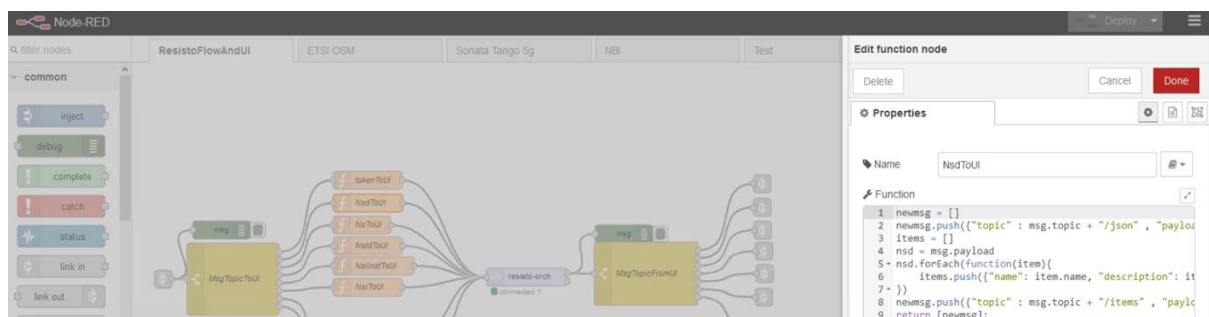
It communicates with ETSI MANO or SONATA TANGO 5G where the Network Services are defined and with Openstack Virtual Manager Infrastructure where will be instantiated.

The HMI is based on the Orchestrator web Viewer.



**Figure 59 - Orchestrator HMI login**

The HMI is made over a module of Node-Red where all the flows and calls to the Northbound API of the MANOs and Openstack are defined.



**Figure 60 - Orchestrator Node-red flows**

The major functionalities of the tool are:

- Interaction with ETSI OSM. (<https://www.etsi.org/technologies/open-source-mano>)
- Interaction with SONATA TANGO 5G (<https://www.5gtango.eu/>)
- NBI call monitoring
- User validation of request done through NBI
- Interaction with Openstack (<https://www.openstack.org/>) for tenant pre-production setup

After login all the Network Services/Network Slices defined on the underlying MANOs and relative instances on VIM are loaded and shown.

## ORCHESTRATOR

RESilience enhancement and risk control platform  
for communication infraSTructure Operators

ETSI OSM
Sonata Tango 5g
NBI Call
Openstack

Network Service Descriptors

Name	Description
slice_nsd	NSD to be used on Slice
slice_middle_nsd	NSD to be used on Slice

Network Services Instances

Name	State
slice_on_resistodemo2.slice_nsd_1	READY
slice_on_resistodemo2.slice_nsd_2	READY
slice_on_resistodemo2.slice_nsd_3	READY

Network Slice Templates

Name	State	Actions
slice_nst	ENABLED	<div style="border: 1px solid #ccc; padding: 2px 5px; display: inline-block;">Chose where instantiate ▾</div>

Network Slice Instances

Name	Description	State
slice_on_resistodemo2	Slice On ResistoDemo2	INSTANTIATED

**Figure 61 - Orchestrator HMI main screen**

Reporting the Network Services and Network Slice configured on OSM, as shown by OSM HMI

### NS Packages

[Home](#) > [Projects](#) > [admin](#) > [ns Packages](#)

[Compose a new NS](#)

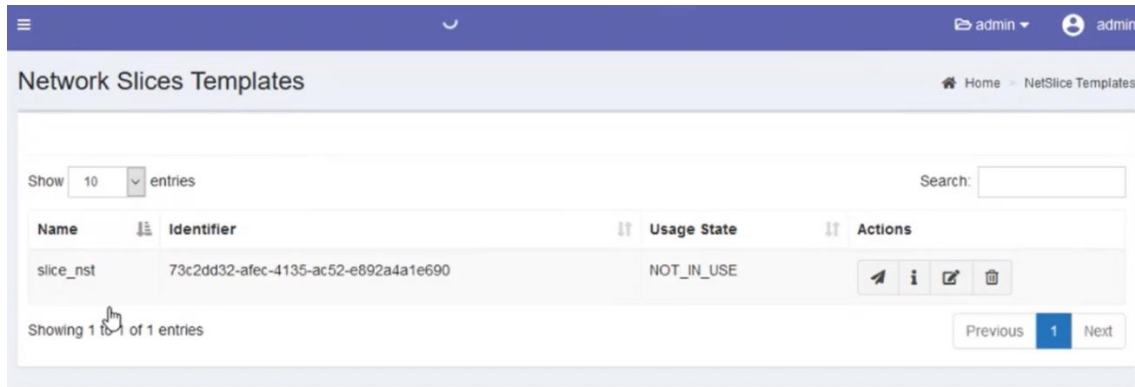
Show 10 entries
Search:

Short Name	Identifier	Description	Vendor	Version	Actions
slice_middle_ns	fe5103fe-3e1e-4ece-8f60-1254ba9dcc8d	NSD to be used on Slice	RM3	1.0	<div style="display: flex; gap: 5px;"> </div>
slice_ns	a98be12e-ca31-4fbc-81a7-69a8c54c42f2	NSD to be used on Slice	RM3	1.0	<div style="display: flex; gap: 5px;"> </div>

Showing 1 to 2 of 2 entries

[Previous](#)
1
[Next](#)

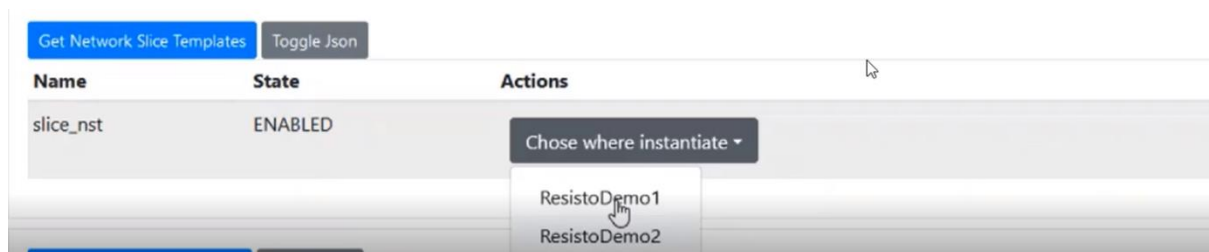
**Figure 62 – Network service defined on OSM**



**Figure 63 – Network slice template defined on OSM**

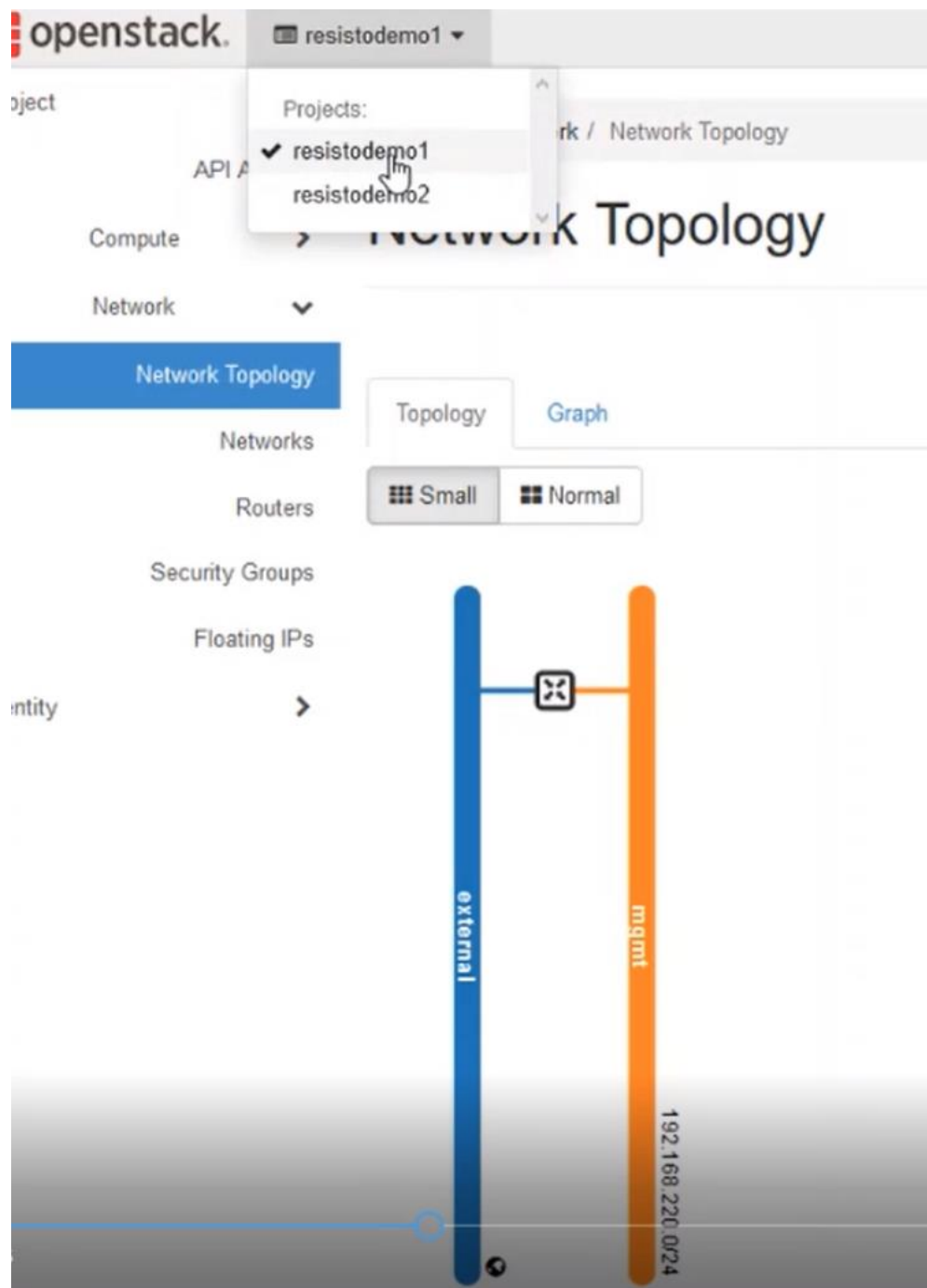
### 2.5.1. Interaction with ETSI OSM

The Actions drop-down menu sends the command to the OSM to instantiate the Network Slice on the selected infrastructure



**Figure 64 – Orchestrator instantiate network slice**

The menu items correspond to the VIMs defined in OSM which correspond to the two Tenants present on OPENSTACK, then selecting one of the two Tenants, the instantiation starts.



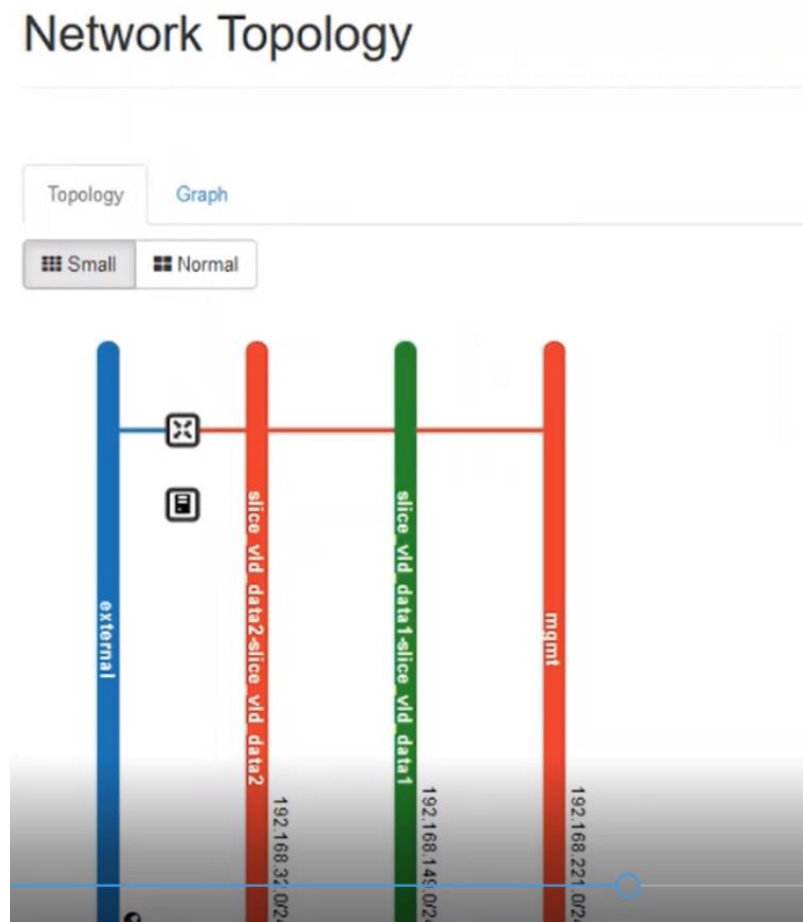
**Figure 65 – Orchestrator verify Network Slice instantiate on Opestack (1)**

The instantiation can be verified also on the OSM HMI

Name	Identifier	Nst name	Operational Status	Config Status	Detailed Status	Actions
slice_on_resistodemo2	78b172ef-9044-4251-8ede-b74fe32df597	slice_nst	init	init	Creating netslice subnets at RO	Actions

**Figure 66 – Orchestrator verify Network Slice instantiate on OSM (1)**

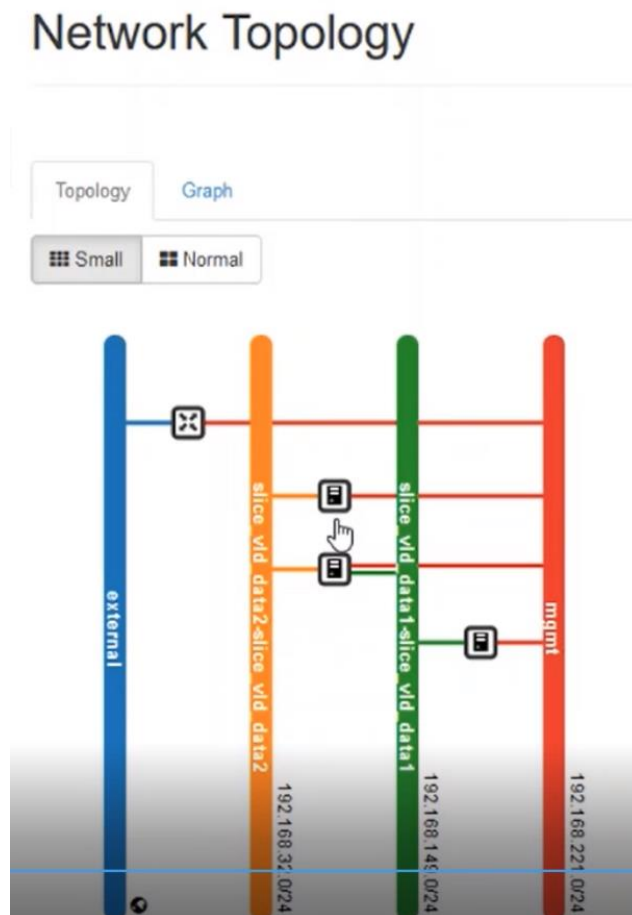
The progress of the instantiation can be verified in the Openstack HMI selecting the correspondent tenant and showing the network topology



**Figure 67 – Orchestrator verify Network Slice instantiate on Openstack (2)**

When all the Slices, the VMs have been instantiated and configured and connected to the correct networks, at the end of the operation the service will be correctly configured will go into RUNNING.





**Figure 68 – Orchestrator verify Network Slice instantiate on Openstack (3)**

The NS that make up the Slice are configured and in RUNNING.

MANO

admin admin

Home NS Instances

NS Instances

Show 10 entries

Search:

Name	Identifier	Nsd name	Operational Status	Config Status	Detailed Status	Actions
slice_on_resistodemo2 slice_nsd_1	a008dc4a-6f64-4a1d-b1c9-84404d20063c	slice_nsd	running	configured	done	[i] [g] [d] Actions
slice_on_resistodemo2 slice_nsd_2	0fe7fb62-b1e1-4229-b8ca-e6794e01146b	slice_middle_nsd	running	configured	done	[i] [g] [d] Actions
slice_on_resistodemo2 slice_nsd_3	3f7f39d2-dccd-4a8c-bd6c-2a1af7932547	slice_nsd	running	configured	done	[i] [g] [d] Actions

Showing 1 to 3 of 3 entries

Previous 1 Next

**Figure 69 – Orchestrator verify Network Slice instantiate on OSM (2)**

Everything results from the Orchestrator HMI.

Network Slice Instances 		
Name	Description	State
slice_on_resistodemo2	Slice On Resistodemo2	INSTANTIATED


**Figure 70 – Orchestrator verify Network Slice instantiate on Orchestrator HMI**

### 2.5.2. Interaction with Sonata Tango 5G

By clicking on the Sonata 5G TAB the Network Services configured in MANO are shown.

ETSI OSM	Sonata Tango 5g	NBI Call	Openstack
----------	-----------------	----------	-----------

Network Slice Instances 	
Name	Description
test-nsid2v	This is a integration test artifact.
test-nsid2v-monit	This is a integration test artifact.

**Figure 71 – Orchestrator Sonata Network Services from Orchestrator HMI**

As can view also on Sonata HMI

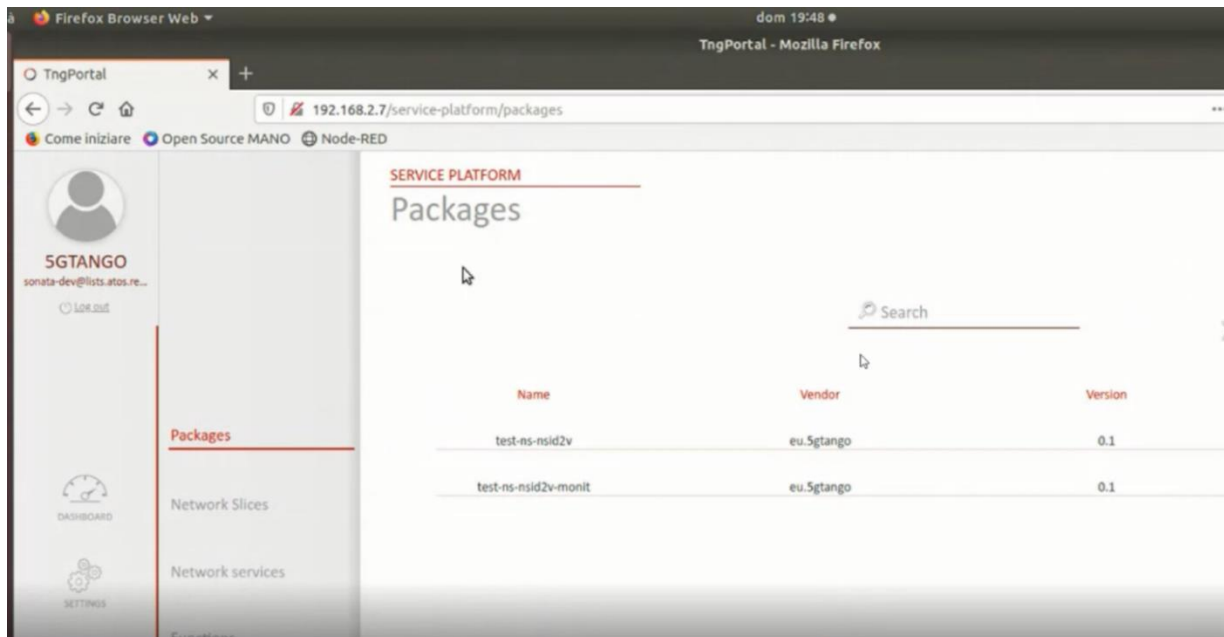


Figure 72 – Orchestrator Sonata Network Services from Sonata HMI

By clicking on the NBI CALL tab it is possible to view the calls to the Northbound interface received (for example from the Workflow Manager). It is possible to configure some APIs so that operator has the right to accept or reject the request.

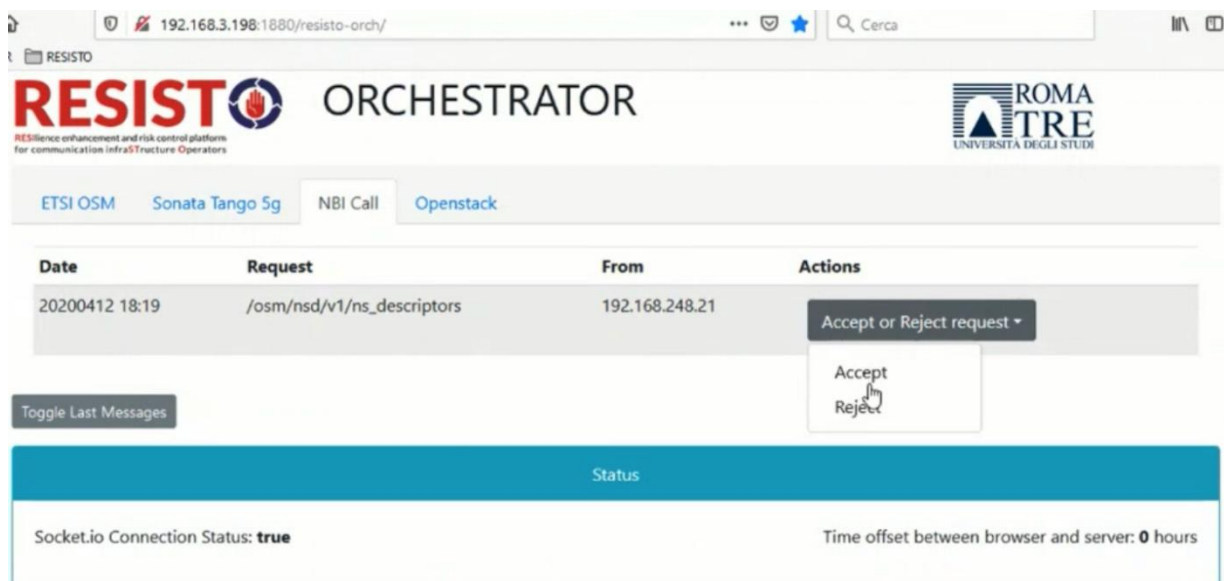
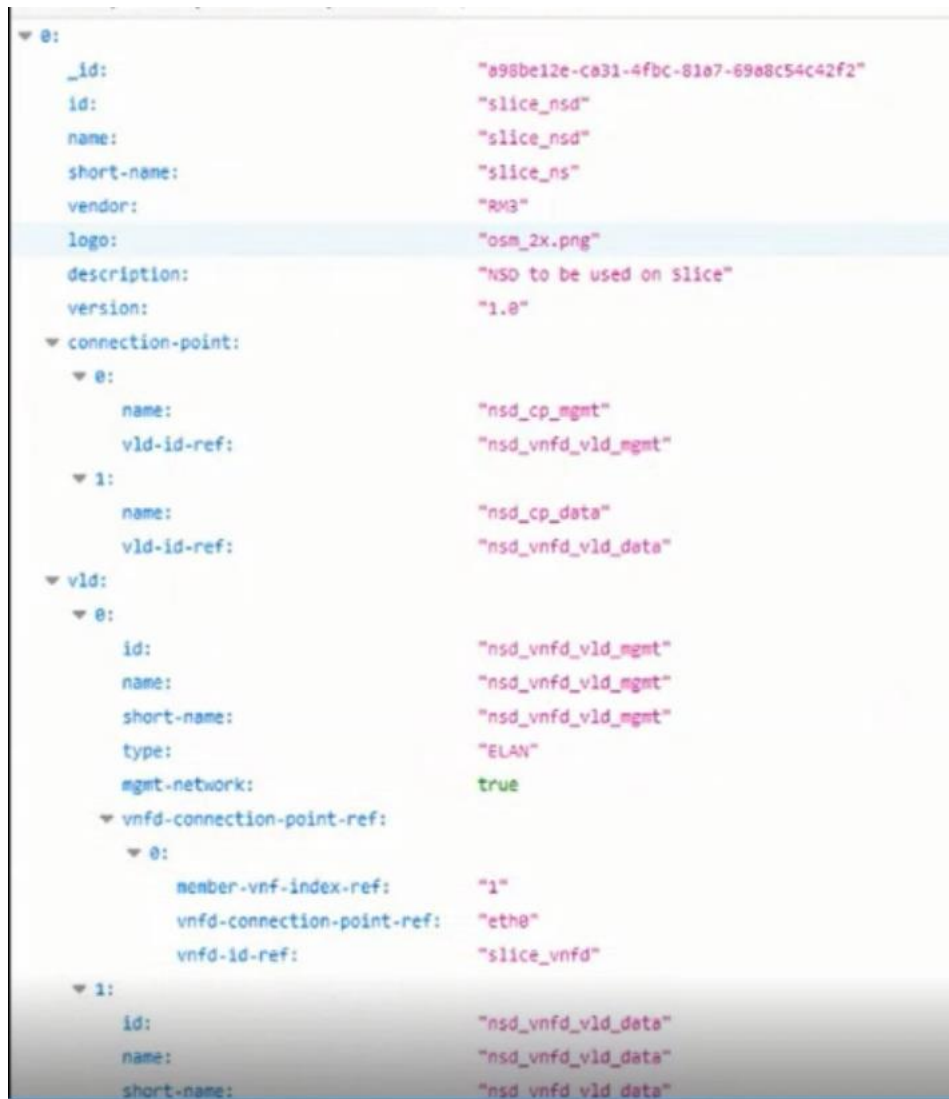


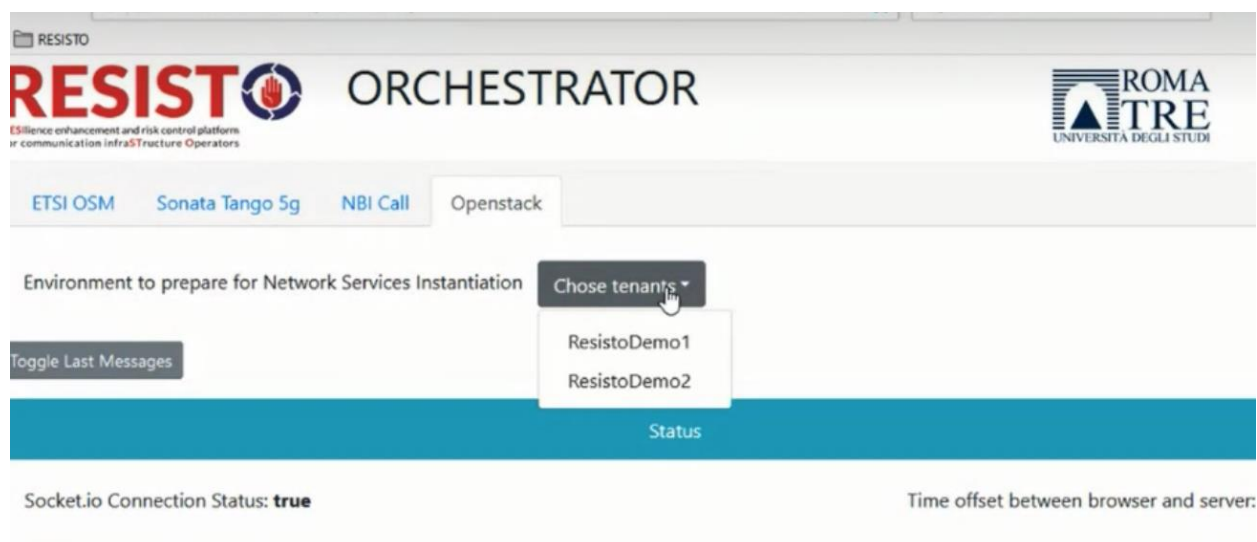
Figure 73 – Orchestrator operator Accept/Reject request from NBI



**Figure 74 – Orchestrator response to NBI request**

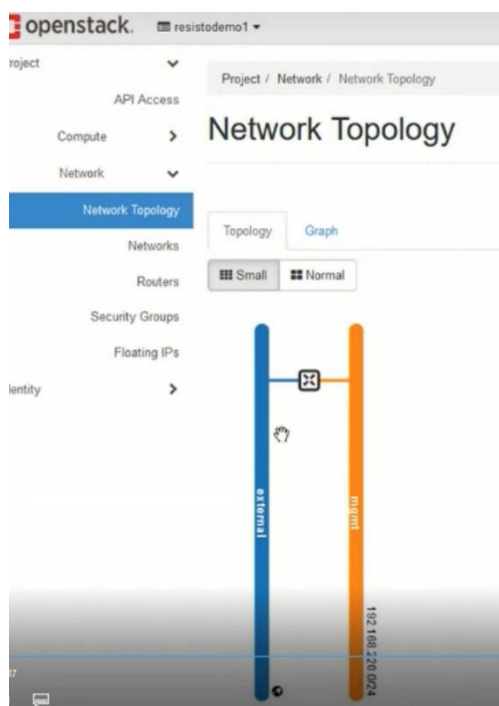
### 2.5.3. Interaction with Openstack

By clicking on the tab Openstack: it is possible to prepare the Tenants of the Virtualized Infrastructure Manager (VIM) configured in OSM so that they have the minimum Network resources to be able to instantiate the Network Service



**Figure 75 – Orchestrator tenant Openstack tenant configuration**

At the beginning the tenants just created by the Openstack administrator only have the connection to the external network (as you can see in the blue bar). The Orchestrator function creates the management records (orange bar) to which the NS will be connected to be managed and creates the connection to the external network by instantiating a virtual router.



**Figure 76 – Orchestrator Openstack minimal configuration**

## 2.6. Audio and Video Detector HMI

The smart surveillance system (including the audio and video detectors) aims to process video and audio streams in real-time for the detection of abnormal activity. Thus, the HMI requirements include the visualization of original and processed streams, the generated alerts and configuration panels.

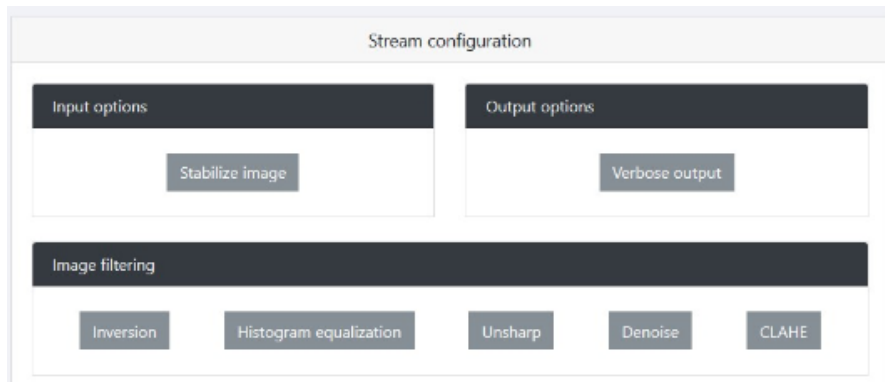
- Visualization of original and processed streams: This requirement is mainly focused on the video streams where the visualization of real-time video streams including the original video as well as the annotation of the detected and classified objects is required. For example, the operator will be able to see the video stream and when a person is detected then a square will appear around it (Figure 77).



**Figure 77 – Annotated detected persons**

- Detections: The detections by the smart surveillance system will appear in the form of alerts to the RESISTO platform. The visualization of the alerts will follow the standard visualization as RESISTO platform offers. The alerts will be communicated with the RESISTO platform through the KAFKA broker.
- Configuration Panel: A dedicated interface for the configuration of the audio and video sensing platform is required. Through this panel the operator will be able to configure, calibrate, enable/disable the sensors as well as to proceed to navigation (movement) actions where is applicable.





**Figure 78 – Video stream configuration**

Another important requirement of the HMI for audio and video detectors is the geo-referencing of sensors, field of view and detections/alerts of the smart intelligence system. To visualize all this information a map view is required. The map will include the geo-reference target detections as well as the location and the field of view of the sensors. Similar, audio sensors will be visualized and the location of detection will be appeared either as exact location or an estimation. Finally, a set of functionalities are allowed through the interactive map.



**Figure 79 – Map view of camera detections and alerts**

## 2.7. RADIOFILTER and RANMONITOR HMI

The integrated RADIOFILTER HMI will be made up of the following components:

- Sensors Management: A dedicated panel for the configuration parameters of the WLAN sensors if required.
- Alarms Panel: A panel showing up on-going alarms related to the threats and attacks that RADIOFILTER is able to detect.
- Detected AP & Devices and Whitelist Table: A table showing the most relevant parameters associated to the devices and access points inside the infrastructure.



- **Building Map:** A map showing the location of the sensors and the approximate location of the devices and access points if required.

A standalone RADIOFILTER HMI has already been developed in the project for RADIOFILTER, of which certain elements will be integrated with the RESISTO HMI platform. The standalone HMI is shown in the two figures below:

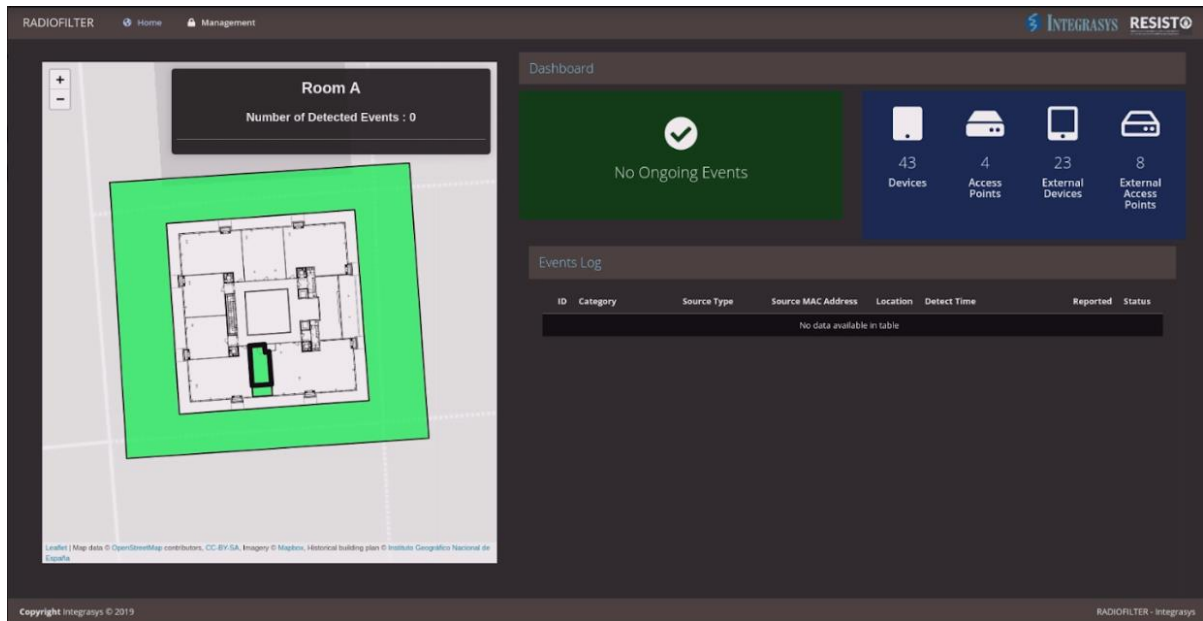


Figure 80 – RADIOFILTER HMI (1)

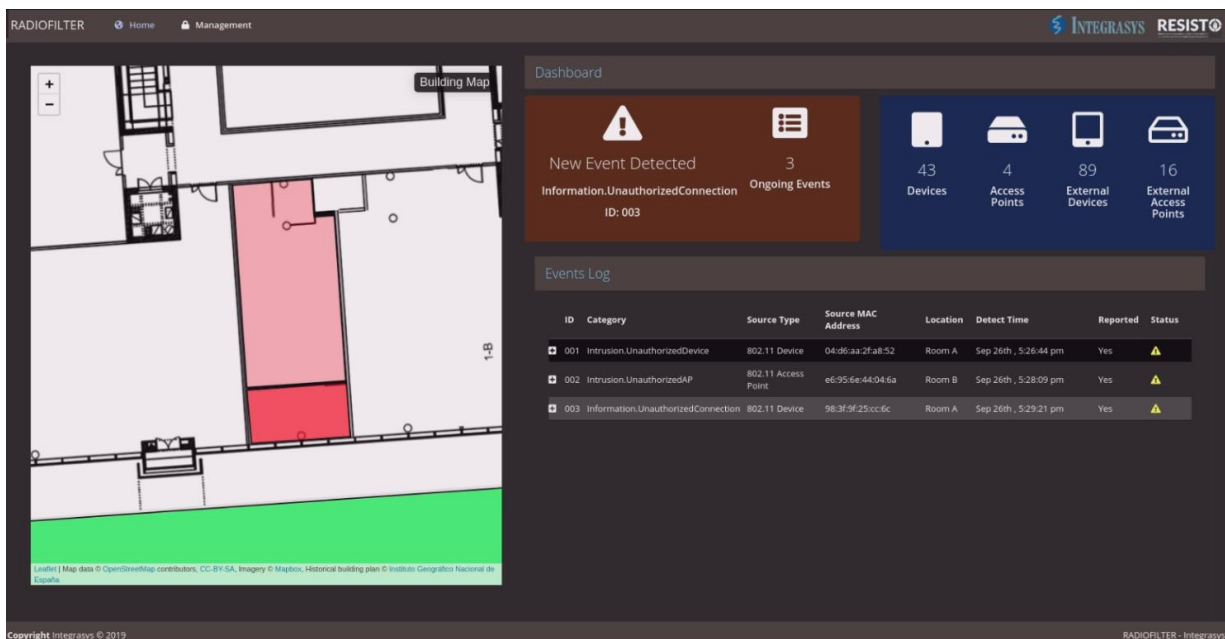


Figure 81 – RADIOFILTER HMI (2)

On the right-hand side of the standalone RADIOFILTER HMI, the Building Map can be seen. The left-hand side is divided into two main panels. The upper panel shows the dashboard for detected events and number of detected devices and access points. The lower panel shows a log table with detected events.

The integrated RANMONITOR HMI will be made up of the following components:

- Sensors Management: A dedicated panel for the configuration parameters of the LTE sensors if required.
- Alarms Panel: A panel showing up on-going alarms related to the threats and attacks that RANMONITOR is able to detect.
- Detected Cells Table: A table showing the most relevant parameters associated to the LTE cells in the area to be protected.
- Cells Map: A map showing the approximate location of the operator's cells/base stations.

A standalone RANMONITOR HMI has already been developed in the project for RANMONITOR, of which certain elements will be integrated with the RESISTO HMI platform. The standalone RANMONITOR HMI is shown in the two figures below:

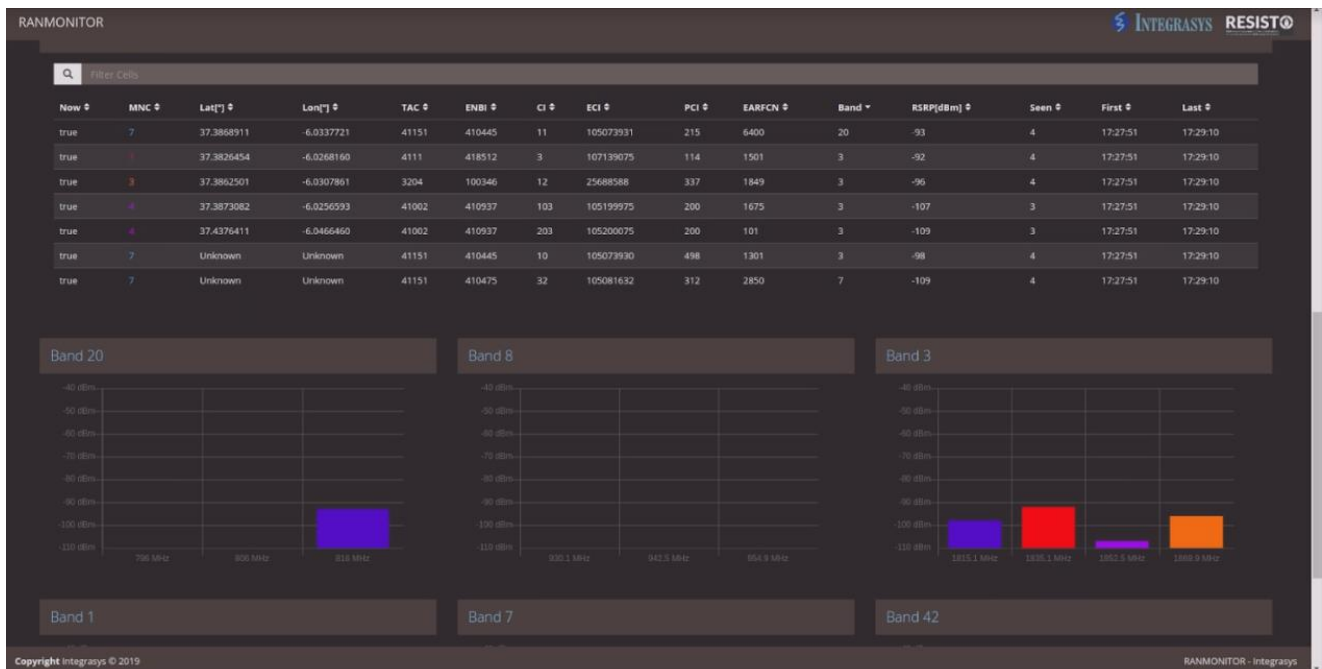
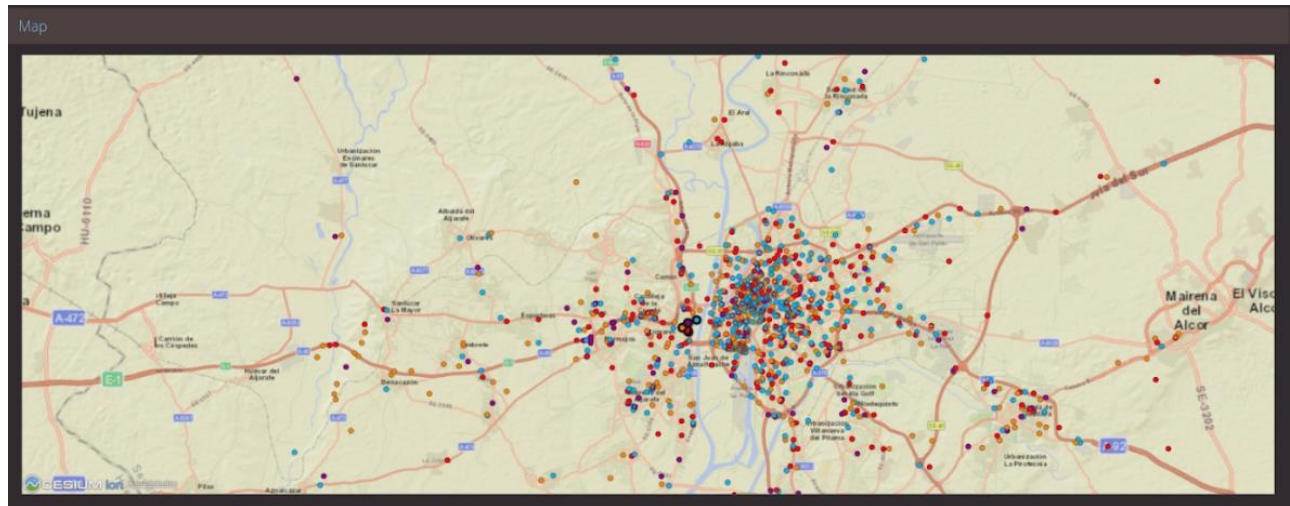


Figure 82 – RANMONITOR HMI (1)



**Figure 83 – RANMONITOR HMI (2)**

In the first figure, a table with the detected cells and its related parameters can be seen in the upper part. Below the table, a visualization space is included with bar graphics representing the received power from the different cells. In the second figure, the map is depicted showing the approximate location of the different cells/base stations.

## 2.8. HMI Adaptation

The HMI adaptation process aims to provide a mechanism for the adaptation/configuration of existing web-based HMI (non RESISTO) or visualization tools to provide a homogenized HMI look and feel with RESISTO HMI platform. The first part of this task was the identification of the HMI requirements of the detectors and the visualization needs of the use cases. Details of the HMI requirements for each detector have been already described in the previous paragraphs of this document. Based on D2.8, the following use cases will be covered by the HMI adaptation:

1. Core Network Failure caused by Physical & Cyber Attacks to Telecommunication sites
2. Terrorist Attack and Natural Hazards causing network failure and telecommunication congestion
3. Telecommunication sites
4. Disruption of major sporting event by combined physical & cyber-attack by a terrorist organization
5. Protection of Cloud Storage Services
6. Cyber and physical protection of network and network elements mechanisms used by critical services that impact users
7. Maritime Safety and Emergency Case
8. PPDR Virtual Operator
9. 5G network response to a security breach

<b>Use Case</b>	<i>Number/Title of the Use Case</i>	
<b>Involved Partners</b>	<i>Owner, Detector providers, etc.</i>	
<b>Detectors</b>	<i>Detector 1</i>	
	<i>Detector 2</i>	
	<i>Detector 3</i>	
<b>Data</b>	<i>Dataset 1</i>	<i>Interface 1</i>
	<i>Dataset 2</i>	<i>Interface 2</i>
<b>Web-Based HMI</b>	<input type="checkbox"/>	
<b>HMI Requirements</b>	Description of requirement	Available HMI <input type="checkbox"/>
		RESISTO HMI <input type="checkbox"/>
		New HMI <input type="checkbox"/>
<b>HMI Adaptation</b>	Details about HMI Adaptation	

**Figure 84 – Template for HMI Adaptation requirements per use case**

An example about the HMI requirements of WP7 scenarios is given below.

- Visualization of video feeds: The video feeds from smart surveillance protection as well as the UAV platforms will be visualized on the RESISTO platform. The usage of existing HMI by Audio/Video Detectors as well as the current RESISTO HMI video players will be used.
- Map visualization: The map visualization will contain information about the Infrastructure, the location of sensors, network assets as well as the visualization of detections.
  - Video Sensors: The location and the field of view of each sensor. In the case of PTZ camera, the field of view will be updated in real-time.
  - Audio Sensors: The location of the sensors as well as the audio coverage. According the type of sensor this will be omni-directional or direct.
  - Airborne Threats Detector: Similar with other sensors, the location and the sector of coverage will be visualized.
  - Visualize of geo-referenced targets/detections. The location of the detected target (from video and radar) will be visualized on the map environment.
  - UAV platform telemetry data: Position and direction of the UAV will be also available on the map environment.
- List of Alerts/Detections: Re-using the RESISTO HMI functionalities, the visualization of a list with generated alerts will be available to the operator.

Business Intelligence (BI) and Analytics: Statistics and network traffic analytics will be available for visualization under the HMI Platform. Following the process of HMI adaptation, existing BI and Network Traffic tools have been adapted and prepared for integration with the HMI.

## 3. PLATFORM INTEGRATION

### 3.1. Introduction

The system integration phase involves installing a first version of the system and putting it into operation. RESISTO is a complex system that uses many components developed and managed by different partners who therefore did not have the possibility of a continuous interaction between them in the development phase. For these reasons, the correct integration of the system is a fundamental and problematic activity that required a considerable effort shared by all the partners involved.

The activity took place in various phases: the type of environment, definition of the necessary resources, preparation of the environment, installation of the components and others. The following chapters describe in detail the activity carried out, the choices made and the results obtained.

### 3.2. Environment design

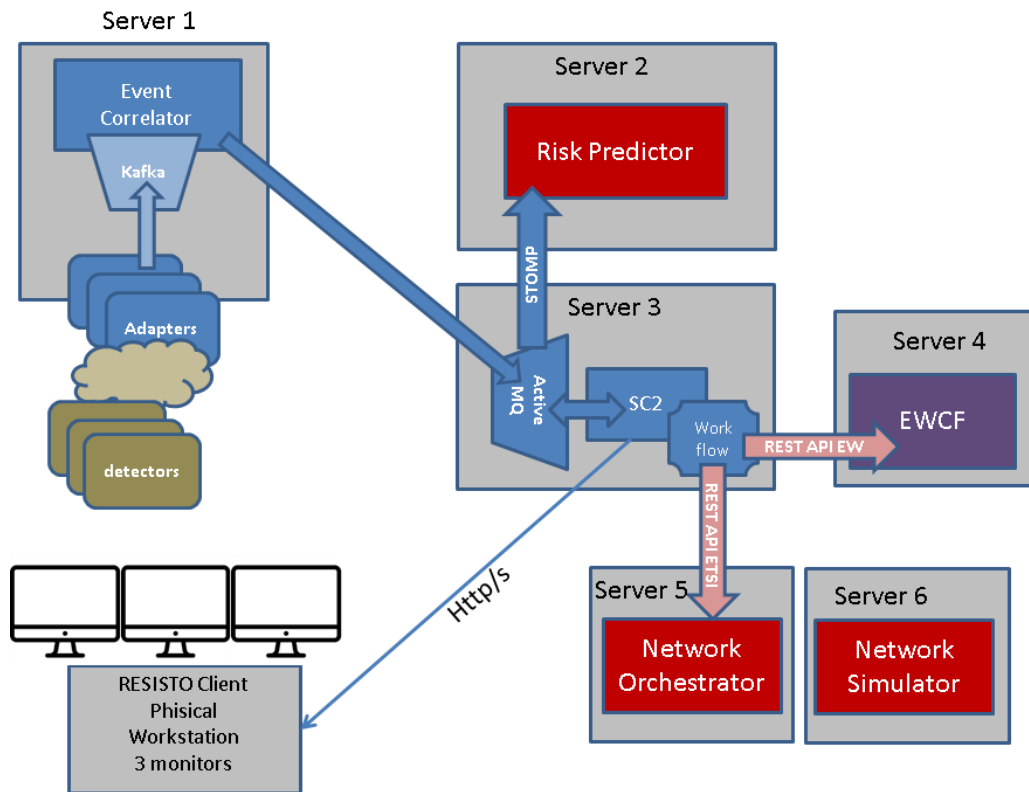
The RESISTO integration environment consists of a series of virtual machines hosted in a cloud-like infrastructure. This infrastructure was made available by the partner Telecom Italia. The cloud service provided for RESISTO is IaaS (Infrastructure as a Service). For some virtual servers, only the virtual machine with on-board operating system was requested, while for others the direct import of the virtual machine to the cloud was made, after format conversion where necessary.

Based on the RESISTO architecture, the environment was designed by evaluating the number of servers needed and the location of the various RESISTO services on the different servers.

This integration environment mainly concerns the "core" side of RESISTO as the detectors and sensors on the field remain located in the various test sites of the network operators. For the Orchestration part, the networks are obviously located at the operators' sites, while a simulator has been installed in the integration environment.

This cloud environment also ensures connectivity with remote sites through secure channels protected by VPN

The scheme of the prepared environment is in **Figure 85**

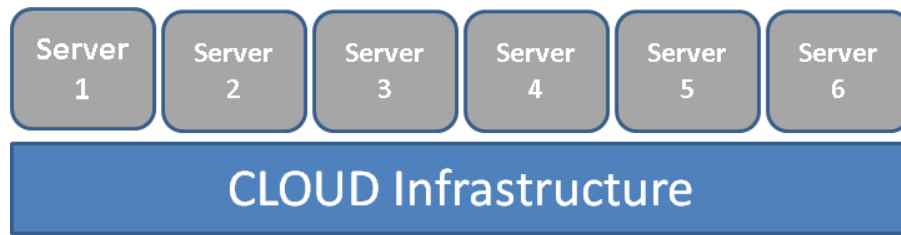


**Figure 85 – Integration Environment**

- **Server 1 – Event Correlator** with Kafka and adapters.
- **Server 2: Risk Predictor**
- **Server 3: SC2**, Workflow manager, Active MQ
- **Server 4 EWCF**
- **Server 5 Network Orchestrator**
- **Server 6 Network Simulator**
- **Client Workstation** (not into the cloud)

The field detectors and subsystems to be monitored in the various use cases remain located at the sites of the network operators but are connected securely.





**Figure 86 – Template for HMI Adaptation requirements per use case**

### 3.3. Evaluation of computing power

An analysis of the computational resources necessary for the correct functioning of the system was made and each partner involved requested the necessary resources for the servers. The result of sizing the servers is as follows:

Server ID	Op. System	Core number	RAM (GByte)	Disk (GByte)
Server-1	Win 10	8 core	16	300
Server-2	Win10	4 core	16	300
Server-3	Win 10	4 core	16	150
Server-4	Ubuntu 18.4	4 core	16	100
Server-5	Ubuntu 18.4	4 core	32	100
Server-6	Ubuntu 18.4	4 core	32	100

### 3.4. Integration work

From the moment when the cloud installation environment was made available, the various virtual servers with the necessary components were installed, as per the scheme described.

Once the individual servers were installed, communication tests were carried out for the various channels envisaged, in particular it was verified that:

- The messages produced by the event Correlator are correctly processed by SC2 and displayed as alarms.
- Risk predictor correctly receives SC2 event and alarm messages and manages them correctly.
- The REST messages sent by SC2 to EWCF, through the workflow manager, are correct and correctly managed by EWCF
- The REST messages sent by SC2 to Orchestrator, through the workflow manager, are correct and correctly managed by the Orchestrator



- For each adapter that can be contacted remotely via VPN, it has been verified that it correctly processes the data provided by the detectors and that it correctly conveys them to the Event Correlator.
- For the use case of Altice Lab it has been verified that the RESISTO orchestrator communicates correctly with the Altice Lab orchestrator for the exchange of messages and commands.

For detectors not reachable from the network, correctness checks were carried out using simulators. In this way it was verified that the core part of RESISTO is complete and correctly functioning.

## 4. CONCLUSION

As described in the previous chapters, the problems faced in the project give rise to the need to design open and flexible solutions also at HMI level, with the prospect of reusing the work done in very different and evolving contexts.

An attempt was made to make the HMI as configurable and expandable as possible. It was imposed, as the only condition for hosted components, to be Web based applications. Work has been done to adapt the interfaces to ensure that they are fairly uniform in appearance, where this has been possible.

For the integration activity, we chose to use a cloud based solution for the RESISTO core part which made the setup of their modules much easier for all partners. For the adapters where possible we have chosen to make them communicate securely with the core through mechanisms such as VPN. This work will greatly facilitate the subsequent part of setup of the final instance for validation. We are confident that these choices will help us even if for the system's dissemination and exploitation initiatives that are scheduled, as it will be possible to make the up and running system available for presentations and promotions of the solution.