

**RESISTO:**

## **D6.2\_ADAPTERS, DSS AND RISK PREDICTOR**



# RESISTO

## D6.2 – ADAPTERS, DSS AND RISK PREDICTOR

<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>	RESISTO_D6.2_200603_01	<b>Version:</b>	1.0
<b>Deliverable:</b>	D6.2	<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

## 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
0.9	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

The RESISTO system integrates with a series of sensors and systems in the field and to do this it must be equipped with a series of adapters that guarantee communication and the correct exchange of data. RESISTO offers a DSS that allows the operator to have a cockpit for monitoring and managing the situation in real time. A series of tools help the user to make the correct choices and with the appropriate timing. The Risk Predictor allows the operator to evaluate the impact of the attack in progress, and to evaluate the effect of the countermeasures.

## CONTENTS

<b>ABBREVIATIONS .....</b>	<b>8</b>
<b>1. INTRODUCTION .....</b>	<b>9</b>
1.1. Deliverable Structure.....	9
1.2. Overview .....	9
<b>2. ADAPTERS.....</b>	<b>10</b>
2.1. SNMP adapter .....	11
2.2. Syslog adapter .....	11
2.3. Audio and Video Detector integration.....	12
2.4. RADIOFILTER, RANMONITOR and IoT Firmware Reliability Sensors integration .....	13
<b>3. DSS.....</b>	<b>15</b>
3.1. Introduction .....	15
3.2. Alarm management .....	15
3.3. Workflow Manager.....	15
3.4. Risk Predictor .....	16
3.5. DSS integrated system.....	16
<b>4. RISK PREDICTOR.....</b>	<b>18</b>
<b>5. NETWORK SERVICES ORCHESTRATOR.....</b>	<b>21</b>
5.1. Catalogue Management Interface.....	22
5.2. LCM Interface.....	22
<b>6. CONCLUSION .....</b>	<b>23</b>

## List of Figures

Figure 1. Kafka based communication interface.....	10
Figure 2. Integration schema for Audio Video Detector .....	13
Figure 3. RADIOFILTER Adapter inside overall architecture .....	14
Figure 4. The architecture of the Risk Predictor from D4.4.....	19
Figure 5. An example of the GUI of the Risk Predictor .....	20
Figure 6 RESISTO Orchestrator overview.....	21

## ABBREVIATIONS

<b>5G</b>	5th generation mobile wireless standards
<b>API</b>	Application Programming Interface
<b>BPMN</b>	Business Process Model and Notation
<b>CSV</b>	Comma Separated Value
<b>DSS</b>	Decision Support System
<b>GIS</b>	Geographic Information System
<b>GUI</b>	Graphical User Interface
<b>IoT</b>	Internet of Things
<b>JSON</b>	JavaScript Object Notation
<b>LCM</b>	Lifecycle Management
<b>MANO</b>	Management and Orchestration
<b>MIB</b>	Management Information Base
<b>OSM</b>	Open Source MANO
<b>QoS</b>	Quality of Service
<b>SLA</b>	Service Level Agreement
<b>SNMP</b>	Simple Network Management Protocol
<b>SOP</b>	Standard Operating Procedures
<b>WP</b>	Work Package



## 1. INTRODUCTION

### 1.1. Deliverable Structure

The deliverable D6.2 is the report of the WP6 related to the activities on Adapters development, definition of the DSS platform and Risk Predictor.

The deliverable comprises 6 sections:

- *Section 1* offers an introductory overview;
- *Section 2* presents the RESISTO Adapters
- *Section 3* presents the DSS component
- *Section 4* presents the Risk Predictor component
- *Section 5* : presents the Network Services Orchestration
- *Section 6* : conclusion of the work

### 1.2. Overview

The document addresses three important aspects of RESISTO: adapters, DSS and Risk predictor. These components allow the system to function correctly as regards the reception of events and the management of related alarms.

The RESISTO system must receive events from a series of detectors. The detectors are of a different nature to each other, and to communicate with the system it is necessary that the data they generate are normalized in a common format that is understandable by the system.

For this reason, suitable adapters have been created that allow the transcoding of data in a format compliant with protocols, in syntactic and semantic terms.

The DSS chapter describes the modality of notification, display and organization of information for the operator and the choices made to optimize the support in the management of alarms from the point of view of the system operator.

In the dedicated chapter 'Risk predictor', this component is described in terms of functionality and utility in the system and it's also shown how this function has been inserted in the specific context of alarm management.

## 2. ADAPTERS

The RESISTO system must communicate with a heterogeneous variety of field sensors and subsystems of a different nature. To avoid the proliferation of adapters, a communication interface to the sensors has been set up, giving the possibility to the various suppliers to send pre-formatted data. This interface is based on messages conveyed by the Apache Kafka broker. For more information you can see: <https://kafka.apache.org/>.

Messages are encoded in JSON standard. JSON is an open standard file format, and data interchange format, that uses human-readable text to store and transmit data objects consisting of attribute-value pairs and array data types (or any other serializable value). It is a very common data format, with a diverse range of applications, such as serving as a replacement for XML in AJAX systems. JSON is a language-independent data format. It was derived from JavaScript, but many modern programming languages include code to generate and parse JSON-format data. For more information you can see: <https://www.json.org/json-en.html>

The detail of this communication interface is described in document “D6.1 – RESISTO Software Architecture”. This decision to expose a general interface for the communication of events to RESISTO will also be useful in the future as any new field subsystem suppliers will be able to integrate with RESISTO without the need for changes to the system core. In addition, the number of adapters developed for RESISTO was contained as many of the consortium partners conformed to this communication interface, limiting the complications and the number of adapters.

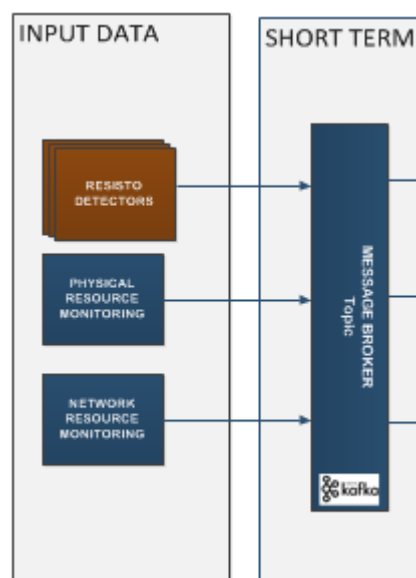


Figure 1. Kafka based communication interface

As can be seen from the figure, the system displays a main integration interface based on the Kafka broker to which an external system can send event data which, if correctly formatted (see D6.1), is processed by the Event Correlator for the generation of the alarms.

For external systems that do not use this native interface, specific adapters must be developed which translate the subsystem protocol into the native interface protocol.

Specific adapters have been developed for sensors or subsystems that cannot be standardized to the interface above. Where possible, we have chosen to base these adapters on standard or widely used protocols to give the product as much generality as possible.

In particular the following adapters have been developed: SNMP adapter, Syslog adapter.

## 2.1. SNMP adapter

SNMP adapter: this adapter manages information in standard SNMP format and is used to receive network diagnostic data in the OTE use case.

Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more.

SNMP is widely used in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organized in a Management Information Base (MIB) which describes the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications.

The data must be sent to the queue in the following CSV format, here is an example:

```
Timestamp,ifInOctets,ifOutOctets,ifOutDiscards,ifInUcastPkts,ifInNUcastPkts  
,ifInDiscards,ifOutUcastPkts,ifOutNUastPkts,ifInErrors  
2019-12-16 18:51:29,36919396,0,0,0,0,0,0,2236378,0
```

## 2.2. Syslog adapter

Syslog adapter: this adapter extracts information from syslog and is used in various RESISTO applications. In particular is used into the use cases of ORO, but not only.

In computing, **syslog** is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity level.

Computer system designers may use syslog for system management and security auditing as well as general informational, analysis, and debugging messages. A wide variety of devices, such as printers, routers, and message receivers across many platforms use the syslog standard. This permits the consolidation of logging data from different types of systems in a central repository. Implementations of syslog exist for many operating systems.

When operating over a network, syslog uses a client-server architecture where a syslog server listens for and logs messages coming from clients.

The data must be sent to the queue in the following in textual format, field are separated by '|' character. Here is an example:

```
CEF:0|SecurityMatters|SilentDefense|3.4.1|mitm_dhcp_sr|DHCP spoofed  
response|Low|externalId\u003d2327153 rt\u003d1421662765312  
src\u003d192.168.12.1 dst\u003d192.168.12.2 spt\u003d dpt\u003d  
proto\u003dUDP app\u003dDHCP in\u003d0 out\u003d0 deviceDirection\u003d  
cs1Label\u003dProfileModule cs1\u003dMITM cs2Label\u003dFEAState cs2\u003d  
cn1Label\u003dAggrAlerts cn1\u003d deviceCustomDate1Label\u003dFEAStart  
deviceCustomDate1\u003d cn2Label\u003dFEADurationSec cn2\u003d  
cs3Label\u003dFieldPath cs3\u003d cs4Label\u003dFieldVal cs4\u003d  
cs5Label\u003dExpVals cs5\u003d msg\u003dPossible MITM attack: the attacker  
responds to a DHCP Request pretending to be an existing DHCP server. This  
is a DHCP spoofed server alert
```

### 2.3. Audio and Video Detector integration

Video and Audio sensors are widely used in surveillance operations and protection of critical infrastructures. Intelligence algorithms are applied in audio and video streams for the real-time detection of events for the early identification of illicit activity. Both Video Analytics Component (VAC) and Audio Analytics Component (AAC) are processing the video/audio streams respectively and produce events with abnormal behavior in the form of JSON messages.

The main content of the event is the type and information about the detected event. Also, the events include geo-referenced information about the sensors and the detected targets. Additionally, the message is enhanced with timing information about the occurred time, the sequence of frame, duration of event, etc.

The Audio and Video detectors will be integrated with the RESISTO platform through the RESISTO KAFKA broker. As depicted in the figure below, the VAC and AAC are the main computational components of the Intelligence Surveillance System while the local storage of events is handled by a local database system.

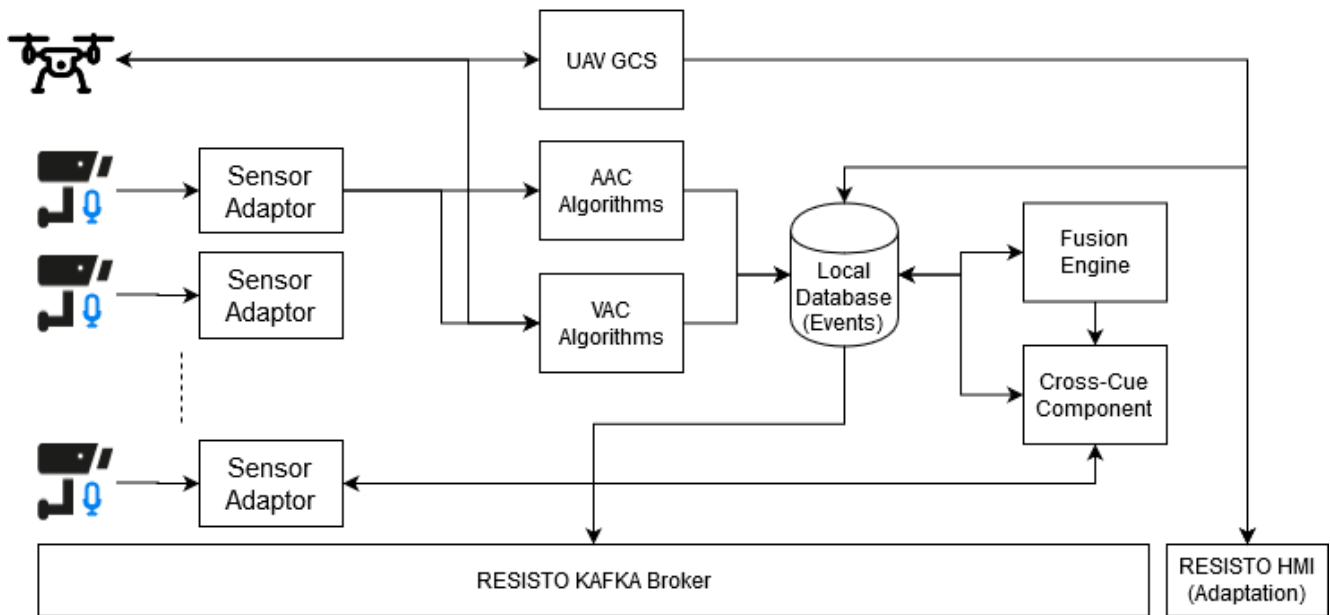


Figure 2. Integration schema for Audio Video Detector

For the integration with RESISTO platform, a KAFKA adaptor is implemented and embedded in the local database system where the communication is established.

## 2.4. RADIOFILTER, RANMONITOR and IoT Firmware Reliability Sensors integration

RADIOFILTER sensors are used to detect WLAN-based threats and attacks at telecom critical infrastructures. The sensors monitor data-link traffic parameters and relay this information to a central node where the information is aggregated and processed to detect threats and attacks. When these events are detected, this information is fed to the RADIOFILTER adapter which is in charge of converting the events and its related parameters into a JSON message following the IDEA format and publish the message to the KAFKA broker.

RANMONITOR sensors are used to detect threats and attacks to the LTE Radio Access Network (RAN). The sensors monitor the radio spectrum as well as the downlink control channel information and relay this to a central node where the information is aggregated and processed to detect threats and attacks. In a similar way to RADIOFILTER, when the events are detected the information is fed to the RANMONITOR adapter which is in charge of converting the events and its related parameters into a JSON message following the IDEA format and publish the message to the KAFKA broker.

Likewise, IoT firmware modification or other related events affecting firmware reliability are detected by the IoT Firmware Reliability Sensors and this information is fed to the Firmware Reliability adapter which is in charge of converting the events and its related parameters into a JSON message following the IDEA format and publish the message to the KAFKA broker.

Therefore, the idea behind the three adapters developed for these three detectors follows a similar, normalized pattern to integrate with the RESISTO platform. In the figure below, a general diagram is depicted for RADIOFILTER adapter.

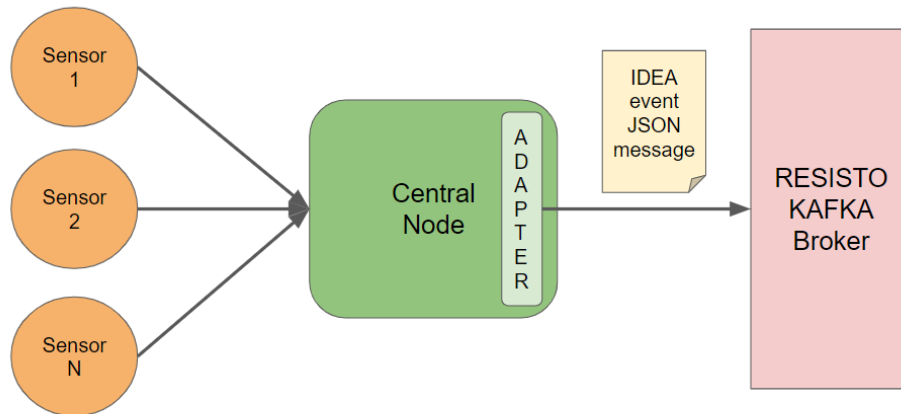


Figure 3. RADIOFILTER Adapter inside overall architecture

## 3. DSS

### 3.1. Introduction

A decision support system (DSS) is an information system that supports business or organizational decision-making activities. DSSs serve the management, operations and planning levels of an organization (usually mid and higher management) and help people make decisions about problems that may be rapidly changing and not easily specified in advance. Decision support systems can be either fully computerized or human-powered, or a combination of both.

The RESISTO DSS is made by:

- Alarm management Dashboard.
- Workflow manager
- Risk predictor

These tools combined into a single HMI can help the RESISTO operator to manage and resolve the alarm situations occurred taking action and monitoring the situation in terms of consequences and cascade effects of an alarm.

### 3.2. Alarm management

The alarm Management dashboard is described in detail into the D6.3 document, here, the usefulness of this component for the purpose of supporting the operator is highlighted from a functional point of view.

When an alarm arises, the system displays it on the operator interface in a clear and evident way, accompanied by significant data for its management such as: type of alarm, sensor that originated it and priority. It is possible to view all the significant data of the event or events that led to the emergence of an alarm situation. The alarm, where this is significant, can be geo-referenced and displayed on a GIS. The onset of the alarm is accompanied by an audible signal that attracts the operator's attention. It is possible to automatically open information windows when an alarm occurs. These information windows contain specific information of the alarm which are not represented or represented in the general alarm data such as: video flows relating to the source of the alarm: if for example a sensor is monitored through a camera, it is possible to view its video flow, or information pages relating to the specific alarm or sensor data that generated it. These additional information forms are configurable so the system is able to manage ever new situations without changes at the core level.

The RESISTO operator therefore, at the onset of the alarm, immediately has all the necessary information available.

### 3.3. Workflow Manager

The use of a workflow engine is used to manage the alarm. This component allows you to guide the operator in alarm management to carry out all the actions foreseen during the workflow design phase.

The workflow component and RESISTO workflows have been described in detail in document D5.3.



In this document, attention is focused on the “Dashboard – Workflow - Risk Predictor” complex, seen as part of a single DSS for the operator.

In this DSS context, the Workflow manager has the most operational role as it guides the operator in the execution of the tasks foreseen for the type of alarm being managed. Some RESISTO Workflows provide for conditional choices and therefore different paths according to considerations made by the operator through data analysis and simulations carried out with the help of the Risk Predictor. In particular, the Risk predictor assesses the cascade impact and therefore also the global damage to the infrastructure following the attack in progress. This makes the user able to assess whether some countermeasures (among those envisaged in the Workflow design phase) are more effective and appropriate than others. It is clear that these choices made by the operator are among those envisaged in the workflow design phase which is in any case consistent with the management process and protocol established in the workflow design phase.

The workflow manager allows a lot of freedom and configurability during the design phase and allows to represent, according to the BPMN standard, the operating procedures established against the alarms or attacks foreseen. The workflows are clearly expandable and editable by the managers during the design phase. During execution, the procedures must be strictly followed, and this is precisely the task of the workflow manager component.

In practice, the workflow manager's task is to implement Standard Operating Procedures (SOPs) that allow for correct and rigorous management of alarm situations.

### 3.4. Risk Predictor

The Risk Predictor component is described in detail into the next section.

From the DSS point of view, the risk predictor is an important component as it helps the operator in making the correct decision as it provides detailed information on the model of the system to be managed complete with all its significant components. It also assesses the cascade effect of an alarm on all system components. All this information is not clear from the alarm management component alone. For example, in some situations, provided by the Workflows, the operator chooses between two or more actions to perform the most appropriate one based on the situation and impact of the alarm assessed using the Risk predictor. In any case, the operator is guided by the workflow which indicates the succession of the tasks to be performed during the alarm management and until its closure. All the operations performed are tracked and can produce reports visible to authorized users. For the tasks to be carried out manually by the operator, he declares and assumes responsibility for having performed them and everything is traced by the system.

### 3.5. DSS integrated system

DSS consists of a system consisting of the components described above but in a highly integrated context. These are not three distinct tools displayed in a single interface, but these components communicate with each other and are synchronized so that when an operation is made the others also receive notifications and update themselves.

In particular, the alarms notified to the dashboard are also sent to the Risk Predictor which shows the cascade impact. When the alarm is managed, the actions carried out are notified to the risk predictor who updates his situation in near real time throughout the alarm management phase, until closing.



Below is an example of DSS operation:

- When an alarm arises, the operator displays the icon and general data in the Alarm tray on the interface,
- an audible alarm is played which continues until the operator mutes it.
- The operator can view specific alarm data through additional pages that are automatically displayed on the interface.
- Displays the data of the events that triggered the alarm
- View the impact of the alarm on system components using the Risk Predictor
- It manages the alarm by carrying out all the tasks that are presented to it by the workflow manager component
- Monitors the evolution of the alarm and countermeasures carried out by looking at the Risk predictor.
- Once all the tasks foreseen by the workflow have been carried out, the alarm is closed.

## 4. RISK PREDICTOR

The Risk Predictor attempts to determine the effects and implications of adverse events (i.e., failures, cyber threats or natural disasters) on the comparison scenario being considered.

The Risk Predictor increases infrastructure operators' understanding of the situation: it assesses the effects on the infrastructure of adverse incidents. We intend faults, failures or ongoing cyber-attacks for adverse incidents. Each CI (Critical Infrastructure) is divided into components (such as devices and equipment), services and also the so- called holistic entities. The model's abstraction level depends on the purpose and the physical process knowledge.

The Risk Predictor exploits CISIAPro 2.0 simulator, as already described in D4.4 "Complete propagation Analysis". CISIAPro is a simulator based on agents, in which each agent has the same structure. The agents are connected in a directed graph. Each agent collects upstream resources and failures and delivers downstream resources and failures. A resource is a product, service or data generated and/or consumed by the agent, which is defined as an entity in CISIAPro 2.0.

The capacity to generate resources is illustrated by the definition of operative level, depending on the availability of provided resources, the occurrence of faults and the entity's own functionality. An entity's operative level is the capacity to do its job correctly, delivering the correct amount of necessary goods/services and the level of failure/malfunction within each dimension of interdependency that can be observed during its process.

The operative level is synonymous with a risk metric: the operational level is higher, and the risk associated with a component or service is less. CISIAPro 2.0 has been exploited for the Risk Prediction.

It is important to note that the Risk Predictor has some groundbreaking features with respect to other simulators of interdependency:

- The Risk Predictor, as shown early in the FP7 MICIE project, can operate in a distributed model with only partial sharing of information, retaining a share view of the overall structure.
- The Risk Predictor can manage cyber-attack details and more precisely can determine the impact of cyber-attacks on physical infrastructures (as done during FP7 CockpitCI project and H2020 ATENA project). In an interdependence case study, no other simulator can consider faults together with cyber-attacks.
- The Risk predictor is quick enough to operate on close real-time connected to control centers to collect the exact condition on the infrastructure's physical components.
- The Risk Predictor assesses services as primary indicators to present to operators. Services are aggregated metrics for critical components, measures already used by operators such as the amount of served consumers or the Service Level Agreement (SLA) to other infrastructures.

The Risk Predictor has an SQL database as a key element which stores information on the design phase and on the execution phase, as represented in Figure 4. The design phase is related to the modeling activities: definition of agents, their interconnections and their behaviors. This phase is realized offline, to model infrastructures at the proper abstraction's level. All the information created during the design phase is stored into the database.

The execution phase is the run-time moment: Risk Predictor runs taking information on the actual state of the monitored infrastructure. The inputs for the Risk Predictor are the information coming from the alarm management and from the workflow. From the alarm management, the Risk Predictor

receives data on the actual situation: failures, and possible threats. From the workflow, the Risk Predictor receives information on the completed actions on the system

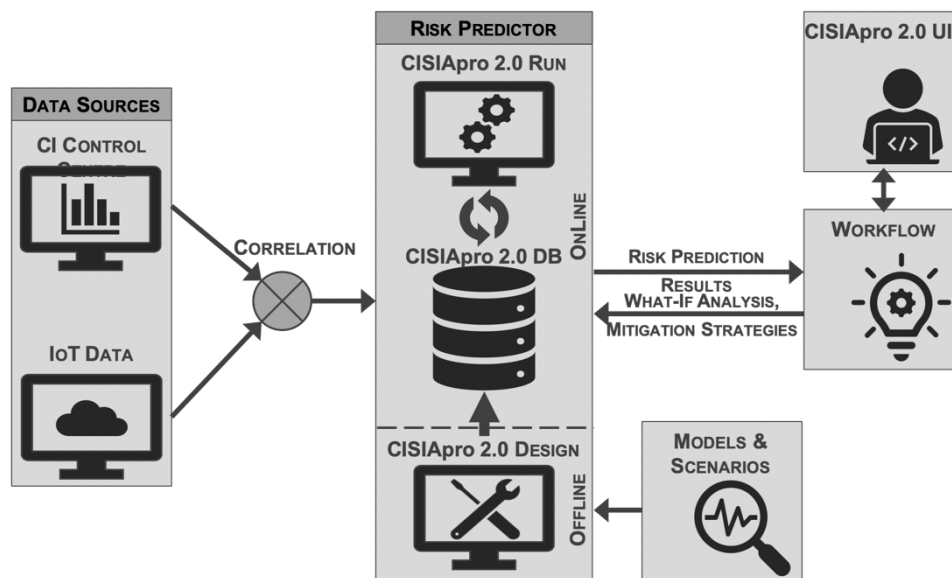


Figure 4. The architecture of the Risk Predictor from D4.4

The Risk Predictor has a web-based interface to display to operator the possible consequences of actual events. This web-based interface must be as much as possible similar to the operator's one. The Risk predictor has a graphical interface, to display additional information to the operator. An example of the Graphical User Interface (GUI) of the Risk Predictor is depicted in Figure 5. In this case, a telecommunication network is depicted. The colors represent the predicted value of the operative level of the entities. The right sidebar contains two kind of data:

1. In the upper side, the graphics details the historical values of the Quality of Service (QoS) of the entire telecommunication infrastructure for assessing resilience metrics, and of some key components as such MPLS networks and the actual state of the buildings.
2. In the below part, the information is related to the single object where you click, describing the foreseeing values of the state variables.

The upper side of the GUI contains a set of gauges representing the services we considered in the modeling phase.

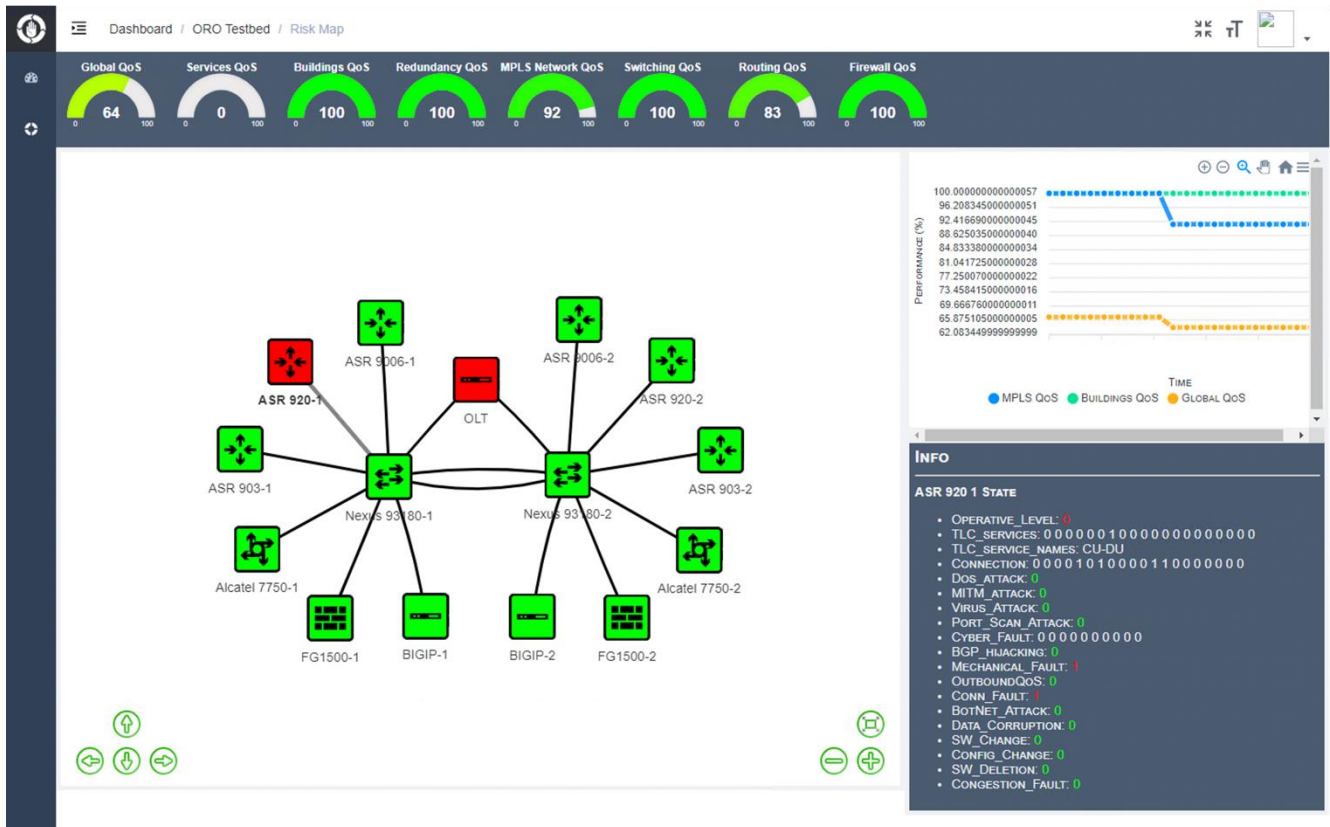


Figure 5. An example of the GUI of the Risk Predictor

## 5. NETWORK SERVICES ORCHESTRATOR

RESISTO Network Services Orchestration application manages 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 (North Bound Interface), a subset of ETSI Open Source MANO (OSM)'s NBI ([https://osm.etsi.org/wikipub/index.php/NBI\\_API\\_Description](https://osm.etsi.org/wikipub/index.php/NBI_API_Description)) compliant to ETSI NFV SOL005.

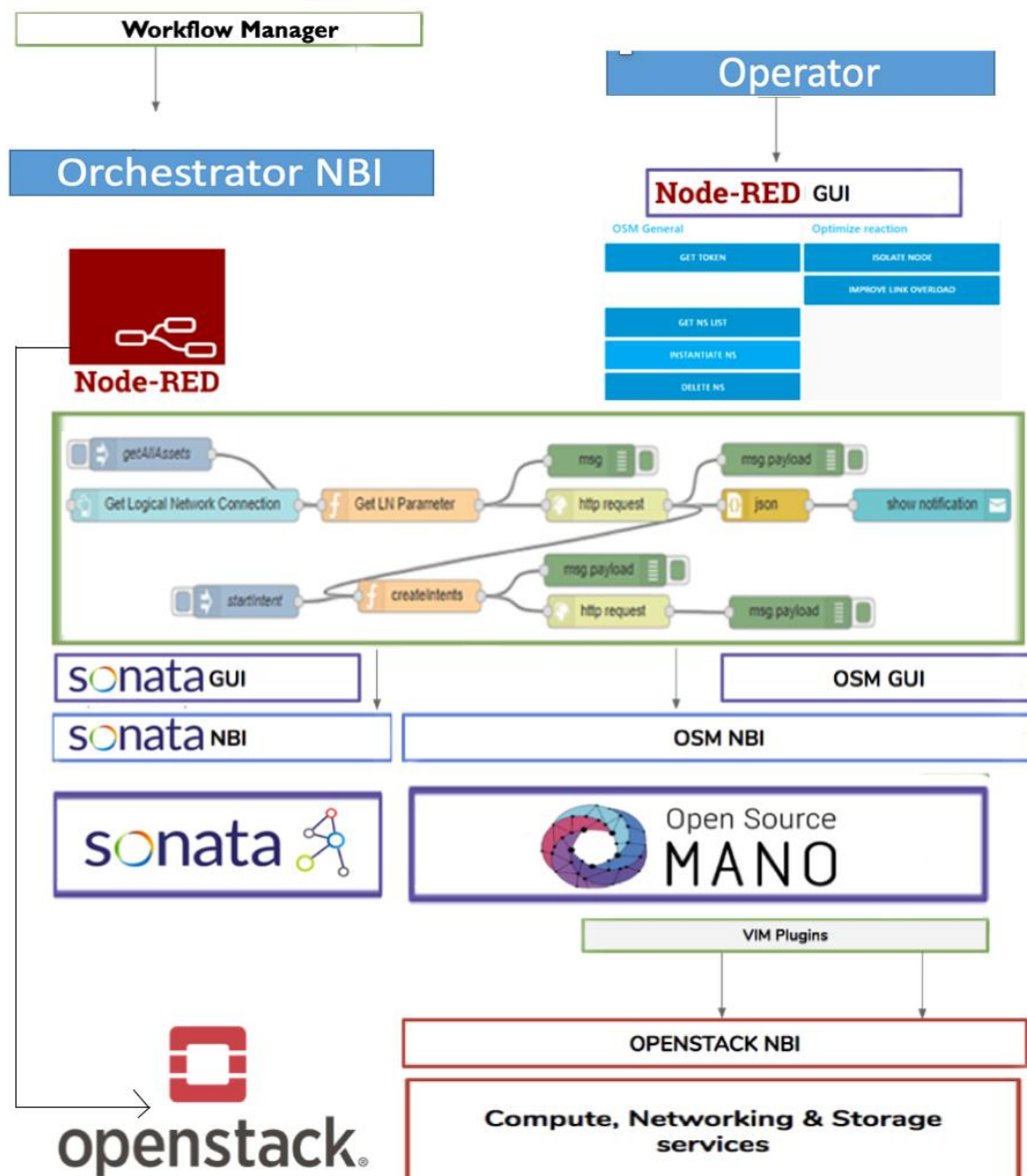


Figure 6 RESISTO Orchestrator overview

For interaction with OSM it acts as an API Gateway with the possibility (for some API) that operator can accept/reject request through NBI.

For interaction with Sonata it also map some OSM APIs with correspondent Sonata APIs (<https://github.com/sonata-nfv/tng-api-gtw>) in order to use same syntax as OSM, that will probably become an ETSI standard also for these not yet included on NFV SOL005.

## 5.1. Catalogue Management Interface

The remainder of this section provides the relevant subset of the SONATA API.

The Catalogue Management allows the interactions with the database of the Service Platform to get Descriptors for NSs (NSDs), as well as for Network Slice Templates (NSTs). OSM and SONATA also store Packages in the Catalogue, which are basically an envelope that contains the configured VNFDs and NSD that can be on-boarded on the virtual infrastructure.

Feature	OSM API	Sonata Mapped API	Description
<b>Services Catalogue Management</b>	/osm/nsd/v1/ns_descriptors	/son/nsd/v1/ns_descriptors Mapped to /api/v3/services	Query information about NSs in the Catalogues
<b>Slices Catalogue Management</b>	/osm/nst/v1/netslice_templates	/son/nst/v1/netslice_templates Mapped to /api/v3/slices	Query information about NST in the Catalogues

Table 1: RESISTO Orchestrator APIs: Catalogues Management

## 5.2. LCM Interface

The Lifecycle Management (LCM) capabilities allow the instantiation of instances of NSs and NSIs from NSDs and NSTs, respectively. Other operations may also be included, like the termination, scaling, migration, etc.

The request of LCM operations is performed using the base APIs described in following table. The path and body include the details of the LCM operation to be requested (list, instantiation, termination, etc.) and the target artefacts (NSs, Network Slices).

Feature	OSM API	Sonata Mapped API	Description
<b>LCM Requests on NS Instances</b>	/osm/nslcm/v1/ns_instances	/son/nslcm/v1/ns_instances Mapped to /api/v3/requests	Issue and Query Requests for LCM operations on NSs
<b>LCM Requests On NetSlice Instances</b>	/osm/nsilcm/v1/netslice_instances	/son/nsilcm/v1/netslice_instances Mapped to /api/v3/requests	Issue and Query Requests for LCM operations Slices

Table 2: RESISTO Orchestrator APIs: LCM Requests Management.

## 6. CONCLUSION

The document highlighted some important aspects of RESISTO that were designed with the aim of making it an effective system in contrasting the attacks treated but at the same time flexible and expandable to cope with attacks not directly addressed in the project.

By analyzing three aspects: adapters, DSS and Risk Predictor, it was intended to highlight:

For adapters, the possibility of integrating detectors, sensors and subsystems of various types through adapters, the possibility of receiving data from the outside in various ways already provided in order to limit the proliferation of the number of adapters with a view to reusing the developments made.

For the Risk Predictor, it was intended to describe this component in its potential for modeling the most diverse systems and the ability to evaluate the cascade effects of a problem on the other components of the system.

The DSS intended to highlight the integration capacity of various tools aimed at maximizing the clarity, completeness and usefulness of the information provided and the effectiveness of user operations.