

**RESISTO:**

## **D5.3\_INTERIM WORKFLOW DEFINITION AND EMERGENCY WARNING COMMUNICATION FUNCTION**



# RESISTO

## D5.3 – INTERIM WORKFLOW DEFINITION AND EMERGENCY WARNING COMMUNICATION FUNCTION

<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_D5.3_191218_01	<b>Version:</b>	1.0
<b>Deliverable:</b>	D5.3	<b>Date:</b>	18/12/2019
		<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>	Marco CARLI (RM3)
<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
Giuseppe Celozzi, Rosa Catapano	TEI	Expert, Senior Developer

## 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	04/06/2019	All	All	Draft ToC
0.2	15/10/2019	All	All	Release for SAB Assessment
1.0	18/12/2019	All	All	Final Release

## COPYRIGHT STATEMENT



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

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

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

## PROJECT CONTACT



LEONARDO

Via Puccini 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 project intends to deal with a series of combined cyber-physical attacks that require appropriate procedures for analysing and managing the anomalous situation. These procedures can be automatic and manual but must be coded and managed appropriately. This Deliverable describes the procedures adopted to be implemented with workflow engines adhering to the BPM 2.0 standard. Furthermore, the Emergency Warning Communication Function (EWCF) component is described, which enables an intervention team to be activated in the event of an alarm situation.

## CONTENTS

<b>ABBREVIATIONS .....</b>	<b>9</b>
<b>1. INTRODUCTION .....</b>	<b>10</b>
1.1. Deliverable Structure.....	10
<b>2. THE RESISTO WORKFLOW ENGINE.....</b>	<b>11</b>
2.1. BPMN Standard .....	11
2.2. Workflow Engine .....	11
2.3. Workflow Management of RESISTO platform.....	15
2.4. Guideline for RESISTO Workflow design.....	17
2.5. Ethical and social implications.....	19
<b>3. WORKFLOW DEFINITION FOR RESISTO PROJECT .....</b>	<b>20</b>
3.1. British Telecom use cases.....	20
3.1.1. Disruption of major sporting event.....	20
3.2. TIM use cases .....	21
3.2.1. Tampering on files containing sensitive data after physical access .....	21
3.2.2. Tampering detection change of file creation time by a process .....	22
3.2.3. Hardware configuration system change .....	23
3.2.4. Disaster Response and Recovery .....	24
3.2.5. Power loss .....	25
3.2.6. Temperature .....	26
3.2.7. Data exfiltration.....	27
3.3. Orange Romania use cases .....	28
3.3.1. Internal DoS attack .....	29
3.3.2. DDoS attack from inside botnet:.....	29
3.3.3. DDoS attack on peering border.....	30
3.3.4. Routing Table Poisoning on core .....	31
3.3.5. BGP Hijacking.....	32
3.3.6. External Network Scanning Lateral Movement.....	33
3.3.7. Detection connectivity to botnets from internal network.....	33
3.4. OTE use cases .....	34
3.4.1. Core Network Failure on Physical & Cyber Attacks.....	34
3.4.2. Earthquake Multiple Terrorist Attacks.....	36
3.5. Altice Lab use cases .....	37
<b>4. EMERGENCY WARNING COMMUNICATION FUNCTION .....</b>	<b>39</b>
4.1. EWC Service REST interface .....	39

4.2. Messaging framework .....	40
4.3. Localization.....	40
4.4. IOT framework integration .....	40
4.5. Android application .....	41
5. CONCLUSION .....	42

## List of Figures

<b>Figure 1:</b> Activity tool stack.....	12
<b>Figure 2:</b> Example of BPMN process.....	13
<b>Figure 3:</b> Start node .....	13
<b>Figure 4:</b> End node.....	13
<b>Figure 5:</b> User Task.....	14
<b>Figure 6:</b> Script Task.....	14
<b>Figure 7:</b> Exclusive Gateway.....	14
<b>Figure 8:</b> Parallel Gateway .....	15
<b>Figure 9:</b> Example of user tasks .....	16
<b>Figure 10:</b> List of Completed tasks .....	16
<b>Figure 11:</b> Script tasks invoking EWCF and Network Orchestrator .....	17
<b>Figure 12:</b> Multicast stream error process .....	21
<b>Figure 13:</b> Tampering process.....	22
<b>Figure 14:</b> Time Creation change process.....	23
<b>Figure 15:</b> Hardware configuration change process .....	24
<b>Figure 16:</b> Disaster Response process.....	25
<b>Figure 17:</b> Power loss process .....	26
<b>Figure 18:</b> Temperature unacceptable process .....	27
<b>Figure 19:</b> Data Exfiltration process.....	28
<b>Figure 20:</b> Internal DoS process.....	29
<b>Figure 21:</b> DDoS process .....	30
<b>Figure 22:</b> DDoS peering border process .....	31
<b>Figure 23:</b> Routing table poisoning process.....	32
<b>Figure 24:</b> BGP Hijacking process.....	32
<b>Figure 25:</b> External Network Scanning on intrusion process.....	33
<b>Figure 26:</b> Connectivity to botnet from internal network process.....	34
<b>Figure 27:</b> Network Cyber Physical Attack process .....	35
<b>Figure 28:</b> Earthquake alarm process.....	37
<b>Figure 29:</b> Altice Lab Use case workflow.....	38
<b>Figure 30:</b> EWC function .....	41



## ABBREVIATIONS

<b>5G</b>	5th generation mobile wireless standards
<b>API</b>	Application Programming Interface
<b>BPMN</b>	Business Process Model And Notation
<b>DDoS</b>	Distributed Denial of service
<b>DoS</b>	Denial of service
<b>EWCF</b>	Emergency Warning Communication Function
<b>LDO</b>	Leonardo SpA
<b>NSP</b>	Network Service Provider
<b>NSSP</b>	Network Slice Subnet Providers
<b>ORO</b>	Orange ROmania
<b>WF</b>	Workflow
<b>WP</b>	Work Package

## 1. INTRODUCTION

The RESISTO project intends to deal with a series of Cyber-physical attacks that require appropriate procedures for analysing and managing the anomalous situation.

In order to cope with a combined Cyber-physical attack, it is necessary to have appropriate anomaly management analysis tools that involve multiple entities belonging to the system. These entities can be network elements, software hardware, physical security devices, operating personnel and others.

To cope with the combined attacks of RESISTO it is necessary to implement the appropriate mitigation actions. These actions must be managed according to procedures defined for the different types of attacks. This document will describe the mitigation procedures guided through workflows. These procedures can be automatic and manual but must be coded and managed appropriately. This Deliverable describes the procedures adopted to be implemented with workflow engines adhering to the BPM 2.0 standard.

Furthermore, the Emergency Warning Communication Function (EWCF) component is described, which enables an intervention team to be activated in the event of an alarm situation.

### 1.1. Deliverable Structure

The deliverable D5.3 is the report of the WP5 related to the activities performed in T5.4: "Workflow definition" and T5.5: "Emergency Warning Communication".

The deliverable comprises 4 sections:

- *Section 1* offers a brief introductory overview;
- *Section 2* Presents the RESISTO workflow management engine
- *Section 2* presents the workflows designed for RESISTO Project
- *Section 3* presents the Emergency Warning Communication Function
- *Section 4* presents the conclusion of the work

## 2. THE RESISTO WORKFLOW ENGINE

This chapter describes the procedures adopted to deal with cyber-physical attacks that are being studied in the RESISTO project. The result of this document is based on what emerged from the analysis of WP2 use cases and WP5 D.5.1 countermeasures that are the basis of the design of these workflows.

LDO SC2 framework shall be adapted to collect automatic and manual reaction strategies and interact with communication infrastructure and operators. The Workflow Management will interact with the Software Defined Security System, as automatic reconfiguration of the ICT network, with the Decision Making System, as guide for supply operations, and with the cyber-security security response, for cyber physical incidents will not aim at reducing only the overall risk of cyber, physical or cyber-physical targets being breached, but they will focus on preferentially minimizing the highest possible damage that can be inflicted by adversaries.

### 2.1. BPMN Standard

The RESISTO Workflows are designed and managed by a Workflow engine based BPMN

The "Business Model Process And Notation" is a standard for the modelling of business processes that provides a graphical representation of the processes based on flow diagrams similar to the activity diagrams used in the UML. The objective of BPMN is to provide support to the management of business processes both for "technical" users and end users through a notation that is intuitive but also able to represent complex processes. The main objective of BPMN is to provide a standard notation that is easily understandable to:

1. Users who create the process
2. Developers responsible for implementation
3. Users who manage and monitor the execution of the process

This document will always refer to version 2.0 of the standard. For the standard Detail see <https://www.omg.org/spec/BPMN/2.0/>

### 2.2. Workflow Engine

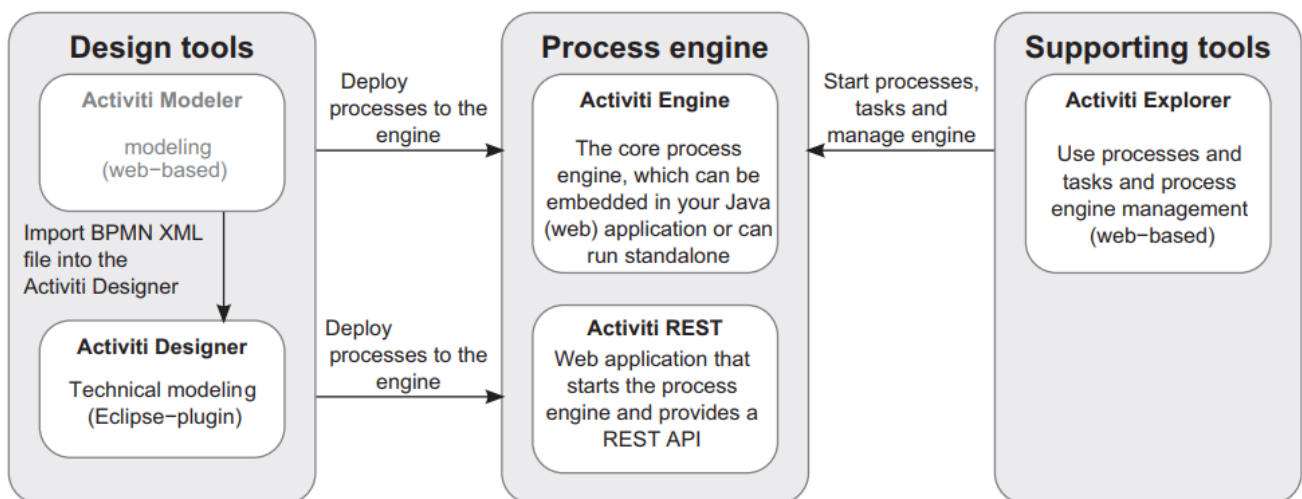
RESISTO project workflow engine is based on a FOSS implementation of the BPMN standard named Activiti.

Activiti is an open source Business Processing Model and Notation (BPMN) 2.0 process engine framework that provides an environment for running your business and technical processes. Activiti provides much more functionality than simply running BPMN 2.0 processes in a rock-solid way. For details see the official product documentation: <https://www.activiti.org/>

Activiti project contains a couple of tools in addition to the Activiti Engine. Figure XX shows an overview of the full Activiti tool stack. Let's quickly walk through the different components listed in figure 1.1. With the Activiti Modeler, business and information analysts are capable of modelling a BPMN 2.0- compliant business process in a web browser. This means that business processes can easily be shared—no client software is needed before you can start modelling. The Activiti designer is an Eclipse-based plugin, which enables a developer to enhance the modelled business process into a

BPMN 2.0 process that can be executed on the Activiti process engine. You can also run unit tests, add Java logic, and create deployment artifacts with the Activiti Designer. In addition to the design tools, Activiti provides a number of supporting tools. With Activiti Explorer, you can get an overview of deployed processes and even dive into the database tables underneath the Activiti process engine.

The **Figure 1** shows the Activiti tool stack: in the center, the Activiti process engine, and on the right and left sides, the accompanying modeling, design, and management tools. The grayed-out components are add-ons to the core Activiti framework



**Figure 1: Activity tool stack**

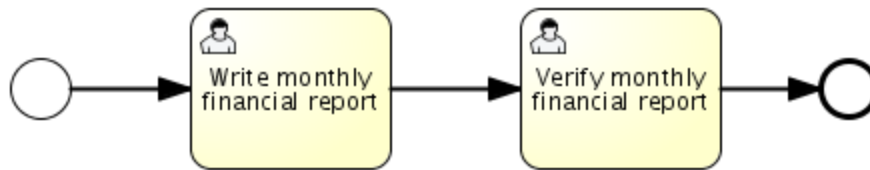
A process is represented by an XML file:

```

<definitions xmlns="http://www.omg.org/spec/BPMN/20100524/MODEL"
  xmlns:activiti="http://activiti.org/bpmn" targetNamespace="Examples">
  <process id="myProcess" name="My First Process">
  </process>
</definitions>
  
```

Within the "process" element you will find the information necessary for the execution of a business process. Through the process designer it will be possible to graphically represent these processes.

An example of a process resembles what is shown in the following **Figure 2**:



**Figure 2:** Example of BPMN process

Here you can identify four elements:

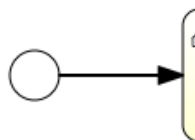
- Process start event (left circle)
- Two "tasks" that must be executed in sequence by a user
- End of process event (circle to the right with thicker border)
- Execution flow represented by the arrows connecting the elements.

The process designer tool integrated into the platform was used for the design of RESISTO workflows. It is directly derived from the Activiti native tool: Activiti Modeller which is a web-based application.

The detailed description of the tool is outside the scope of the document and therefore we refer you to the specialized documentation (e.g. <https://www.activiti.org/userguide/>) but here the main basic components used for the design of RESISTO workflows are described.

### Start process

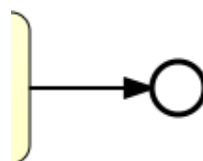
The element that define the start of a process



**Figure 3:** Start node

### End Process

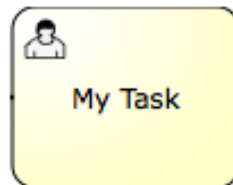
The element defines the end of a process when the process encounters this component the execution ends.



**Figure 4:** End node

### User Task:

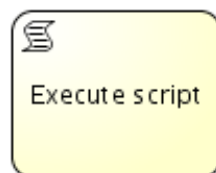
A "user task" is used to model work that needs to be done by a human actor. When the process execution arrives at such a user task, a new task is created in the task list of the user(s) or group(s) assigned to that task.



**Figure 5:** User Task

### Script Task:

A script task is an automatic activity. When a process execution arrives at the script task, the corresponding script is executed.



**Figure 6:** Script Task

### Exclusive Gateway

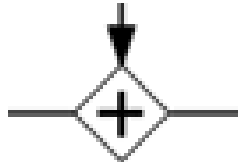
An exclusive gateway (also called the *XOR gateway* or more technical the *exclusive data-based gateway*), is used to model a **decision** in the process. When the execution arrives at this gateway, all outgoing sequence flow are evaluated in the order in which they are defined. The sequence flow which condition evaluates to true (or which doesn't have a condition set, conceptually having a 'true' defined on the sequence flow) is selected for continuing the process.



**Figure 7:** Exclusive Gateway

## Parallel Gateway

Gateways can also be used to model concurrency in a process. The most straightforward gateway to introduce concurrency in a process model, is the **Parallel Gateway**, which allows to "fork" into multiple paths of execution or "join" multiple incoming paths of execution.



**Figure 8:** Parallel Gateway

## 2.3. Workflow Management of RESISTO platform

In this paragraph will be described the use of workflow engine into the RESISTO platform. The workflow engine of RESISTO platform is used for alarm management to guide the RESISTO user to correctly manage every type of alarm provided by the system.

For the correct alarm management, we have to define at least a workflow for each alarm type.

The RESISTO platform can allow the assignment of a workflow for each alarm type and each status of the alarm.

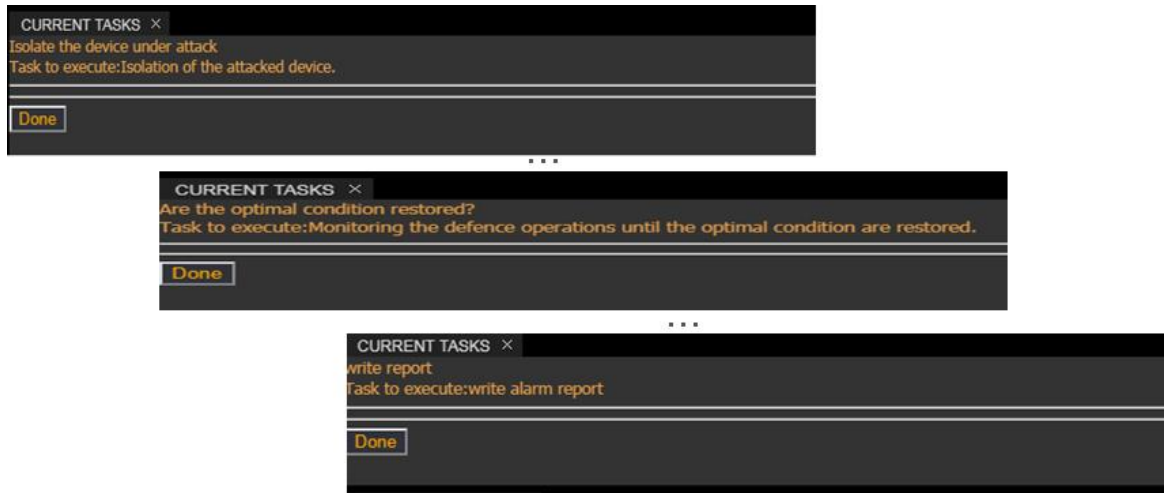
The alarm status can be:

- **NEW:** an active not yet managed by the user
- **MANAGED:** an alarm took in charge by a user to take action in order to resolve the situation
- **CLOSED:** an alarm resolved and closed by the user

The RESISTO platform allows manual tasks to be entered only in workflows associated with the MANAGED status. Workflows associated with the NEW and CLOSED status must contain only automatic tasks

During the execution of the workflow the tasks configured in the pre-established order and according to the conditions set will be invoked.

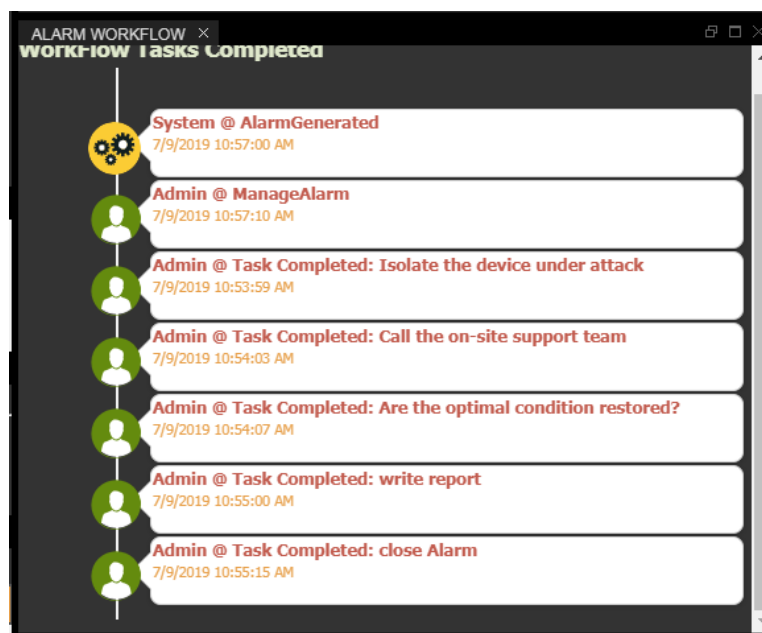
Script-based automatic tasks will be transparent to the user. Instead, manual tasks will be presented to the user as forms that will appear in the correct sequence set by the workflow. The operator will have to perform them all before closing the alarm.



**Figure 9:** Example of user tasks

The tasks already performed are shown on the HMI as in

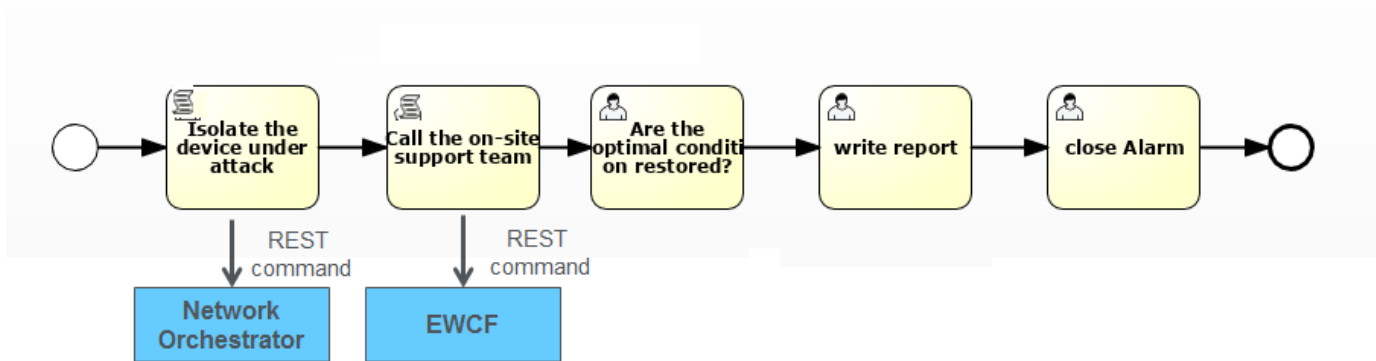
**Figure 10:**





**Figure 10: List of Completed tasks**

The automatic tasks are mostly based on scripts for example JavaScript and they can call external system as EWCF or Network orchestrator using REST protocol.



**Figure 11: Script tasks invoking EWCF and Network Orchestrator**

## 2.4. Guideline for RESISTO Workflow design

The correct design of a workflow must take into account various factors and problems. The workflow has the characteristic of being very flexible in configuration but rigid in execution therefore all the possible actions at runtime must have already been foreseen in the configuration phase it is necessary to foresee and verify the following properties:

- **Correctness:** the workflow must guide the operator correctly and limit as much as possible the possibility of erroneous actions that could endanger the monitored systems.
- **Sequence:** in a workflow the sequence of operations is very important and must be foreseen in the design phase. It is not possible to change the task order at runtime, if a task is not executed it is not possible to perform other tasks subsequent to it and then proceed to close the alarm.
- **Performances:** it is necessary to consider the possible duration of the tasks to be carried out since especially the manual tasks have variable execution times and tend to be longer than the automatic ones. Where possible it is better to put the automatic tasks of the manual ones first unless there are direct dependencies to be respected. The automatic tasks must not contain infinite loops and timeouts that are too long to not compromising the performances.
- **Resilience:** a definition of resilience say: *"the capacity of a system to absorb disturbance and re-organize while undergoing change so as to still retain essentially the same function, structure, identity, and feedbacks"*. Attack mitigation actions are designed to ensure (or maximise) system resilience, this means that in the face of an attack of a certain importance the system will inevitably undergo an attack that will temporarily degrade its performances but mitigation actions tend to have it reorganized, either independently or with the help of humans (operator), in a way to maintain a certain level of functionality in a transitory period until the optimal functionality of the system is restored. In some cases, it is expected and provided that some features are not available or are degraded. However, the countermeasures put in place must ensure that the system is largely able to "absorb the shock"

The workflow design takes into account the countermeasures to be implemented which have been described in the document: *D5.1 - Countermeasures Draft Definition*.

In particular, workflows are made to the “Respond” and “Recovery” part of the countermeasures. The countermeasures document lists the main countermeasures to be implemented for the defence of the considered attacks. In this deliverable only those relating to the “Short term control loop” have been considered. Of these countermeasures, those envisaged and used in the attacks dealt with in the RESISTO use cases were selected. We moved from the theoretical study to the practical use of countermeasures in specific RESISTO use cases. These countermeasures will then be implemented and deployed on the test beds made available to operators.

The countermeasures applied in the RESISTO project must be of “Relevance” for the main purpose of the project: “Prevention, detection, **response** and **mitigation** of the combination of physical and cyber threats”. In this deliverable we deal with **Response** and **Mitigation**.

This deliverable highlights the unified approach to mitigating combined cyber and physical threats. It can be seen how the mitigation of threats follows the same approach whether they are mainly cyber, physical or combined.

The RESISTO workflows are based on a series of recurring basic actions in various situations of which we can distinguish the following cases which are the most frequent:

- User Tasks to be performed manually: in this case the operator must execute the task autonomously. In some cases, the task involves using tools or interfaces made available by RESISTO, in others the operator must perform the action with other means and finally click on the “Done” button. In this case there is no control as to whether the operator actually carried out the action but it remains tracked on the database for subsequent checks, so the operator assumes responsibility for having declared that the action has been carried out.
- Manual user tasks with multiple choices: the operator must make a choice by selecting from a combo of predefined values and press “Done”. The choice is registered on the data base. The choice usually selects a branch on the workflow path.
- Script Task for Alerting people: this type of task usually involves the invocation of the EWCF component that deals with communication with the field in case of emergency. There may be cases in which the operator must instead call by phone.
- Task script for interaction with Network Orchestrator: this type of task involves the automatic invocation of the network orchestrator to execute specific commands. In test beds that provide direct action on the network, we prefer to act through a network orchestrator. RESISTO has at least two types: SDN orchestrator and ETSI 5g Orchestrator. In some cases, it is not possible to act directly with a network orchestrator and then proceed manually using an Orchestrator native User Interface (Embedded into RESISTO HMI if possible) or by alerting the staff in charge to take those actions.

For the correct design of the workflow it is necessary to identify the tasks to be performed and the order of execution.

When two tasks are not in logical sequence but can be performed simultaneously, it is advisable to insert a parallel execution node: “parallel gateway”. In this case the engine executes the two branches in separate threads. If the tasks are manual, they are both presented on the HMI and the operator can decide which one to execute first. It is important to be able to perform several tasks at the same time, as possible delays in execution are avoided, for example if two different entities are to be warned, in the opposite case if for example a security team has to be warned to block an intruder it must intervene first of the maintenance team that will have to repair the damage due to the intrusion.

The execution of tasks can be conditioned by choices made by the user, in this case an "Exclusive gateway" is inserted which allows to execute a workflow branch only if the operator has actually confirmed the choice. In some cases, certain tasks are conditional: for example, the movement of certain services to an alternative site using the orchestrator. For example, in the presence of an attack it is advisable that the consequences of the attack occur first, for example by using the Risk Predictor and then the services are migrated if appropriate.

In certain use cases the operator has the possibility of verifying the extent of the damage due to an attack or a disaster by using appropriate tools such as cameras with video analysis, drones, field sensors, etc. He can always use the Risk predictor to have the situation in real time and to simulate the effect of an event or action by performing a what-if analysis. In some cases, it is also possible to establish that the alarm is false and therefore to close the alert. The workflow must provide for these possibilities.

In some cases, it may not be possible to operate directly on the network orchestrator because the test bed does not allow it. In this case the RESISTO operator must report to a third party in charge of operating on the network to take the necessary actions.

## 2.5. Ethical and social implications

The choice and design of the correct mitigation measures for an attack also has ethical and social implications. Attacks on critical infrastructures often create uneasy fear and damage to both people and goods.

In particular, communication infrastructures have a strong impact on modern society and population. In Europe there is a great sensitivity to the protection of sensitive data and the privacy of citizens, therefore attacks that endanger these intangible assets are particularly felt. The physical security of citizens is of great importance and its protection is an increasingly complex and diversified mission. Citizens who live and work in a territory and make extensive use of telecommunications infrastructure, land and sea transport, may be victims of natural disasters or terrorist attacks and other threats can have significant benefits from systems such as RESISTO that set themselves the goal to resist and mitigate the increasingly complex and ever-evolving threats.

The ethical aspect is important in the decisions to be taken in the event of attacks on communication infrastructures. Which services has to be considered as priority and therefore which services has to be maintained in a degraded operating context. Which services has to be restored first. For large-scale attacks, how to decide which areas to restore first or try to keep active (based on the number of users, the criticality of the services, the infrastructure present, etc.).

Another problem with important ethical implications is the unauthorized loss or diffusion of personal and sensitive data caused by an attack on a communication infrastructure.

The latest generation of 5G telecommunications networks can carry many important services for the population, and in the near future they will constitute the backbone for the functioning of most telematics infrastructures. It is evident that a human attack or natural disaster that compromises its functioning would have a disastrous impact on the population with serious social consequences.

The 5G network is based on slices that can be individually isolated. When countermeasures are put in place that imply the isolation of a slice and therefore the loss of one or more services for the citizen, it is necessary to consider the impact that this will have on that population and raise the ethical problem of choosing which services to consider more or less important for the citizen.



### 3. WORKFLOW DEFINITION FOR RESISTO PROJECT

In this chapter we describe all the workflows used by RESISTO project. These workflows allow the RESISTO operator managing all the alarms related to the project.

The next paragraphs will describe the workflows designed for each use case. For the detailed description of the use cases, please refer to the use case document: D2.8

Note: the workflows indicated can be modified in the implementation phase for performance optimization and better usability, some "automatic" defined tasks will be transformed into manual tasks executable by the staff in charge if the automation is not possible on the reference test beds.

#### 3.1. British Telecom use cases

##### 3.1.1. Disruption of major sporting event

**Alarm type:** "Multicast Service Error":

**Description:**

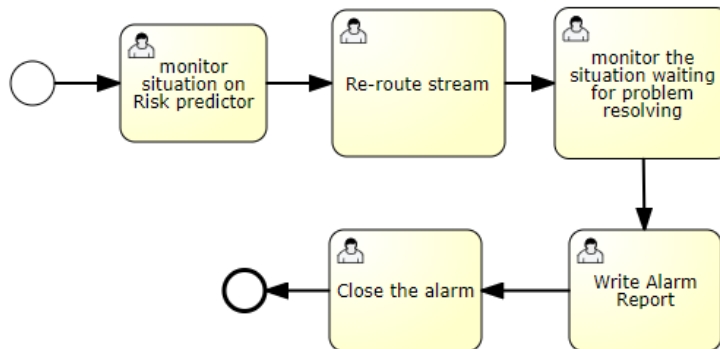
In order to respond to major multicast service disruption, depending on the situation, the RESISTO workflows will recommend the operators to perform one or more of the following actions:

- Re-route the multicast streaming for affected routers or end-devices
- Reject packet retransmissions for selected group of end-devices to ease the network congestion
- Request the change of encoding scheme at source to degrade the video quality in order to reduce the network traffic in general
- Request the change of encoding schemes at content server (i.e. to degrade the video quality) in order to reduce unicast traffic to every single end-devices, i.e. both multicast-capable (e.g. STB) or unicast-only devices
- Request the (unicast) receivers to switch to public access node (e.g. public WiFi) nearby (if available) if multicast streaming can be activated on that particular access node
- Request the video source to switch to high-speed radio networks (e.g. LTE-A or 5G) for streaming

**RESISTO Workflow:**

An example workflow is described in which the countermeasure adopted is to Re-route the multicast streaming

- Verify consequences on the Risk Predictor
- Re-route the multicast streaming
- Monitor the situation until the problem is resolved
- Write the alarm report
- Close the alarm



**Figure 12:** Multicast stream error process

if one of the other possible countermeasures is implemented, the workflows will be similar to the one presented.

### 3.2. TIM use cases

The TIM operator proposes a series of cases concerned to the Protection of Cloud Storage Services.

#### 3.2.1. Tampering on files containing sensitive data after physical access

**Alarm type:** “File Error”, an alarm attribute will specify that it’s a tampered file

**Security Threat:**

- Detection of unauthorized access to physical system
- Anomaly starts of processes
- Change in system configurations
- Tampering on file that containing sensitive information (configuration files)

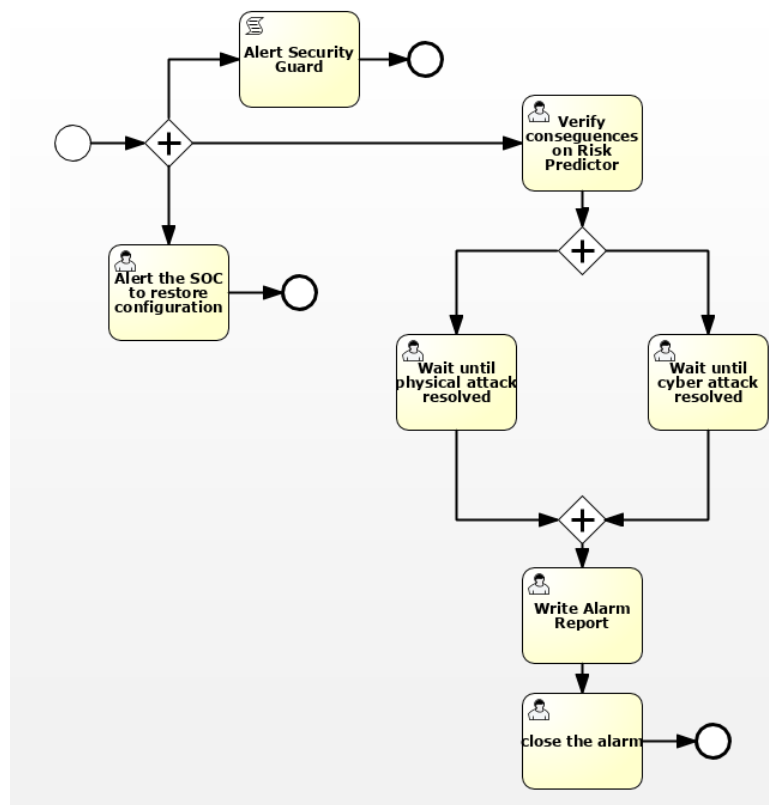
**Description:**

Rack or door sensor sends an event about physical access to RESISTO platform. ICT System monitoring detect anomaly in running processes or configuration changes and send an alert to RESISTO.

When a configuration changes after a detected physical access to the site, the detector sends an alert to RESISTO the alarm is of type: “Configuration changed after unauthorized physical access”.

**RESISTO Workflow:**

- Alert the security guard
- Alert the SOC that can restore the tampered file of network configuration or file related to a device firmware.
- Verify possible consequences on the Risk Predictor
- Wait for the physical intrusion resolution, the security guard the guard must ensure that the intruder has been identified and stopped or that he is no longer present on the site.
- Wait for the SOC to resolve the cyber threat restoring the original configuration
- Write the alarm report
- Close the alarm



**Figure 13: Tampering process**

### 3.2.2. Tampering detection change of file creation time by a process

**Alarm type:** “File Error”. An alarm attribute will specify that it is “change creation date”

**Security Threat:** Tampering file creation time by a process is related to anomaly behaviour associated with a hacking or a malware attack

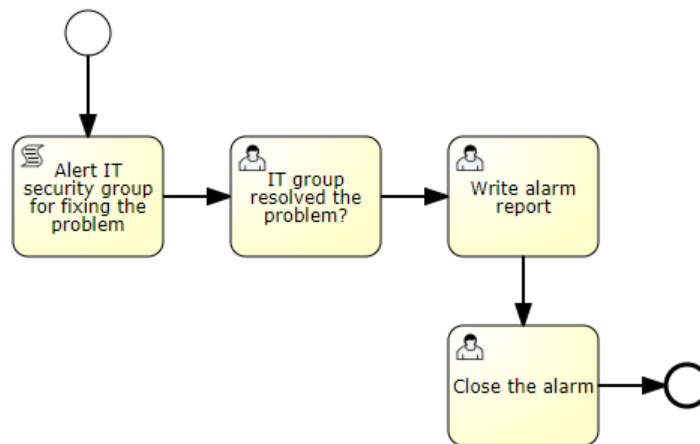
**Description:**

If creation time is modified by a process and path of executable is not %Windir% or ProgramFiles (Windows platform) but, for example a specific folder like /tmp, the sensor sends an event to RESISTO of type: “File Creation time changed”

**RESISTO Workflow:**

- Alert the IT security group for fixing the problem
- Wait for the problem resolution
- Write the alarm report
- Close the alarm





**Figure 14:** Time Creation change process

### 3.2.3. Hardware configuration system change

**Alarm type:** “Configuration Error”: an alarm attribute will specify that it is “Hardware configuration Change”

**Security Threat:** Detect physical intrusion, change of hardware configuration, like removing or adding a new device.

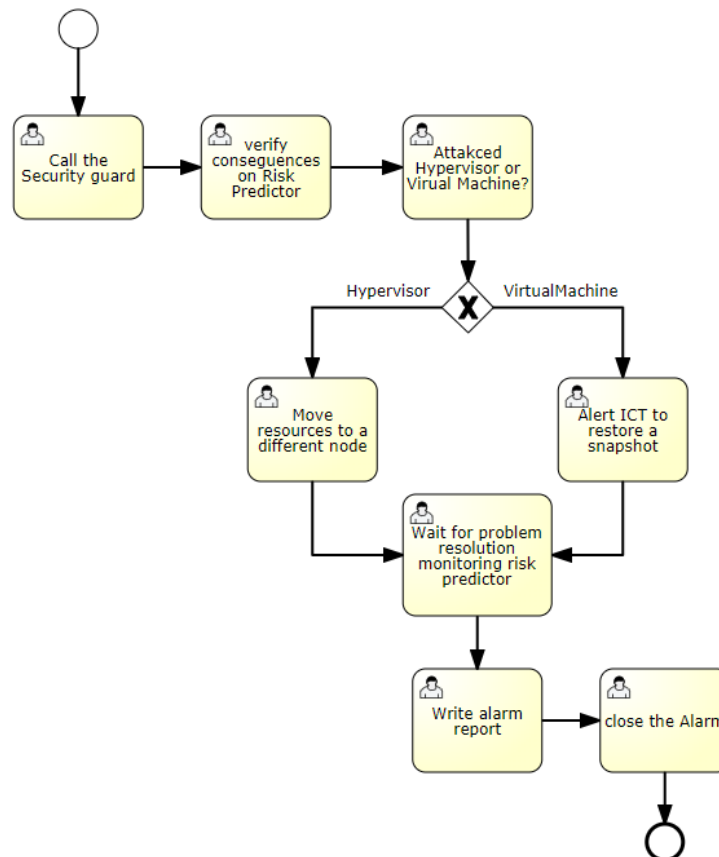
#### Description

Detect the opening of rack and change of node HW/configurations, send an alert to RESISTO of type: “HW Configuration Change”

#### RESISTO Workflow:

- Call the security guards
- Verify possible consequences on the Risk Predictor
- If the system attacked is the hypervisor
  - Move resources to a different node
- If the system attacked is a Virtual Machine
  - send an alert to ICT team to evaluate the restore of a snapshot
- Wait for the problem resolution
- Write the alarm report
- Close the alarm





**Figure 15:** Hardware configuration change process

### 3.2.4. Disaster Response and Recovery

#### Alarm Type: “Disaster Alarm”

**Security Threat:** The system could be damaged by a natural disaster such as floods, extreme temperature condition or political motivated threat like strike, terrorism that could lead to an interruption of critical services or could block intervention on site by personnel.

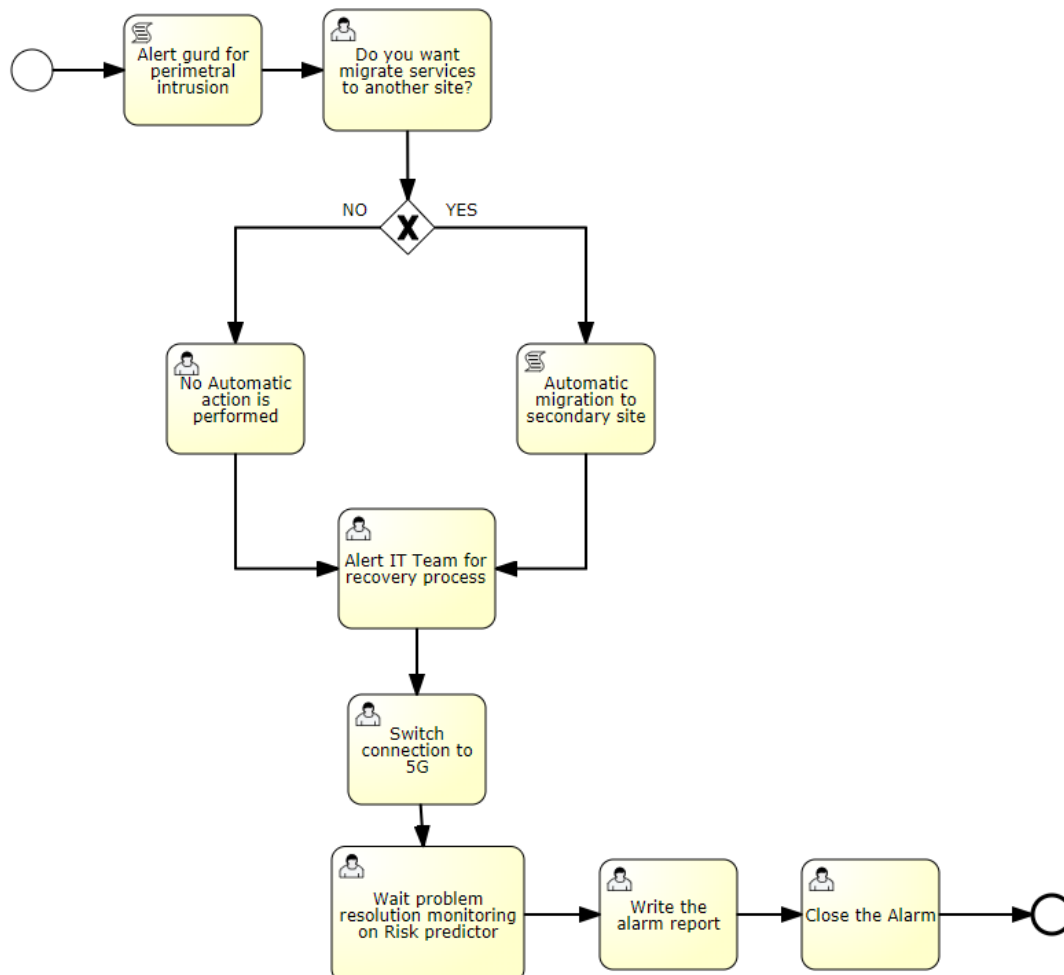
#### Description

In case of a natural threat or other kind of threats that make a critical service unavailable, or could prevents a correct treatment of threat

#### RESISTO Workflow:

- alerting the guard for perimeter a control of site perimeter
- Ask the RESISTO operator for migrate automatically a service to a secondary site
- If the operator answers YES
  - migrate automatically a service to a secondary site
- If the operator answer NO
  - Take no automatic action
- alert IT team personnel to initiate the recovery process and provides support for a fast recovery of all involved services in an alternate and safe site

- Switch the network connections to 5G
- Wait for the problem resolution
- Write the alarm report
- Close the alarm



**Figure 16:** Disaster Response process

### 3.2.5. Power loss

**Alarm Type:** “Power Problem”

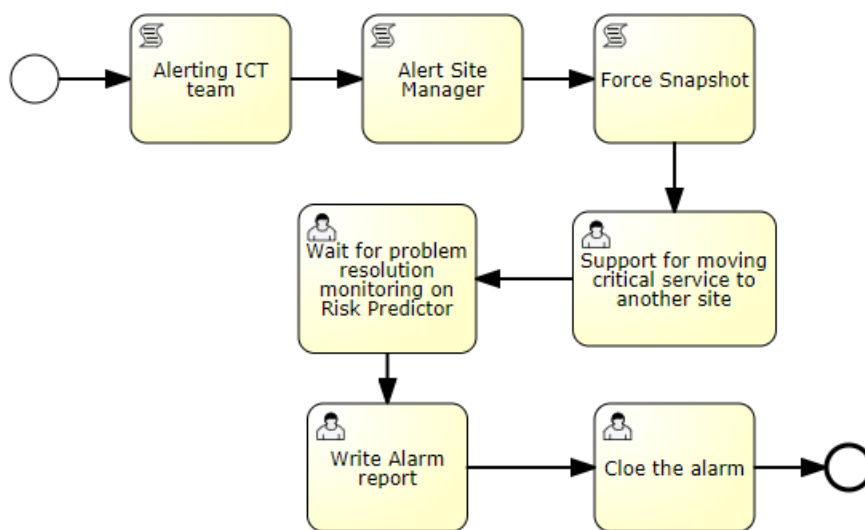
**Security Threat:** there are the fluctuations of electric power such as power outage that can be momentary (fault) or prolonged (blackout).

#### Description

In case of power loss, the sensors sent an event to RESISTO

### RESISTO Workflow:

- alerting the ICT team and Site manager
- force snapshot
- Support for moving critical services to another node or site.
- Wait for the problem resolution
- Write the alarm report
- Close the alarm



**Figure 17:** Power loss process

### 3.2.6. Temperature

**Alarm Type:** “Temperature Unacceptable”

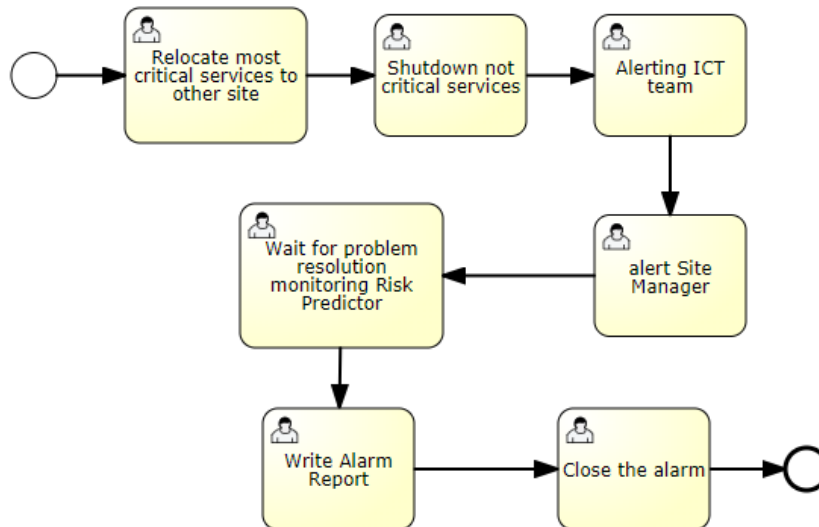
**Security Threat:** A temperature of site is out-of-range, the system could be damaged and create a disaster event that could lead to an interruption of critical services.

### Description

The sensors and systems events are sent to RESISTO of type: “Temperature out of Range”

### RESISTO Workflow:

- Relocation most critical services to alternate site
- Shutdown the not critical services
- Alerting the ICT team and Site manager
- Wait for the problem resolution
- Write the alarm report
- Close



**Figure 18:** Temperature unacceptable process

### 3.2.7. Data exfiltration

**Alarm Type:** “Data exfiltration”

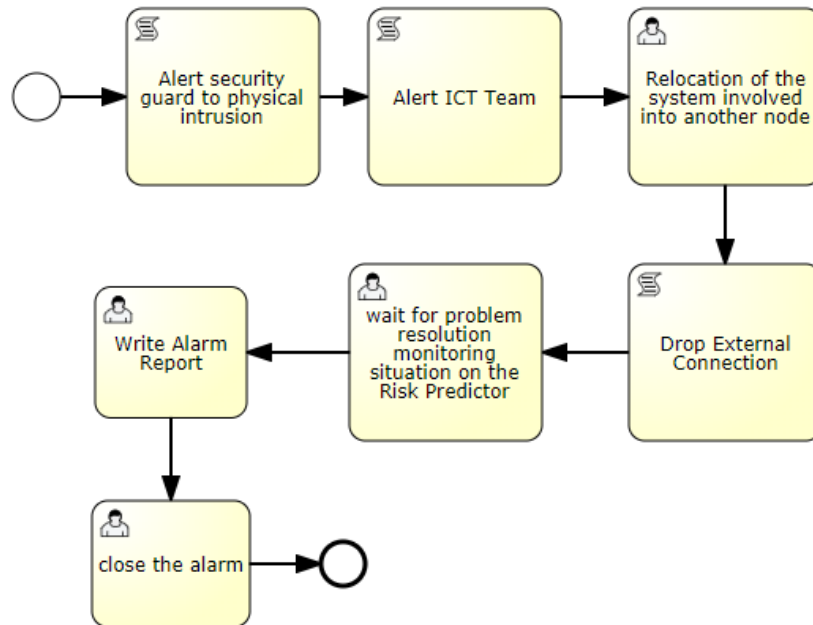
**Security Threat:** Large amount of data has been extracted from storage system that indicates a possible data exfiltration. The PSIM detects unauthorized access to systems, like rack door opened or an external device is attached to the system

#### Description

The detector sends an alarm to RESISTO platform of type “Data Exfiltration”

#### RESISTO Workflow:

- Alert Security guards for the Physical intrusion
- Alert ICT team
- Relocation of the system involved into another node
- Drop external connections
- Wait for the problem resolution
- Write the alarm report
- Close the alarm



**Figure 19: Data Exfiltration process**

### 3.3. Orange Romania use cases

The use case is named: “Cyber and physical protection of network and network elements mechanisms used by critical services that impact users”.

#### Description:

Use ORO IP/RAN/Core/Security network elements for relevant information collected from generally named “sensors” for malicious events recognition. Sensors will be implemented at every network boundary e.g. IDS/IPS, DoS mitigation platform, WAF.

The use case aims to:

- Aggregate the threats information into a database collection for future pattern attack recognition.
- Analyze the information and generate a dashboard for (near) real-time recognition and proper action to be taken, including automated mechanism of mitigation.
- SOC team is to analyze log events and make decision about high risk intrusion and also filter possible false positive events.
- Identify business critical assets and implement best-practices for protection and resilience.
- Implement physical network access protection to limit the intrusion possibilities. Integrate into the system the physical network access control for supervision of unwanted physical access.
- Use MDM platform(s) to redirect mobile devices traffic over a secured connection when using internet/intranet services.
- Protect traffic between highly sensitive information nodes in the network using encryption and anti-replay protection

For each of the considered attacks a specific type of security alarm is generated, for each type of alarm a specific management workflow is implemented as described below.

### 3.3.1. Internal DoS attack

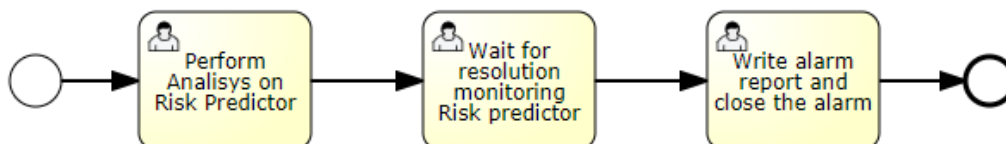
**Alarm Type:** “Congestion”, an alarm attribute specifies that it is “Internal Dos Attack”

**Detection:** trigger from Arbor DDoS mitigation platform

**RESISTO Workflow:**

- Perform analysis with Risk predictor
- Wait for the problem resolution monitoring risk predictor
- Write the alarm report
- Close the alarm

The Isolation of the attacker IP address will be performed automatically by the Arbor tool.



**Figure 20:** Internal DoS process

### 3.3.2. DDoS attack from inside botnet:

**Alarm Type:** “Congestion”, an alarm attribute specifies that it is “DDoS Attack”

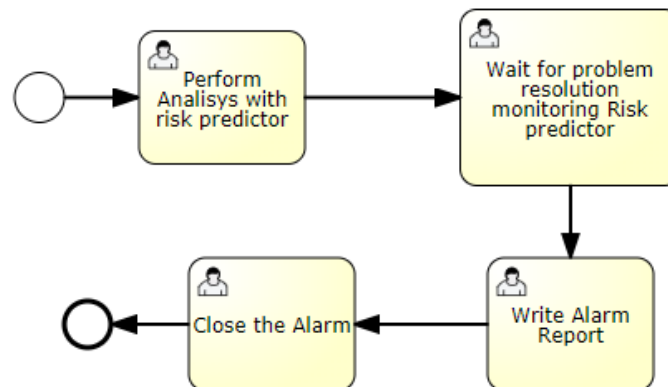
**Detection:** correlating triggers from Arbor DDoS mitigation platform and FortiGate Firewalls

**RESISTO Workflow:**

- Perform analysis with Risk predictor
- Wait for the problem resolution monitoring risk predictor
- Write the alarm report
- Close the alarm

The communication between client and C2C server is performed automatically by the security system in this case RESISTO will allow the user only to monitoring the situation

A C2C Server is a machine hosted anywhere in the internet that controls and orchestrates the attack activity of the compromised hosts ‘zombies’ in a botnet. Severing the connection between C2C Server(s) and compromised hosts usually slows down or stops the DDoS attack.



**Figure 21:** DDoS process

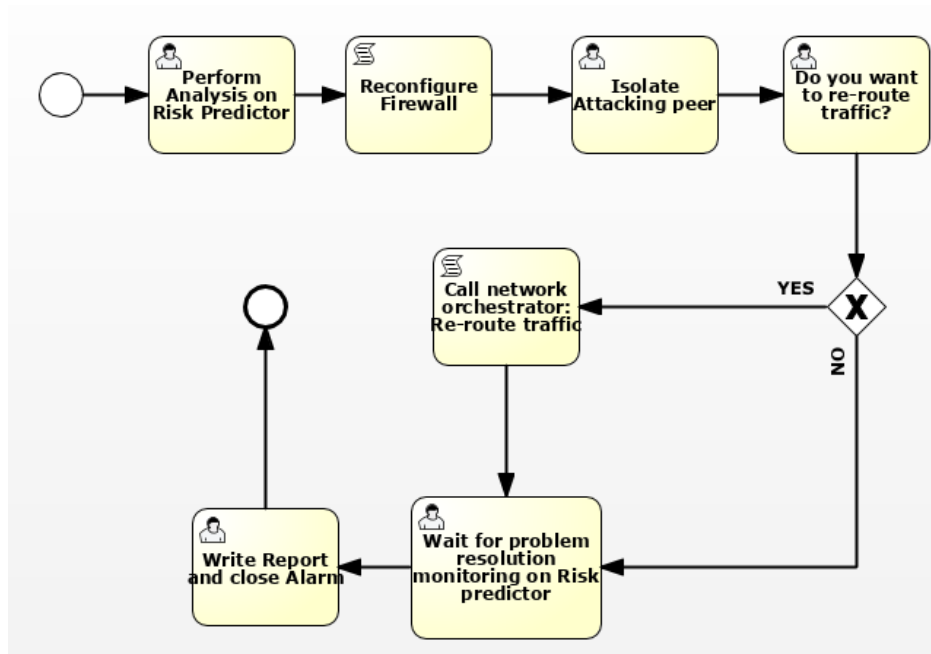
### 3.3.3. DDoS attack on peering border

**Alarm Type:** “Congestion”, an alarm attribute specifies that it is “DDoS Attack on border”

**Detection:** Trigger from Arbor DDoS mitigation platform

#### RESISTO Workflow:

- Perform analysis with Risk predictor
- Reconfigure Firewalls
- isolate attacking peer
- It is possible re-route traffic? Yes/No
  - If Yes -> using Network Orchestrator to Re-route traffic
  - If No -> go to next task
- Wait for the problem resolution monitoring risk predictor
- Write the alarm report
- Close the alarm



**Figure 22:** DDoS peering border process

### 3.3.4. Routing Table Poisoning on core

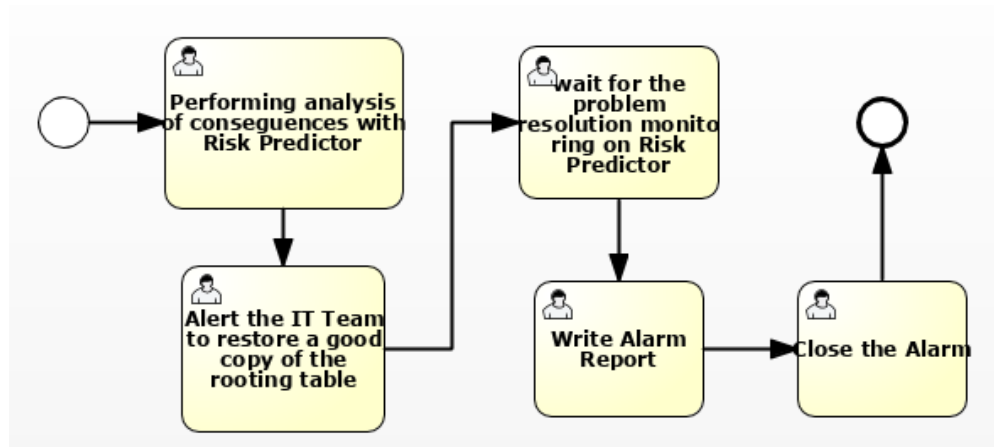
**Alarm Type:** “corrupt data”: an alarm attribute specifies “Routing Table Poisoning”

**Detection:** will verify, possibly by polling logs from routers + anomaly detection.

**RESISTO Workflow:**

- Perform analysis of consequences with Risk predictor
- Alert the IT Team to Restore Known Good Copy of Routing Table
- Wait for the problem resolution monitoring risk predictor
- Write the alarm report
- Close the alarm





**Figure 23:** Routing table poisoning process

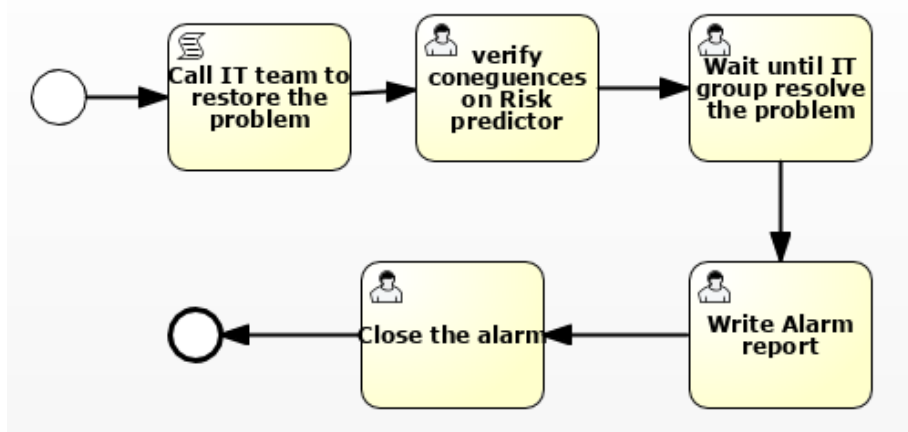
### 3.3.5. BGP Hijacking

**Alarm Type:** “Corrupt Data”: an alarm attribute specifies “BGP Hijacking”

**Detection:** This attack can be detected by using tools like ARTEMIS or similar, mitigation can have some automatic mechanism but in some cases the problem has to be solved by IT Cyber security team.

#### RESISTO Workflow:

- Alert the IT Team to defending by BGP Hijacking attack
- Perform analysis of consequences with Risk predictor
- Wait for the problem resolution monitoring risk predictor
- Write the alarm report
- Close the alarm



**Figure 24:** BGP Hijacking process

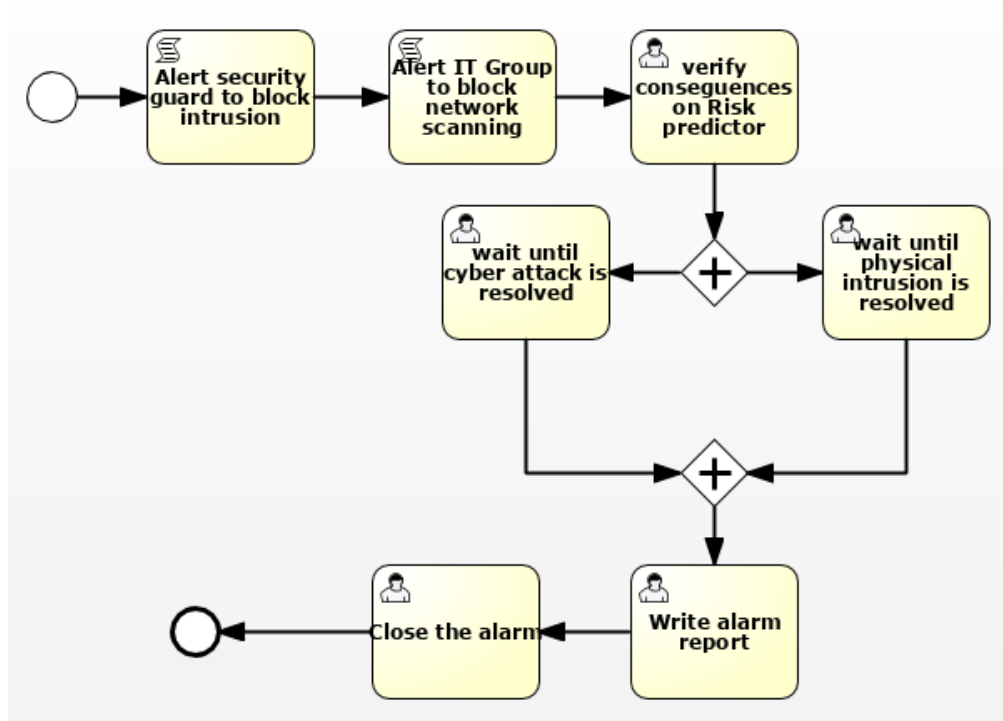
### 3.3.6. External Network Scanning Lateral Movement

**Alarm Type:** “External Network Scanning on Intrusion”

**Detection:** detected polling from FortiGate Firewalls/IDSs logs and correlating to a physical intrusion on ORO buildings

**RESISTO Workflow:**

- Alert security guard to block intrusion
- Alert the IT Team to defending by network scanning attack
- Verify consequences with Risk predictor
- Wait until cyber-attack is resolved monitoring risk predictor
- Wait until physical-attack is resolved monitoring risk predictor
- Write the alarm report
- Close the alarm



**Figure 25:** External Network Scanning on intrusion process

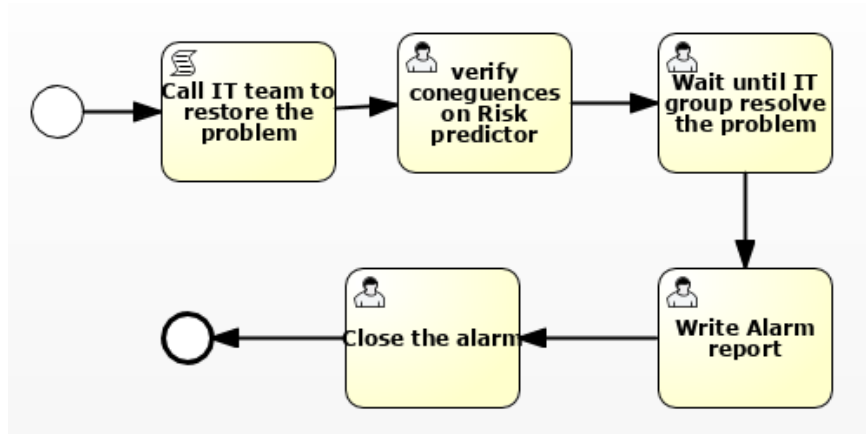
### 3.3.7. Detection connectivity to botnets from internal network

**Alarm Type:** “Connectivity Botnet from Internal Network”

**Detection:** Correlation of firewall logs with known C2C servers IPs, anomaly detection

### RESISTO Workflow:

- Alert the IT Team to defending by Connectivity Botnet
- Verify consequences with Risk predictor
- Block connections to C2C server IPs
- reconfigure the Firewall
- Wait until cyber-attack is resolved monitoring risk predictor
- Write the alarm report
- Close the alarm



**Figure 26:** Connectivity to botnet from internal network process

## 3.4. OTE use cases

### 3.4.1. Core Network Failure on Physical & Cyber Attacks

**Name of use case:** “Core Network Failure caused By Physical & Cyber Attacks to Telco sites”

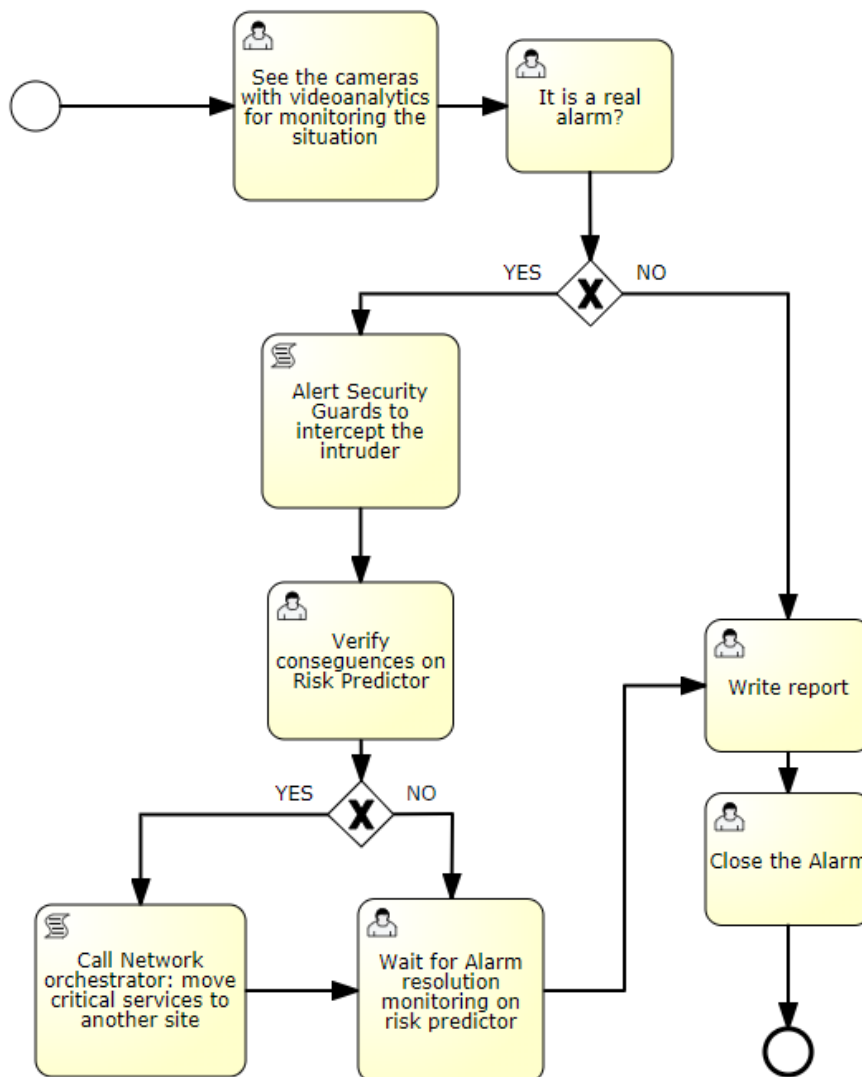
**Alarm Type:** “Network Cyber Physical Attack”

#### Brief description of the use case

- Unauthorized Intrusion in Lab Premises in Athens
- Passes all physical security controls (guards, locked doors etc.)
- Video Analytics used for peripheral surveillance.
- The intruder Enters Core Lab and Causes damage like network failure /or cyber-attack may cause physical damage to the network
- Network services and Operation malfunctions with Several assets affected
- Detection by whom / which component.
- Security alarms are sent to persons responsible

### RESISTO Workflow:

- See the cameras with video analytics to monitoring the situation
- Check if the alarm is real or fake seeing the video in real time
- If the alarm is real
  - Alert Security guard to intercept the intruder
  - Verify consequences using Risk Predictor
  - Do you want move services to another site?
    - If yes call the orchestrator to perform the action
    - If no : take no action
- Wait until the problem is resolved monitoring the situation on risk predictor
- Write alarm report
- Close the alarm



**Figure 27:** Network Cyber Physical Attack process

### 3.4.2. Earthquake Multiple Terrorist Attacks

**Name of use case:** *“Telecommunications congestion caused by Earthquake Multiple Terrorist Attacks”*

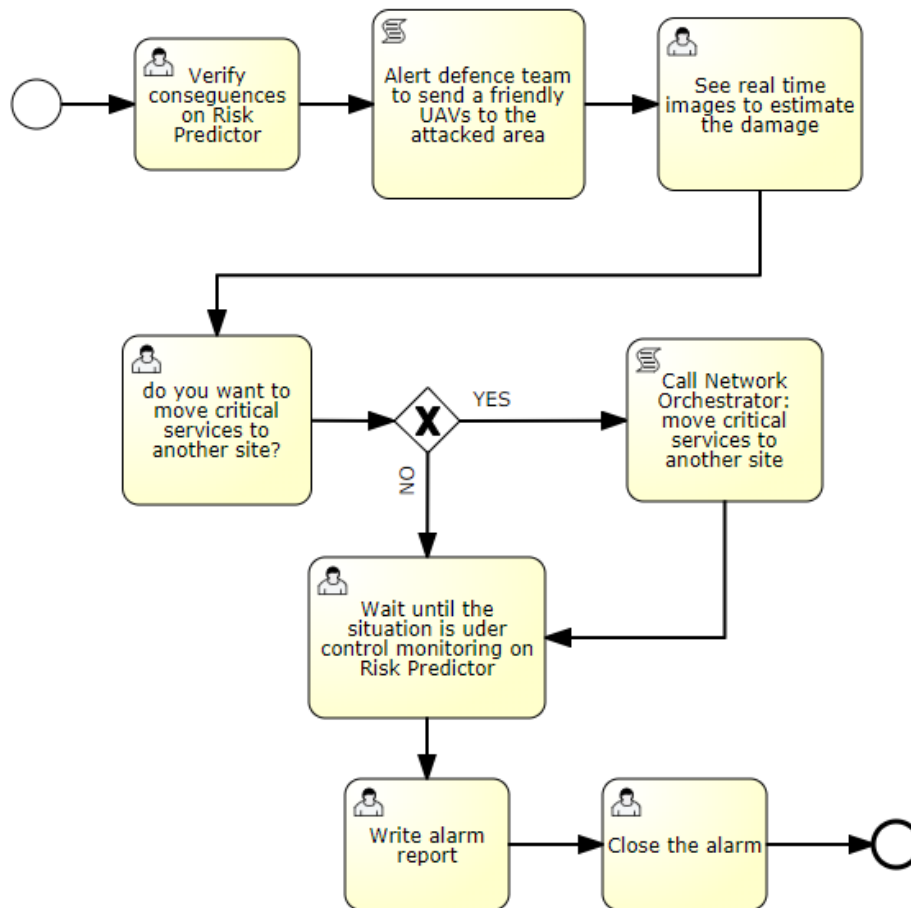
**Alarm Type:** “Earthquake alarm”

#### **Brief description of the use case**

- A terrorist attack using hostile UAVs has taken place and a major part of the network has been destroyed)
- Everyone is trying to contact family and friends, so we have network congestion
- A friendly UAV equipped with Electro-Optic payload will be used in order to provide real-time image to the estimation of the damage
- Traffic rerouting from network operator will be needed

#### **RESISTO Workflow:**

- Verify consequences using Risk Predictor
- Alert the defence team to send the drone into the damaged areas
- See the real time images to estimate the damage
- Do you want to move services on another node?
  - If Yes: Call orchestrator to move the critical services on another site
  - If no: take no action
- Wait until the situation is under control monitoring the Risk Predictor
- Write report
- Close the alarm



**Figure 28:** Earthquake alarm process

### 3.5. Altice Lab use cases

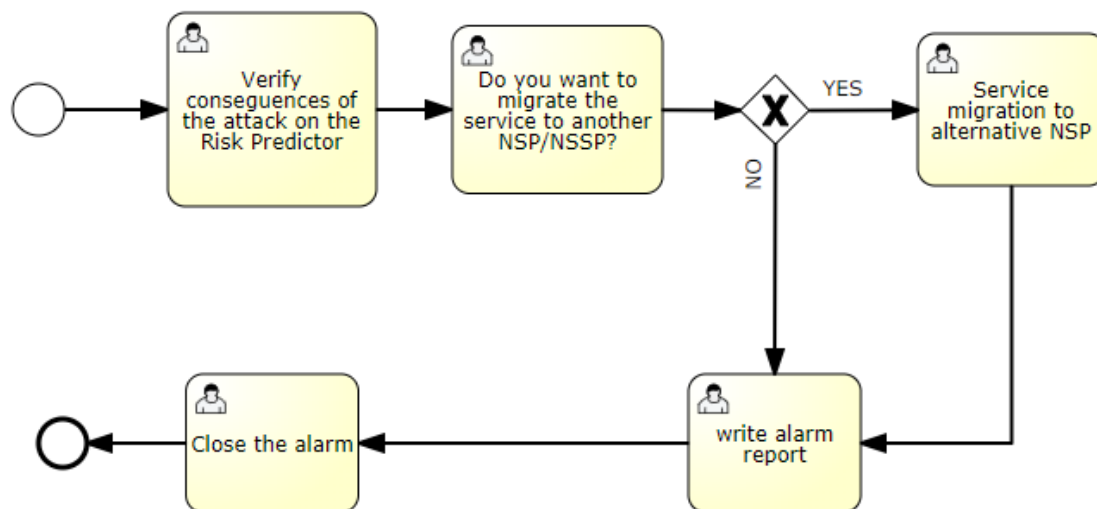
**Name of use case:** “5G network response to a security breach”

**Brief description of the use case:**

- Automatic detection of cyber/physical attack by continuous analysis of network element failures or abnormal behaviour.
- Upon detection of this threat, the network management and orchestration layer will react in line with predefined policies and actions.
- Two candidate scenarios are possible, during the implementation phase (WP9) a decision will be made as to which scenario, or both, will be deployed.
  - Scenario 1: When a security event is detected in the network slice, the SP/NSP migrates the affected Slice Subnets from NSSP A to NSSP B
  - Scenario 2: Based on a pre-established business agreement between the SP and NSPs A and B, once a security event is detected in the network slice provided by NSP A, the service is migrated to a different network slice, with similar characteristics, provided by a different NSP B, which is established on-demand.

### RESISTO Workflow:

- Verify consequences of the attack on the Risk Predictor
- Do you want migrate the service on another NSP/NSSP?
- If Yes:
  - Call Network Orchestrator to perform the migration
- If NO: no action is performed
- Call the maintenance team with EWCF
- Wait monitoring on risk predictor until the situation is under control
- Write alarm Report
- Close the alarm



**Figure 29:** Altice Lab Use case workflow

## 4. EMERGENCY WARNING COMMUNICATION FUNCTION

The implementation choices have been dictated by the need to explore innovative solutions to handle emergency warning messaging that are not based on the current standardized services, to propose a different evolution for this service in a world that is changing and as reported in <sup>1</sup> citizens do not sit around waiting for the city authorities. In fact the key findings of the article cited are that 40 percent feel safer when out and about with a smartphone; one in four think that having a smartphone makes citizens less risk-averse than they would be otherwise. Citizens actively engage in personal safety. Three in four already use emergency apps or functions on their smartphones, and many express a high interest in using more security apps.

The scope of the EWC is to send targeted alerts and/or informational messages to specific categories of users such as rescue teams or security officers that will be physically present on specific target areas where events like natural disasters, physical or cyber-attacks are discovered by RESISTO platform and some action that requires people on site must be triggered.

The function can be integrated in 5G networks as well as in existing telecommunications networks and is made available “as a Service” also to specific public safety agencies.

The implementation will include a server and an Android application. The server will expose an interface towards the other modules of RESISTO framework that need to communicate information concerning a physical-cyber attack to the intervention team that operates where the telecom infrastructure is located. The rescue team will leverage on the application information, both textual and visual. In particular, the position of points of interests or of the other team members will be collected and visualized. The app will be available on Android smartphones, or any other Android device. Rescue teams will be ordered to go where events are happening and will receive relevant information when events like natural disasters, physical or cyber-attacks occur.

Although the main target of this version of the Emergency Warning Communication Function has been to provide an implementation that closes the short-term control loop, the service can be extended to provide warnings to a neighbouring population through a smartphone application. Communication with populations in the event of an attack to a critical infrastructure is currently possible only by specific application to be installed on the user device.

The architecture is made of several components:

1. a native cloud service that can be deployed as a microservice
2. a messaging framework
3. an android app
4. an IOT framework

### 4.1. EWC Service REST interface

The cloud native service like all communication services in the 5G architecture exposes a REST interface towards the Workflow manager that can perform typical administration tasks like adding users and groups that are configured also dynamically to respond to a security attack. The users will

---

<sup>1</sup> <https://www.ericsson.com/en/trends-and-insights/consumerlab/consumer-insights/reports/public-safety-goes-personal>



be arranged in groups on the fly around a security event occurring in a specific physical location in order to be involved in the handling of the incident mitigation actions.

The service offers a CRUD REST based interface that covers the definition of users and groups of users for administration.

The REST interface moreover allows the dispatching to the teams that are defined on security events that RESISTO platform detects. The event is delivered to the team members (users in the groups) that will have the Android application LocationInfo available on their devices and listening for messages coming from RESISTO.

## 4.2. Messaging framework

The messaging framework that has been integrated in the current implementation is firebase cloud service from google Firebase can be easily integrated and since is a cloud service while on one side it offers the messaging on top of the data layer and does not require any specific server in the operator network on the other is not integrated in the telecom infrastructure and cannot be reliable as the other telecom messaging services for which the same resilience of the network is provided, but also does not allow for cell broadcasting. Alternative implementation that can be easily added are for instance traditional SMS or the new standard for messaging RCS.

## 4.3. Localization

Current implementation of localization is based on the GPS information that is recovered from the smartphone itself. This is an alternative to cell localization which does not require a connection to the GMPC server of the Operator network; the 2 systems though can be integrated to give a more reliable service which combines input from both networks.

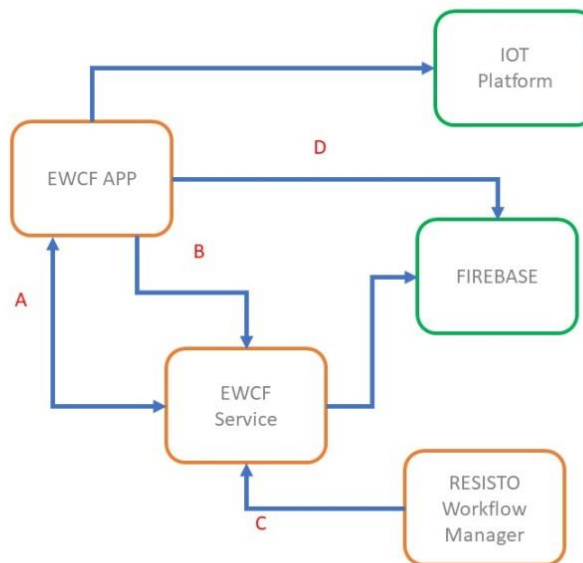
## 4.4. IOT framework integration

In order to collect vital signs of the people involved in the rescue team and also their GPS signal an IOT framework has been integrated in the Android Application.

The IOT framework can also be used to report in the Android application the status of neighbouring IOT devices like fire sensors or other alarms that are located close to the team members.

The interfaces between the components are shown in the Figure 30 interface will receive messages from RESISTO that need to be delivered to the team regarding targeted alerts and/or informational instant messages to the users of the EWCF-APP. C interface provides a service based REST API (Application Program Interface) to RESISTO to make requests to the EWC service.

- A and B interfaces shall be used to collect location information and other information from sensors in field.
- D interface (as an alternative to A) can be used to send messages via standard protocols using available telecom messaging capabilities (e.g. SMS, IMS) to target groups in future implementation current one as we already stated is using an OTT firebase cloud service.



**Figure 30: EWC function**

## 4.5. Android application

The application will show on the map the location of the event sent from RESISTO framework and any additional information regarding the event that is collected and elaborated in the mean time for instance access to servers or any failure in a telecom device.

The application will also show the location of the other users in the group of the owner of the device.

## 5. CONCLUSION

This deliverable presents the RESISTO workflow study and implementation activities and includes, in addition to this document, the workflows presented here that were actually developed in the standard BPMN 2.0 format. The implementation parts of the calls to EWCF and Network Orchestrator are beyond the scope of the Deliverable and will be carried out at a later stage, but the workflows that invoke the tasks have actually been developed.

The RESISTO product was developed with components such as the Workflow that allow a wide flexibility and configurability to face ever new and constantly evolving threats. So an advantage of the RESISTO system is the possibility of being kept constantly updated to deal with these new threats.

An integral part of the system is the Designer workflow that allows you to create new workflows and modify existing ones.

The RESISTO system presents a series of various use cases but does not claim to be exhaustive for all possible threats, so this work must be considered a starting point to face new and more evolved cyber, physical and combined threats with an approach unique, integrated and innovative which is the purpose of the project's innovation action.

And finally RESISTO system mitigation action, that are part of the workflow, are taking advantage of a personal application that supports and dispatches people implementing security countermeasure to perform coordinated controlled action upon receiving information about security events directly on their smart-phones.