

RESISTO:

D5.4_ Real Time Response and Mitigations Results



RESISTO

D5.4 – REAL TIME RESPONSE AND MITIGATIONS RESULTS

Document Manager:	Jorge Carapinha	ALB	Editor
--------------------------	-----------------	-----	--------

Project Title:	RESilience enhancement and risk control platform for communication infraSTructure Operators
Project Acronym:	RESISTO
Contract Number:	786409
Project Coordinator:	LEONARDO
WP Leader:	RM3

Document ID N°:	RESISTO_D5.4_200603_01	Version:	1.0
Deliverable:	D5.4	Date:	03/06/2020
		Status:	APPROVED

Document classification	PUBLIC
--------------------------------	---------------

Approval Status	
Prepared by:	Jorge CARAPINHA (ALB)
Approved by: (WP Leader)	Marco CARLI (RM3)
Approved by: (Coordinator)	Bruno SACCOMANNO (LDO)
Advisory Board Validation (Advisory Board Coordinator)	NA
Security Approval (Security Advisory Board Leader)	Paolo DI MICHELE (LDO)

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Federico Colangelo	RM3	Contributor
Marco Carli	RM3	Contributor
Federica Battisti	RM3	Contributor
Alberto Neri	LDO	Contributor
Emanuele Aonzo	LDO	Contributor
Javier Valera	INT	Contributor
Moisés Valeo	INT	Contributor
Jose Manuel Sánchez	INT	Contributor
Jorge Carapinha	ALB	Contributor
Paula Cravo	ALB	Contributor
Luís Cortesão	ALB	Contributor
Giuseppe Celozzi	TEI	Contributor
Cosimo Zotti	TEI	Contributor
Giovanna Spadaccio	TEI	Contributor

DISTRIBUTION LIST

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

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
0.1	20.11.2019		All	Draft ToC
0.7	01.04.2020		All	First complete draft
0.8	16.04.2020		All	Draft for revision
0.9	13.05.2020		All	Final Release for SAB assessment
1.0	03.06.2020		All	Final version

COPYRIGHT STATEMENT



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

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

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

PROJECT CONTACT



LEONARDO

Via Puccini 2 – Genova – 16154 – Italy

Tel.: +39 348 6505565

E-Mail: bruno.saccomanno@leonardocompany.com

RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

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

EXECUTIVE SUMMARY

This deliverable summarizes the activities performed in the Algorithms and actions for Real Time Mitigation and Action work package in the RESISTO project. The research and the developed algorithms have been devoted to providing models and components for implementing the short term control loop. In particular, it enhances RESISTO architecture dealing with response and mitigation, through the definition of possible countermeasures thus supporting the security operator in selecting the best reaction/mitigation strategy through an optimized workflow and the orchestrator. Furthermore, an emergency communication functionality is developed

CONTENTS

ABBREVIATIONS.....	12
1. INTRODUCTION	13
2. CYBER-PHYSICAL THREATS COUNTERMEASURES	15
2.1 REVIEW OF AVAILABLE COUNTERMEASURES W.R.T. DEFINED THREATS CLUSTERS.....	15
2.1.1 IDENTITY MANAGEMENT AND ACCESS	15
2.1.2 DISRUPTION OF DATA OR HW LOSS	17
2.1.3 NETWORK RELIABILITY	18
2.1.4 DOS ATTACKS HANDLING	19
2.1.5 NATURAL DISASTER.....	21
2.1.6 PHYSICAL SECURITY – PHYSICAL INTRUSION.....	22
3. MITIGATION FRAMEWORK.....	27
3.1 USE CASE: DISRUPTION OF MAJOR SPORTING EVENT BY COMBINED PHYSICAL & CYBER-ATTACK BY A TERRORIST ORGANIZATION	27
3.2 USE CASE: MARITIME SAFETY AND EMERGENCY CASE.....	28
3.3 USE CASE: PPDR VIRTUAL OPERATOR MARITIME SAFETY AND EMERGENCY CASE.....	29
4. EMERGENCY WORKING COMMUNICATION.....	30
4.1 USE CASE 1 CORE NETWORK FAILURE CAUSED BY PHYSICAL & CYBER ATTACKS TO TELECOMMUNICATION SITES.....	30
<i>Sub case 1 – Storytelling</i>	<i>30</i>
<i>Sub case 2 – Storytelling</i>	<i>30</i>
4.2 USE CASE 3 TELECOMMUNICATION SITES.....	31
<i>Sub case 1 – Storytelling</i>	<i>31</i>
4.3 USE CASE 5 PROTECTION OF CLOUD STORAGE SERVICES.....	31
<i>Sub case 1 – Storytelling</i>	<i>31</i>
5. EXTENSIONS OF THE SDS MODEL.....	33
5.1 MULTI-OBJECTIVE COUNTERMEASURE OPTIMIZATION	33
5.1.1 ON-GOING EXPERIMENTATION.....	39
5.2 SOFTWARE DEFINED RADIO SECURITY	41
5.3 MACHINE LEARNING-BASED CELL FAULT DETECTION	42

5.3.1	INTRODUCTION	42
5.3.2	OVERVIEW	42
5.3.3	BUSINESS UNDERSTANDING	43
5.3.4	DATA UNDERSTANDING.....	43
	<i>Alarm data</i>	<i>44</i>
	<i>Inventory data.....</i>	<i>45</i>
	<i>TTK data.....</i>	<i>46</i>
5.3.5	MODELLING	47
	<i>Feature engineering.....</i>	<i>47</i>
5.3.6	APPROACHES.....	48
5.3.7	INTEGRATION IN RESISTO	48
5.4	MACHINE LEARNING-BASED POSITIONING FOR PHYSICAL SECURITY	49
6.	CONCLUSIONS	51
7.	REFERENCES	52

List of Figures

Figure 1: Scope of WP5 in RESISTO architecture	13
Figure 2: Disruption major event workflow.....	28
Figure 3: Maritime use case workflow.....	28
Figure 4: PPDR workflow	29
Figure 5: Example topology with nodes enumeration.	35
Figure 6: Example crossover procedure.	36
Figure 7: Example of deletion mutation.	38
Figure 8: Example of flipping mutation.	38
Figure 9: Representation of the GEANT network topology.	40
Figure 11: Alarm characterization – Spatial Perspective	44
Figure 12: Network snapshot.....	47
Figure 13: Cell fault detection integration with other RESISTO components	49

List of Tables

Table 1 - Password Protection	15
Table 2 - Badge, smart cards protection.....	16
Table 3 - Phishing attacks	16
Table 4 - Session Hijacking	17
Table 5 - Disruption of data or HW loss.....	18
Table 6 - Network failures.....	19
Table 7 - (D)Dos	21
Table 8 - Service Continuity	22
Table 9 - Physical Intrusion	22
Table 10 - Use cases to countermeasures mapping	23
Table 12 - Source description	44
Table 13 - Alarm key features	45
Table 14 - Inventory key features	46
Table 15 - Ticket key features	46

ABBREVIATIONS

2G, 3G, 4G, 5G	Second, third, fourth and fifth generation of mobile phone systems
CCTV	Closed-Circuit Television
CI	Critical Infrastructure
DDoS	Distributed Denial of Service
DoS	Denial of Service
DSS	Decision Support System
EWC	Emergency Warning Communication
IoT	Internet of Things
LTE	Long Term Evolution (= 4G)
NFV	Network Function Virtualization
NS	Network Service
NSGA	Non-dominated Sorting Genetic Algorithm
PPDR	Public Protection and Disaster Relief
RAN	Radio Access Network
PON	Passive Optical Network
SDN	Software Defined Networks
SDS	Software Defined Security
SLA	Service Level Agreement
TTK	Trouble Ticket
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
WP	Work Package

1. INTRODUCTION

This document is the final deliverable of RESISTO WP5 whose main focus is represented by the shaded area in Figure 1. Essentially, WP5 is aimed at delivering the RESISTO components dealing with response and mitigation, including the definition and implementation of the mitigation framework for defining the best reaction/mitigation workflow strategy. We can say that WP5 addresses the decision and actuation phases of the control loop. The actuation phase includes direct actions on network equipment by mean of the Orchestrator Controller, as well as human teams driven through an emergency communication function.

To some extent, the current deliverable updates and extends results provided in previous WP5 deliverables.

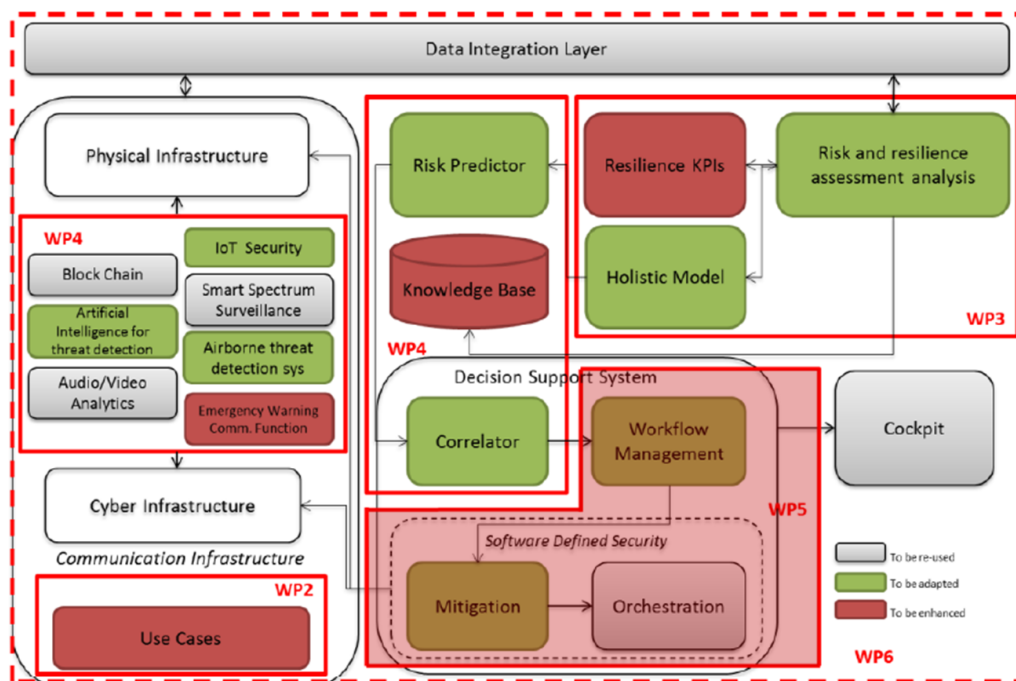


Figure 1: Scope of WP5 in RESISTO architecture

As described in the following sections, the work performed in WP5 has been essentially devoted to the definition and modelling of possible countermeasures (described in D5.1 [3]), also related to the defined use cases. A graphical representation model, exploiting attack tree, has been selected and used. The mitigation framework has been defined and implemented (see D5.2 [1]), and the emergency communication functionality realized (D5.3 [4]). Following this introductory section, the present deliverable is structured as follows:

- Section 2 describes an updated analysis of the possible countermeasures especially with respect to the use cases that have been defined and that will be addressed in RESISTO.
- Section 3 describes, with respect to the mitigation framework, modifications that have been made on workflows regarding some use cases that were not yet defined or that have been modified.

- Section 4 describes the emergency communication function
- Section 5 describes results of activities carried out in the scope of WP5, which can be seen as extensions to the Software Defined Security model.
- Finally, section 6 provides the general conclusions of the deliverable.

2. CYBER-PHYSICAL THREATS COUNTERMEASURES

2.1 Review of available countermeasures w.r.t. defined threats clusters

2.1.1 Identity management and Access

Typical threats related to identity management categorized in communication system, see [24], are Spoofing of identities and elevation of privilege, typical identity spoofing involves illegal access of a user's authentication (e.g. username and password, smart card, badge, a phone used for multi authorization). Once a user identity is spoofed the next step is elevation of privilege, if doing so the attacker has penetrated system's defenses and is considered part of the trusted system this is one of the most dangerous situations, in fact the possibility to raise the user privileges paves the way to the possibility to compromise or destroy a system.

Identity management is an extremely important set of actions and for an infrastructure are similar in nature to both in the physical that in the digital part of the CI of telecommunications systems. We have several countermeasures that are related to the pretended identity of a person that operates a telecommunication infrastructure. Stealing the operator identity in our analysis is described both in terms of physical assets than of the telecommunication software systems.

Credentials to access either a physical infrastructure or a software system both need to be carefully protected and procedures must be defined to handle their lifecycle and operation.

An operator of a telecommunication infrastructure is identified with a set of credentials physical (e.g. a badge, a key) or a digital identity (e.g. a PIN, a user/password).

Table 1 - Password Protection

Password protection
Preventive
<ul style="list-style-type: none"> [1] Do not allow passwords to be sent in cleartext (don't use protocols like FTP or TELNET, ensure proper application layer authentication frameworks are used, [2] Encryption algorithms or hashing functions used should satisfy the highest possible security standards. [3] Employ one-time password tokens and/or other 2fa authentication methods (eg. biometrics) [4] Use hard-to-guess passwords of at least 12 characters long. [5] Rotate passwords frequently. [6] Employ an IDS to detect suspicious behavior. [7] Use dictionary-cracking tools to find weak passwords chosen by users. [8] Use special characters, numbers, and upper- and lowercase letters within the password (<i>The password should not be constrained by any length or character limitation</i>) [9] Keep sw up-to-date including latest security patches [10] Protect password files. [11] Salt the password database [12] Any software system shouldn't use default accounts and passwords [13] Periodic Vulnerability Scan [14] Do not allow password reuse

<p>[15] Use captcha when multiple wrong passwords are submitted from an account, IP or other identity</p> <p>[16] Develop a lockdown policy according to the number of wrong password submissions</p> <p>[17] Develop responsible disclosure & bug bounty programs to encourage security researchers to report vulnerabilities identified in a defined scope</p>
Reactive
<p>[18] User account lock out, de-authenticate or revocation</p> <p>[19] Force password resets</p> <p>[20] IP address lockout</p>

Table 2 - Badge, smart cards protection

Badge, smart cards protection
Preventive
<p>[21] Access limitations for critical rooms/areas</p> <p>[22] Access logging</p> <p>[23] Video monitoring</p>
Reactive
<p>[24] Badge lockout</p>

Table 3 - Phishing attacks

Phishing attacks
Preventive
<p>[25] Plan activity for raising security awareness in the personnel</p> <p>[26] Be skeptical of e-mails indicating you must make changes to your account.</p> <p>[27] When in doubt, call the legitimate company representative to find out if this is a fraudulent message on a different communication channel</p> <p>[28] Review the address bar to see if the domain name is correct.</p> <p>[29] When submitting any type of financial information or credential data, Transport-level encryption (SSL or TLS). Moreover, any URL in the address bar must start with https:// and a closed-padlock icon in the browser at the bottom-right corner. This means transport-level encryption is implemented.</p> <p>[30] Do not click an HTML link within an e-mail. Type the URL out manually instead.</p> <p>[31] Do not accept e-mail in HTML format.</p> <p>[32] Up-to-date antivirus to detect keyloggers, rootkits, ransomware and other malicious applications</p> <p>[33] Do not download or open any suspicious attachment files</p> <p>[34] Spam and e-mail filtering in place</p> <p>[35] Report any suspicious email addresses to the responsible in IT security departments</p>
Reactive
<p>[36] Send alerts regarding fraudulent messages found</p> <p>[37] Disable User Account</p> <p>[38] Block a Malware Domain</p> <p>[39] Block any malicious sender IP addresses</p> <p>[40] Remove a malicious file from the computer</p> <p>[41] Block a malicious email address</p>

Table 4 - Session Hijacking

Session Hijacking
Preventive
<p>[42] Encryption of data in transit using TLS 1.2 or newer to prevent sniffing style attacks.</p> <p>[43] Ensure usage of encryption or hashing schemes that are strong enough for today's standards such as: SHA256 for hashing, AES-256 GCM, CTR or CBC.</p> <p>[44] Usage of salt and true randomness algorithms to prevent guessable sessions</p>
Reactive
<p>[45] Multi Factor Authentication to check against identity of the user.</p> <p>[46] Regenerating of Session ID after a Successful Login and Expiration of the Session at Logout and all Sessions at Password Changes</p>

2.1.2 Disruption of data or HW loss

This section describes the following classes of threats: Data tampering, Repudiation, Information disclosure.

Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.

Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise. For example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non-repudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.

Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it. For example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.

Sensitive data and files that should not be subject to un-authorized modification in Resisto is protected via a specific module using the novel MIDA framework that is more extensively described in "D2.7 RESISTO platform and tools reference architecture – final" section 3.4.4, repudiation is prevented by proper auditing in place and audit trails.

Table 5 - Disruption of data or HW loss

Disruption of data or HW loss
Preventive
<ul style="list-style-type: none"> [47] Continuity and Disaster Recovery plans in place (Regular updates and testing of Continuity and Disaster Recovery Plans) [48] Geographical redundancy of hw/sw defined for critical systems [49] Backup and recovery measures in place [50] Protect sensitive data via encryption of disks and other media devices. [51] Limited access to HW/SW according to Access Policies [52] Organized data in segments protected according to sensitivity levels, including the development of data access policy [53] Tamper protection for security-critical components [54] Protection against theft and third-party influence [55] Protection against illegal use of removable media [56] Removable media locking [57] Network segmentation [58] Regular Security Reviews [59] Implement continuous availability checks for HW/SW systems and services [60] Usage of OSINT (Open Source Intelligence) tools to monitor popular internet services against leaked information [61] Implementation of anomaly detection methods for data transferred between employees and external connections [62] Development of responsible disclosure & bug bounty programs to encourage security researchers to report vulnerabilities identified in a defined scope
Reactive
<ul style="list-style-type: none"> [63] Backup and disaster recovery plans and procedure for data [64] Switch procedure on stand-by HW/SW systems

2.1.3 Network reliability

Failures in Communication networks must provide a certain level of availability which is considered in telecom network design. Failures that can happen with a relevant probability and that can be implemented at a reasonable cost to support availability guarantees stated in service-level agreements. The countermeasures implemented to this extent can be used to counteract the effects of natural disasters or intentional cyber or physical attacks. Network element reliability is defined as the probability of a network element to be fully operational during a certain time frame [16]. Network element availability is the probability of a network element to be operational at one point in time.

Network integrity is the ability of a network to provide the desired QoS to the services, not only in normal (i.e., failure-free) network conditions. Network survivability is a subset of integrity; it is the ability of a network to recover the traffic in the event of a failure, causing few or no consequences for the users [17].

The causes of an unplanned network failure due to external causes such as electricity breakdown, lightning, storm, earthquake, flood, digging accident, vandalism, sabotage or hacker attacks.

Since it is not so easy to estimate the impact of some dramatic failures (such as major earthquakes) a practical strategy used is to identify the most frequently occurring failures, and to provide measures to overcome them[25]

Table 6 - Network failures

Network Reliability	
Preventive	
[65]	Single link or node failure procedure and extra link or nodes in place when de-centralized solution applies (duplicate critical nodes)
[66]	Modeling of shared risk groups (SRG)
[67]	Using Ring protection schemes in the transport layer
[68]	Network design to guarantee critical users and services
[69]	Spare parts available on sites close to critical equipment (the number and types of available spare parts influences the time to repair)
[70]	Armored casing for cables or locating cable deep in the ground
[71]	Limited access to cable and equipment locations
[72]	Temperature and smoke detection system, automatic sprinkler system, direct connection with the fire department
Reactive	
[73]	Network monitoring and network, nodes and links recovery or resilience schemes, including ring protection, path recalculation, stand-by switchover (automatic, manual, hot, cold, ect.).
[74]	Trouble Ticketing procedure in place for on site repair
[75]	Alert fire department if no automation is implemented
[76]	Alarm system with notifications of un-authorized or forced access

2.1.4 DoS attacks handling

Denial of service (DoS) attacks deny service to valid user, for instance flooding its target machine with so much traffic that it prevents it from being accessible to any other requests. The target machine is kept busy responding to the traffic it is receiving from its attacker and therefore rightful users cannot get the required services. A distributed denial of service (D-DOS) attack adds a many-to-one dimension. Protecting against DoS threats improves system availability and reliability.

Dos can be to any part of the network at all protocol levels and devices (i.e. phones, routers, switches). Auditing and monitoring of this type of activity should be in place to uncover patterns that could indicate an attack. Example of this are phone dialing, SYN flood, UDP flood, MAC flooding, etc.

There are multiple attacks techniques to perform DOS such as:

- DOS based on attack tools that leverage malicious applications to embed Denial of Service techniques, such as Slowloris, [Stacheldraht](#). These are difficult to prevent because sometimes they use legitimate stress testing tools such as LOIC or HOIC.
- Application-layer attacks are usually exploits that leverage software vulnerabilities to consume service resources such as RAM, Disk, GPU, CPU cycles. These techniques can only be blocked at Layer 7 and usually with specialized solutions since the footprint is low, and

most of the time the requests look benign. Examples of such attacks are: HTTP slow POST DoS attack, Challenge Collapsar (CC) attack

- Degradation-of-service attacks are usually DDoS attacks that slow down applications and services but not making it unavailable. This technique is quite difficult to detect but can introduce unexpected financial losses, for eg. search engines penalize sites that are loading slower
- Peer-to-peer attacks are attacks that leverage vulnerabilities in peer-to-peer applications, such as DC++ or torrents and use resources of the network in a malicious way
- Permanent denial-of-service attacks or PDOS are attack techniques that, when used can make a system unusable in such a way that require replacement or reinstallation of the hardware
- Reflected / spoofed attack involve sending crafted or forged requests to a very large number of computers, that in return reply the response to the victim which translates into a volumetric denial of service
- Amplification attacks leverage that particular protocols and services are extremely verbose and return large amount of data. Combined with a spoofing techniques, an attacker can send a particular number of bytes to a vulnerable service, whereas the service replies with data to a victim but with an amplification factor. For eg, Memcached before 1.5.6 was previously used to perform such attacks with a factor for 50000, meaning that if you send 1MB/s to a service he will reply to the victim with a maximum potential of 50GB/s. Other popular services are DNS, NTP, BitTorrent, Chargen, QOTD etc.

Mitigation techniques can use a combination of tools to increase the attack detection, better classify the traffic request and response, aiming at better identify legitimate traffic and anomalies. Such techniques can involve bandwidth management hardware in conjunction with routers and switches, blackholing and sinkholing, IDS/IPS, Firewalls, Upstream filtering etc.

The DDOS can be classified as (1) Volumetric attacks, that overwhelm a network's infrastructure with bandwidth or resource requests, (2) TCP state attacks, where state of the TCP protocol is used to use up all resources in network nodes and (3) Application layer attacks to Layer 7 of the protocol stack. Locate data centers in distributed locations and use hw resilient to DDoS attacks[19].

DDoS mitigation solution requires tools that support: detection, filtering and eventually revert cleaned traffic back to network applications. For detection, for instance some traffic patterns through signatures are baselined to detect different usage patterns, that are able to distinguish between normal system users and bots (e.g. hijacked web browsers or IoT devices).

Filtering using one of the following possible techniques: connection tracking, IP reputation lists, deep packet inspection[20], blacklisting/whitelisting, and/or rate limiting. Use of deep packet inspection tools able to filter and analyze traffic in layers trying to detect harmful traffic and applying filters to stop the menace on the specific layer.

Mitigation action can be to lower or stop traffic coming from the sources deemed part of the attack or cloud based solutions [21] that can provide an offload or in the worst case relocation in case of

DDOS attacks. In this latest case cloud-based solution will take care of receiving the malicious traffic from the original site to a scrubbing center, which can perform the cleaning and return the filtered traffic back for normal handling.

Table 7 - (D)Dos

(D)Dos	
Preventive	
[77]	Perform brute force attacks to find weaknesses and hanging modems.
[78]	Make sure only necessary phone numbers are made public.
[79]	Provide stringent access control methods that would make brute force attacks less successful.
[80]	Specify the maximum number of MAC addresses that can be learned on ethernet ports
[81]	dynamic packet filtering rules on MAC addresses installed by a AAA server
[82]	DMZ protection against unauthorized access from outside and controlled connection establishment from the LAN into public networks/services
[83]	Perform fuzzing against popular services such as http, telnet, DNS, FTP, POP, SMTP, etc.
[84]	Perform vulnerability scanning against systems to identify known vulnerabilities
[85]	Analysis traffic bandwidth (average, peak etc...) in the MEC or Service
[86]	Connectivity to the service (SIMs, users, IP sources etc...)
[87]	Caching and buffering
[88]	Packet filtering
[89]	IP traffic analysis (IP source, IP destination)
[90]	Perform stress testing against services
[91]	Data centers and nodes that can be configured to be redundant, shall be in different physical location, and networks access to them shall have diverse paths and possibly shall use different IP network segments, moreover, shall not have notable bottlenecks or single points of failure
[92]	Evaluate DDoS robust HW (network firewalls, web application firewalls, and load balancers can defend against protocol attacks and application-layer attacks, DDoS mitigation appliances
[93]	Allocate extra capacity in case of attacks
[94]	Adopt a cloud based solution for DDOS mitigation and/or direct management of DNS services
[95]	Monitor OSINT sources for botnet activity or threat activity
Reactive	
[96]	Block/Shun an IP
[97]	Monitor and audit for such activity.
[98]	Employ an IDS to watch for suspicious activity.
[99]	Set and enforce lockout thresholds both cyber and physical
[100]	Limit the incoming number of connections and traffic dimension
[101]	Disable Switch Port
[102]	Activate cloud based mitigation solution
[103]	Disable affected systems, services or application features

2.1.5 Natural Disaster

Natural disaster (weather, flood, pandemic or earthquake) countermeasures are related to the possibility to operate the infrastructure when major natural events happen in a certain area. They are very similar to the ones described in the availability section apart from the fact that the damage can impair a large number of equipment at the same time.

Table 8 - Service Continuity

Service Continuity	
Preventive	
[104]	Continuity plan in place
[105]	Disaster Recovery procedures in place for large disasters with spare equipment that can be moved easily to the disaster area (i.e. in a box solutions)
[106]	Geographical redundancy of hw/sw defined for critical systems
[107]	Plan for spare capacity of resources to allow relocation of services in case of disaster
[108]	Monitor public sensor networks (i.e. seismic, weather station, flood sensor networks)
Reactive	
[109]	Switch procedure on stand-by hw/sw systems
[110]	Operate with temporary equipment installation

2.1.6 Physical Security – Physical Intrusion

Physical security countermeasures address physical intrusion concerns that could affect the infrastructure and the assets. The physical protection of telecom infrastructure assets (i.e. data center) can be implemented with multiple layers of security. The first layer of protection may include fences, gates, lighting systems enhanced with intrusion detection sensors (i.e. fibre optic, vibration sensors, perimeter CCTV systems, etc.). The second layer which is located within the area of the infrastructure includes patrolling of security personnel, badge checks, incident response procedures, emergency communications, video/audio surveillance systems, etc.). The last level of security refers to the means of securing the building's and equipment. Such means may include, intrusion detection systems, monitored electrical/mechanical door locks, smart access control, CCTV systems, etc.

Table 9 - Physical Intrusion

Physical Intrusion	
Preventive	
[111]	Remove any dense vegetation for the perimeter area
[112]	Identify all critical resources in the area (fire stations, hospitals, etc)
[113]	Utilize topographic plans to assess adjacent land use
[114]	Select and design barriers based on threat level
[115]	Install security lighting
[116]	Install CCTV (Video/Audio Surveillance) system
[117]	Prohibit parking beneath or within a building
[118]	Designate entry points for commercial and delivery vehicles away from high-risk areas
[119]	Provide intrusion detection sensors
[120]	Anti-drone systems for the detection of possible aerial threats
Reactive	

- | | |
|-------|-----------------------------------------------------------------------------------------|
| [121] | Use spectrum analyzer to detect rogue stations |
| [122] | Use vehicles (patrol units) as temporary physical barriers during high risk period |
| [123] | Make proper use of signs to inform interested group of people (i.e. evacuation process) |
| [124] | Remote control to restart electronic systems in case of temporary failures |
| [125] | Security personnel to verify an occurred event that may be threat |
| [126] | Usage of alternative video feeds (adjacent cameras, UAV systems) |

Table 10 summarizes the applicability of the countermeasures for each use case. Since some of these countermeasures can be seen more generally as good practices and not strictly significant in the context of the use case, classification is based on three values:

“-“ not relevant

“*” relevant countermeasure but not key to build the use case (to be used, optionally)

“**” key countermeasure

D means that the countermeasure is planned to be demonstrated in the framework of the respective WP7/8/9 pilots.

Table 10 - Use cases to countermeasures mapping

UC/Count.	1-OTE	2-OTE	3	4-BTC	5-TIM	6-ORO	7-RTV	8-RTV	9
[1]	D**	-	**	D**	**	**	**	**	*
[2]	D**	-	**	*	*	**	**	**	*
[3]	**	-	**	-	*	*	**	**	*
[4]	**	-	**	*	**	*	**	**	*
[5]	**	-	**	*	*	*	**	**	*
[6]	*	-	**	*	*	-	**	**	*
[7]	*	-	**	-	-	-	**	**	*
[8]	**	-	**	*	**	*	**	**	*
[9]	**	*	**	*	*	*	**	**	*
[10]	**	-	**	*	*	*	**	**	*
[11]	**	-	**	*	*	-	**	**	*
[12]	D*	-	*	*	*	*	*	*	*
[13]	*	-	**	*	*	-	**	**	*
[14]	*	-	**	*	*	*	**	**	*
[15]	*	-	**	*	-	-	**	**	*
[16]	-	-	*	*	**	-	*	*	-
[17]	*	-	-	-	-	-	-	-	*
[18]	**	-	**	*	D**	*	**	**	*
[19]	*	-	**	*	*	-	**	**	*
[20]	D**	-	**	-	*	-	**	**	*
[21]	D**	-	**	*	**	**	**	**	*

[22]	**	-	**	*	**	**	**	**	*
[23]	**	-	**	*	**	*	**	**	*
[24]	*	-	**	*	**	*	**	**	*
[25]	*	-	**	*	*	-	**	**	-
[26]	*	-	**	-	*	-	**	**	-
[27]	*	-	*	-	-	-	*	*	-
[28]	**	-	*	-	-	-	*	*	-
[29]	*	-	**	*	*	-	**	**	-
[30]	**	-	**	*	*	-	**	**	-
[31]	**	-	**	*	*	-	**	**	-
[32]	**	-	**	*	**	-	**	**	-
[33]	*	-	*	-	*	-	*	*	-
[34]	*	-	*	-	*	-	*	*	-
[35]	*	-	*	-	**	-	*	*	-
[36]	*	-	*	*	**	-	*	*	-
[37]	**	-	**	*	*	-	**	**	-
[38]	**	-	**	*	*	-	**	**	-
[39]	*	-	**	*	-	-	**	**	-
[40]	**	-	**	*	*	-	**	**	-
[41]	**	-	**	*	*	-	**	**	-
[42]	*	-	**	*	*	*	**	**	*
[43]	**	-	**	**	**	**	**	**	
[44]	**	-	**	**	**	**	**	**	
[45]	**	-	**	*	*	*	**	**	*
[46]	*	-	**	*	-	*	**	**	*
[47]	D**	**	**	**	**	**	**	**	D**
[48]	**	**	**	**	D**	**	**	**	D**
[49]	**	**	**	*	**	**	**	**	D**
[50]	**	-	**	*	**	**	**	**	*
[51]	*	*	*	*	*	*	*	*	*
[52]	**	-	**	*	**	**	**	**	*
[53]	*	-	**	**	**	*	**	**	*
[54]	**	-	-	*	-	-	-	-	*
[55]	**	-		-	**	-			*
[56]	*	-	**	*	-	**	**	**	*
[57]	**	**	**	*	*	**	**	**	*
[58]	*	-	*	*	**	-	*	*	-
[59]	**	-	-	*	-	-	-	-	-
[60]	*	-	-	-	**	-	-	-	-
[61]	*	-	**	**	**	*	**	**	-
[62]	-	**	**	*	D**	**	**	**	*

[63]	D**	**	**	*	D**	**	**	**	D**
[64]	D*	**	**	D**	**	**	**	**	*
[65]	D*	**	**	-	*	*	**	**	*
[66]	-	-	**	*	*	*	**	**	*
[67]	-	**	**	*	*	**	**	**	**
[68]	-	**	**	*	*	*	**	**	*
[69]	*	**	**	*	**	**	**	**	*
[70]	**	*	**	**	**	**	**	**	*
[71]	-	**	**	*	**	*	**	**	*
[72]	*	**	**	D**	-	**	**	**	D**
[73]	-	*	**	*	-	**	**	**	*
[74]	-	**	**	*	**	*	**	**	*
[75]	**	*	**	**	D**	**	**	**	**
[76]	D**	-	D**	-	-	*	D**	**	*
[77]	-	-	D**	-	-	-	D**	**	-
[78]	**	*	D**	*	-	**	D**	**	-
[79]	D*	-	D**	*	*	**	D**	**	-
[80]	*	-	D**	*	*	*	D**	**	-
[81]	**	-	D**	**	*	**	D**	**	*
[82]	*	-	D**	-	-	*	D**	**	*
[83]	**	-	D**	*	*	*	D**	**	*
[84]	-	-	D**	-	-	-	D**	D**	-
[85]	-	-	D**	-	-	-	-	D**	-
[86]	-	-	-	-	-	-	D**	-	-
[87]	-	-	-	-	-	-	D**	-	-
[88]	-	-	-	-	-	-	D**	-	-
[89]	*	**	**	**	-	*	**	**	*
[90]	*	**	**	**	D**	**	**	**	D**
[91]	-	-	**	**	-	**	**	**	*
[92]	-	**	**	D**	*	**	**	**	**
[93]	-	*	**	*	-	**	**	**	-
[94]	-	*	**	*	-	**	**	**	-
[95]	**	-	**	*	*	**	**	**	-
[96]	**	-	**	*	*	*	**	**	*
[97]	**	-	**	*	*	**	**	**	*
[98]	**	-	**	*	*	*	**	**	-
[99]	*	-	**	D**	*	**	**	**	-
[100]	*	-	**	*	*	**	**	**	-
[101]	*	**	**	*	*	*	**	**	-
[102]	**	**	**	*	**	**	**	**	**
[103]	*	*	*	*	*	*	*	*	*

[104]	-	**	**	*	**	*	**	**	*
[105]	D**	D**	**	**	**	**	**	**	D**
[106]	**	**	**	D**	**	*	**	**	**
[107]	**	**	**	**	**	*	**	**	**
[108]	**	**	**	D**	D**	*	**	**	D**
[109]	**	**	**	*	*	**	**	**	*
[110]	*	*	**	-	-	*	**	**	-
[111]	-	*	**	*	**	**	**	**	-
[112]	-	**	**	*	*	*	**	**	-
[113]	*	*	**	*	*	*	**	**	-
[114]	*	*	**	*	**	**	**	**	-
[115]	**	D**	**	*	**	**	**	**	*
[116]	**	**	**	*	-	*	**	**	-
[117]	*	*	**	*	-	*	**	**	-
[118]	**	*	**	*	D**	**	**	**	*
[119]	-	**	**	*	**	*	**	**	*
[120]	D**	D**	-	*	-	-	-	-	*
[121]	**	**	-	*	-	-	-	-	-
[122]	*	*	-	*	*	*	-	-	-
[123]	*	*	-	*	*	**	-	-	-
[124]	**	*	-	*	D**	**	-	-	*
[125]	**	**	-	**	-	*	-	-	*

3. MITIGATION FRAMEWORK

The mitigation framework, developed in RESISTO, supports the operator in reacting to a threat by means of workflows, which are activated to cope with specific threats detected by the RESISTO architecture, thus orchestrating available infrastructure resources.

In particular, the RESISTO system provides a Decision Support System (DSS) which guides and informs the operator helping him to make the right choice.

The RESISTO DSS consists of three components:

- Alarm manager Dashboard: notifies the alarm and displays all the data associated with it.
- Workflow manager: guides the user's operations in carrying out the tasks assigned to him according to the alarm to be managed
- Risk Predictor: assesses the impact of the overall state of the system and the "cascade" impact of an attack on all system components.

The RESISTO DSS is described in more detail in document D6.2 (Adaptors, DSS and Risk predictor).

3.1 Use Case: Disruption of major sporting event by combined physical & cyber-attack by a terrorist organization

The short term response actions indicated into D2.8 [2] are:

- 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/headend (i.e. to degrade the video quality from 4K to HD/SD) 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

Probably these response actions cannot be performed automatically by the RESISTO platform but the countermeasure workflow can be configured in this way:

- Perform analysis of attack consequences with Risk predictor
- Alert the maintenance Team to Restore take a recovery action
- Wait for the problem resolution monitoring risk predictor
- Write the alarm report
- Close the alarm

The workflow schema is shown in Figure 2.

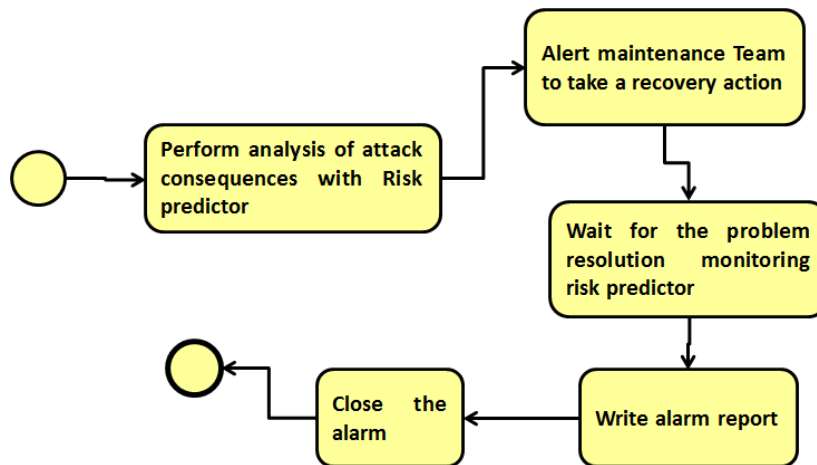


Figure 2: Disruption major event workflow

3.2 Use Case: Maritime Safety and Emergency Case

This use case allows you to test the effectiveness of the RESISTO platform in the event of a physical attack resulting in a Cyber attack. Physical intrusion is detected using an anti-intrusion system. If the intrusion is followed by abnormal traffic, it is very likely that these two events are related. In the case of this type of combined attack the implemented workflow is the following:

- Perform analysis of attack consequences with Risk predictor
- Alert Security team on the field using EWCF to verify Physical Attack
- Alert IT Security to protect for Cyber Attack
- Wait for the problem resolution monitoring risk predictor
- Write the alarm report
- Close the alarm

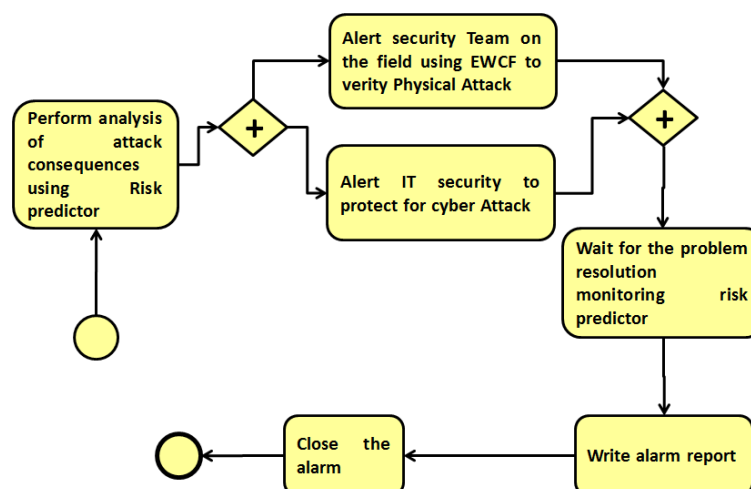


Figure 3: Maritime use case workflow

3.3 Use Case: PPDR Virtual Operator Maritime Safety and Emergency Case

The objective of the integration with RESISTO platform is to have a real time response in order to mitigate the attack. The RESISTO Short Term should detect the cyber-attack as soon as possible in order to avoid the negation of service. RESISTO should provide first the corresponding alert message to the corresponding profiles and moreover some recommendations on how to proceed to avoid the shut-down of the network. In this case the the possible automatic mitigation action is to disable the network slice attacked calling the network orchestrator.

The workflow actions are the following:

- Perform analysis of attack consequences with Risk predictor
- Ask the operator: “do you want to disable the attacked network slice?”
- If yes: Disable the network slice
- If no: the operator can perform other manual mitigation actions
- Wait for the problem resolution monitoring risk predictor
- Write the alarm report
- Close the alarm

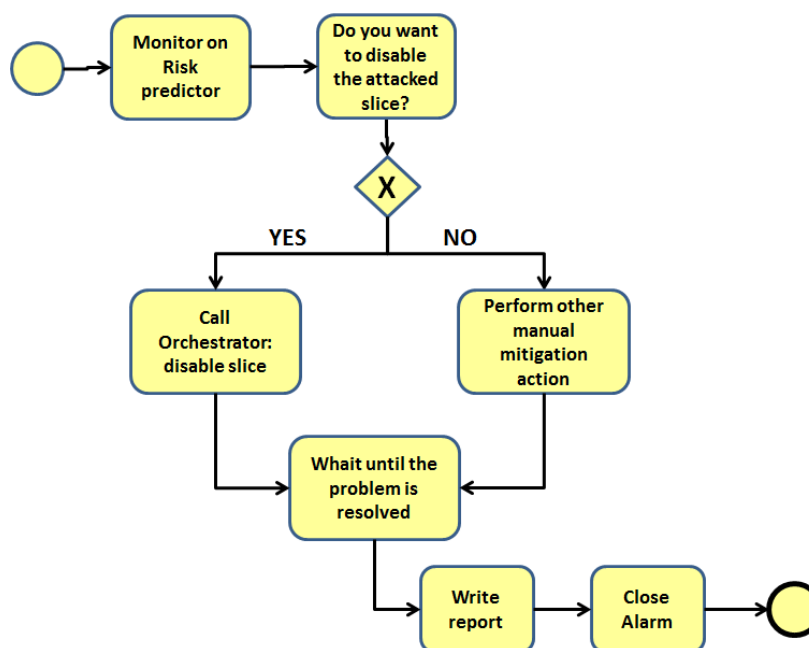


Figure 4: PPDR workflow

4. EMERGENCY WORKING COMMUNICATION

The scope of the Emergency Warning Communication (EWC) Function is to create a communication channel between the threat findings of the RESISTO platform and the teams that physically shall operate where actions can be carried out as a response to the threats following a pattern typical of the public safety applications.

When handling of threats needs a team to be allocated to the handling of a specific threat event that involves both a physical and a cyber-attack part the Emergency Warning Communication Function to dynamically setup the team and handle the communication between team member and RESISTO application.

Each time a team must be formed and assigned to an on-going attack this is implemented using the EWC service.

In many cases more than one person must be involved in the application of the countermeasures in case an attack is performed.

In this chapter we will describe in which of the use cases reported in D2.8 [2] the EWC can be used as a tool as a refinement of the real time response and mitigations actions implementations.

4.1 Use case 1 Core Network Failure caused by Physical & Cyber Attacks to telecommunication sites

Sub case 1 – Storytelling

- After the DoS attack is detected and a cyber attack event is issued by RESISTO. RESISTO suggests a prevention / mitigation action, i.e. deactivation of the switch and redirection of normal traffic to the users, EWC can be used to send the instructions

Sub case 2 – Storytelling

- In subcase 2, an unauthorized sperson breaches the secure perimeter and tries to gain access to the interior of the building.
- It is detected by RESISTO's sensors for video and audio analytics and a perimeter breach event is issued. Moreover OTE's assets in the vicinity are identified as "compromised" by RESISTO. This information is sent to the EWC to the team that is responsible for the "compromised" site.
- A prevention/mitigation action is suggested and the malware is removed from the network.

Both subcases represent realistic cyber-physical attacks targeting critical telecommunication infrastructure and cannot be detected and mitigated efficiently by conventional security systems already used by telecom providers. Although separate physical and cyber security mechanisms may be in place.

4.2 Use case 3 Telecommunication sites

Sub case 1 – Storytelling

The EWC can be used with small variations in several scenarios to synchronize the people that are responsible of the physical security and the NOCs. Someone not-authorized is accessing the remote site where the maritime site is located.

The various steps of this use case are the following:

- An un-authorized attempt of accessing a remote site is made and an alarm is sent to the “physical security” team through the main security interface that is also able to connect to the cameras (this is not connected directly to RESISTO).
- Using a different device IoT deployed on site by RESISTO, separate access events are identified by RESISTO, this access (for instance looking at the local server logs or based on the fact that the visit was not planned and alarms have been raised at the telecom company NOC) and sends this Event to the group “security company” that has EWC App that is installed on a tablet in the security room. The RESISTO responds by issuing a damage inspection order to “physical security” team.
- The “physical security” team shall perform a damage inspection procedure using security cameras, inspecting the provider’s premises affected by the “suspect” access. The “physical security” team sends an extensive building and asset damage event after detecting the damages at the provider’s telecom assets.

Without the RESISTO system, the un-authorized access would not be identified, and inspection would not be as responsive. Even though a mitigation action could be initiated, it wouldn’t be the optimal one, since the information on the loss of network resources caused by the people that accessed the site would not have been correctly addressed. Even in this case, the overall response of the network and the application of the mitigation strategy would be significantly slower compared to the case where the RESISTO system is used to automate and facilitate the whole procedure.

4.3 Use case 5 Protection of Cloud Storage Services

Sub case 1 – Storytelling

Rack or door sensors detect a first event about a physical access and consequently send an alarm to the RESISTO platform. The intruder will perform several actions that RESISTO platform collecting and correlating the events as detailed in D2.8 [2].

- An unauthorized cybercriminal accesses a protected area
- attacker accesses to one system with a theft credential
- start a program from a privilege folder or temporary folder of system to change one or more information stored on system:
 - Data contained on sensitive files (system configuration, firmware of router, etc.)

- time of creation of sensitive files

As a result of RESISTO correlation the actions will be identified as malicious and a dynamic virtual team will be created to handle the recovery actions which can consist of a combination of the following, send the event details to the security guard and/or to the SOC team and/or IT Security group using EWC function depending on the findings. For instance the SOC team will be instructed to restore the tampered with file and resume the normal operation, the security guard will receive other detailed instructions on the check to be made (e.g. as checking for the presence of a rogue AP) and the IT Security group will receive details on the files that have been modified and how to revert the changes.

5. EXTENSIONS OF THE SDS MODEL

5.1 Multi-objective countermeasure optimization

The problem of optimizing the deployment of network countermeasures in a Software Defined Network (SDN)/ Network Function Virtualization (NFV) environment and the possible use of multi-objective evolutionary algorithms has been introduced in **Errore. L'origine riferimento non è stata trovata..** A brief summary is hereby reported for the sake of clarity.

Many network threats can be framed as re-routing problems. This include man-made attacks (e.g., route critical traffic avoiding untrusted/compromised nodes) as well as the effects of a natural disaster (e.g., maintaining network availability even after the disruption of a part of a network caused by a natural disaster). Furthermore, modern networks require a finer approach to routing. Scenarios that require enhanced routing include, but are not limited to, complying with Service Level Agreements (SLA) and network slices requirements, ensure that only trusted devices are part of a path and minimize the energy consumption of the network. Summarizing, novel routing solutions should take into account:

- Compliance with SLA and other performance constraints
- Resiliency
- Green constraints (energy saving)
- Trustworthiness of the device

While the impact of routing on resiliency may not be obvious, it is widely known that overloading equipment may have a detrimental effect on its service life. Findings in literature seems to confirm this heuristic [3][2], suggesting how an higher workload ultimately leads to higher failure rate for network elements. Furthermore, energy-aware routing algorithms are often based on switching off underutilized portions of the network. This procedure increases the load on the remaining part of the network thus reducing the service life of the switched off devices as well due to thermal effects **Errore. L'origine riferimento non è stata trovata..**

Trust also represent an important metric in a SDN/NFV network, as devices can be compromised on a software level [1]. Recent research in security has also shown that software isolation can be broken in a currently unavoidable manner **Errore. L'origine riferimento non è stata trovata.****Errore. L'origine riferimento non è stata trovata..** Thus, untrusted traffic/Network Services (NS) instances should not share physical mediums.

In this scenario, determining a route for a network flow requires solving an inherently multi-objective optimization problem, as multiple and non-correlated metrics must be considered. The solution should allow for fast optimization and should have scalability with respect to the number of elements in the network. For this reason, evolutionary algorithms have been selected. The idea of applying evolutionary multi-objective optimization has been explored in the past **Errore. L'origine riferimento non è stata trovata.****Errore. L'origine riferimento non è stata trovata.****Errore. L'origine riferimento non è stata trovata.****[9]Errore. L'origine riferimento non è stata trovata..** However, to the best of our

knowledge, research in the RESISTO project has been the first to consider the joint problem of the energy-efficiency/reliability trade-off as well as other SLA/quality of service metrics.

The algorithm selected for this procedure is the Non-dominated Sorting Genetic Algorithm-II (NSGA-II) **Errore. L'origine riferimento non è stata trovata.** NSGA-II has been selected based on the following criteria:

- it has low computational complexity with respect to other Multi-objective evolutionary algorithms;
- it applies an elitist non-dominated selection, thus preserving solution of past iteration based on their performances, favoring non-dominated solutions (see **Errore. L'origine riferimento non è stata trovata.** and **Errore. L'origine riferimento non è stata trovata.** for a review of the terminology);
- it uses a diversity preserving principle.

As was described in **Errore. L'origine riferimento non è stata trovata.**, the iteration of a genetic algorithm can be summarized as follows:

1. to evaluate fitness of the current population. Terminate the algorithm if the maximum number of iterations is reached;
2. select the population for mating based on fitness level;
3. mate the current population;
4. randomly introduce mutations in the population;
5. go to 1.

NSGA-II alters the Selection process (step 2). More specifically:

1. non-dominated fronts are computed. Basically, individuals are clustered into groups. Individual in the groups do not dominate each other;
2. select up to n individuals (n being a user-selected parameter), from the best non-dominated fronts. If there is more than one individual in the last front, the most diverse solution amongst the remaining one is selected.

A more complete discussion of NSGA sorting procedure is reported in **Errore. L'origine riferimento non è stata trovata.** Then, the algorithms proceed with ordinary crossover and mutation. For the

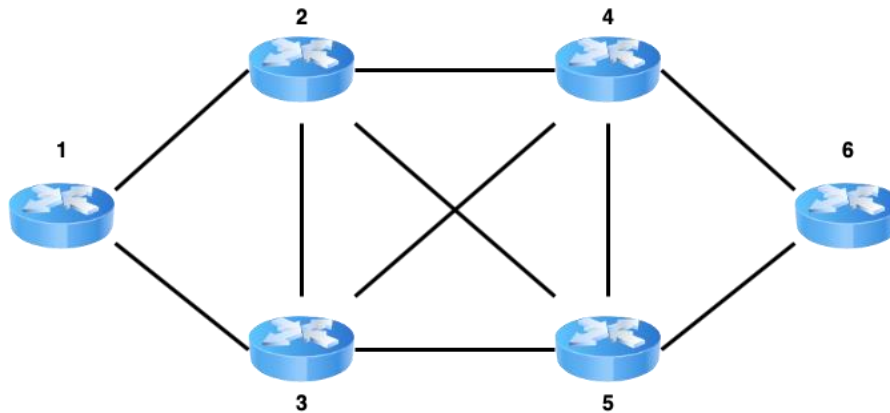


Figure 5: Example topology with nodes enumeration.

purpose of network routing, however, ordinary crossover and mutation could lead to substantial inefficiency. More specifically, crossover and mutation operations normally proceed by mating/mutating a binary-encoded representation of the individuals. These operations can result in non-valid individuals, i.e. paths that are not physically available. In literature, this problem is often solved by verifying the validity of the individuals after the crossover and mutation, eventually removing individuals failing the test and performing again the procedure. However, in the case of network paths, a large number of configurations is not physically possible and thus the algorithm could end up wasting a large amount of time in this step. To cope with this issue, custom crossover and mutation functions based on an integer encoding of paths have been developed. Given a topology, nodes are numbered incrementally, as is shown in Figure 5. A path between two nodes is thus encoded as a sequence of integers, representing one of the nodes.

The crossover function operates on path encoded in this manner. Given two paths, the valid merging points between the paths are enumerated. Then a one-point crossover procedure is applied randomly selecting the merging point among the valid ones. More specifically, given two paths p_1 and p_2 :

- For each element in p_1
 - For each element in p_2 , check if this is a valid connection
 - If it is and the resulting path does not contain loops, add $(\text{pos}(p_1), \text{pos}(p_2))$ to the list of valid merging points, where $\text{pos}(p_1)$ is the currently examined element in p_1 and $\text{pos}(p_2)$ is the currently examined element in p_2 .
- Select a random valid merging point
- Perform a one- point crossover between p_1 and p_2

An example of this procedure, referred to the topology of Figure 5, is shown in Figure 6.

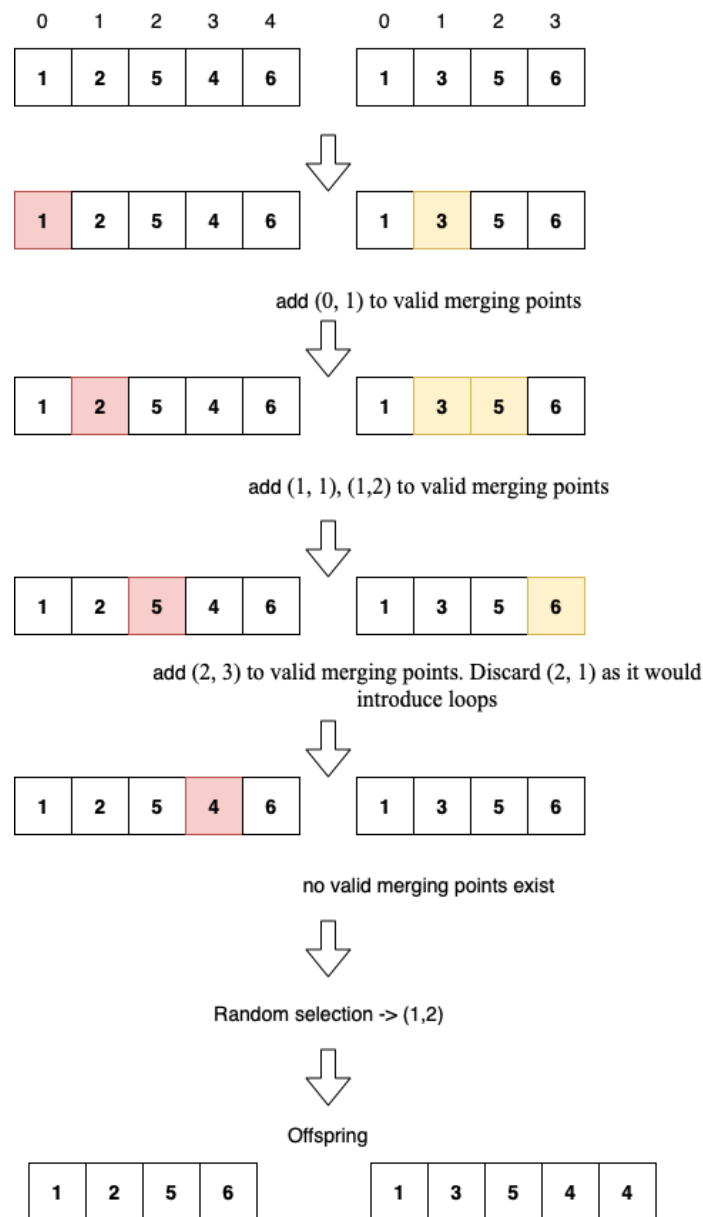


Figure 6: Example crossover procedure.

The custom mutation function considers mutations specific to the problem considered. Specifically,

three possible mutations are considered: shortening of a link, insertion of a node and flipping of a node. The first two mutations consider topologies where a connection could be shortened or elongated. An example of connection shortening is shown in Figure 7.

The third mutation is possible when there are two equivalent connections (i.e. a redundant path). In this case, the active node is exchanged. An example of this mutation is shown in Figure 8.

The custom mutation operators first enumerate the possible mutations, then selects a random one and applies it with probability p .

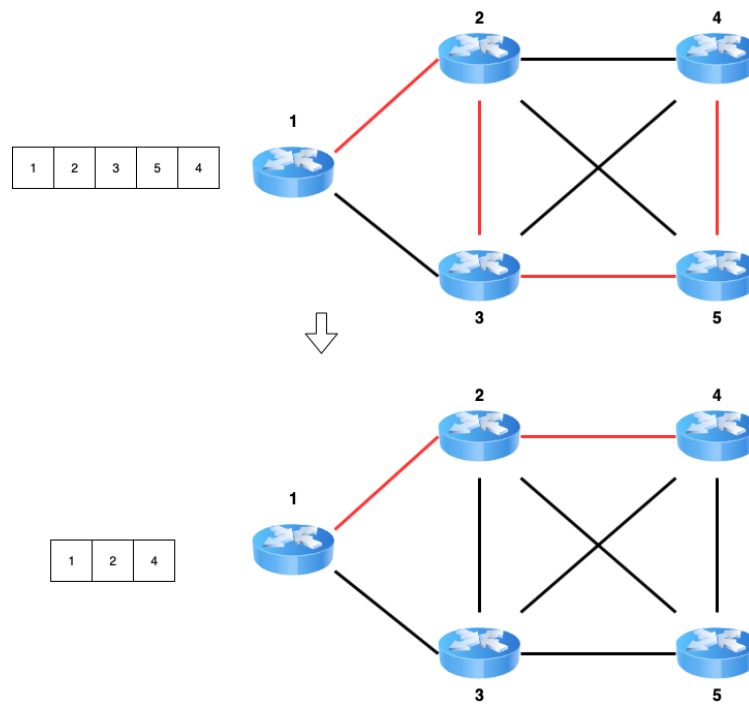


Figure 7: Example of deletion mutation.

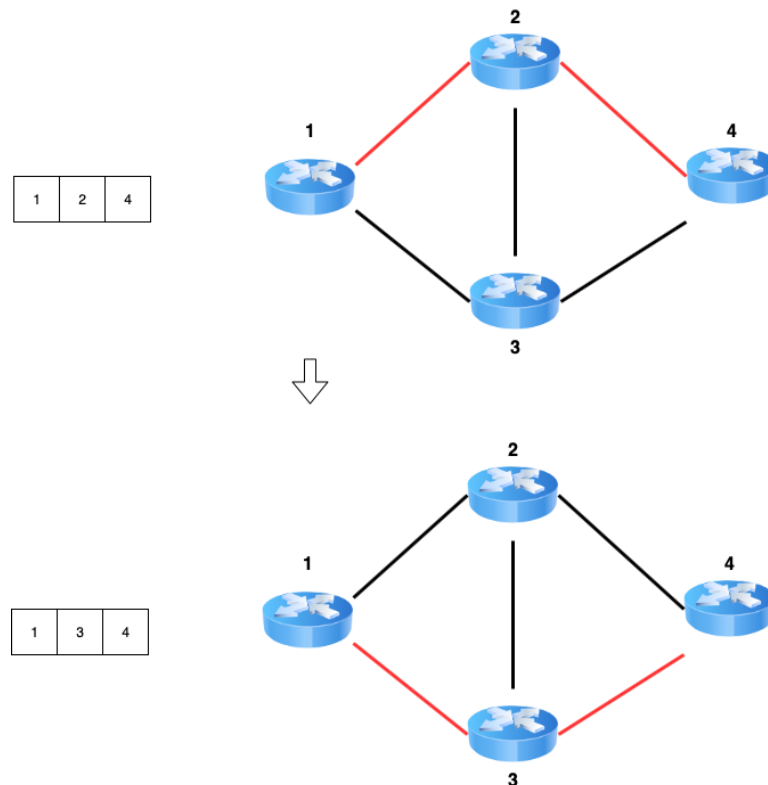


Figure 8: Example of flipping mutation.

The fitness function for the algorithm is specified in terms of two functions: a green routing fitness and a reliability-based function computed based on each element utilization. The first function is

calculated as the total energy consumption of the network. For the energy consumption of network elements, a simple model will be used in the first phase of experimentation. More specifically, switched on nodes will have a fixed energy absorption while switched on links will have an absorption that grows linearly with the hypothesized length. This function also incentivizes the optimization procedure to minimize the number of hops per path. If this measure will prove insufficient, an explicit path length constraint will be added.

The second function will use a quadratic cost function. Specifically, each network element will have a cost function yielding minimum cost when the usage percentage is at 60% and a quadratically growing cost if usage goes toward 0 or 100%. No cost will be added for switched off elements. This function incentivizes paths that do not tend to overload nor underutilize connections.

Finally, a constraints function will be added. Evolutionary algorithms typically include constraints in the form of very large penalties. In this case, a large penalty is assigned to solutions that violate a pre-defined SLA. In the first phase, the SLA will be specified only in terms of latency. This measure is due to the fact that is difficult to model jitter and packet loss for individual network elements, while a simple form of latency modelling for links can be done based on the length.

The algorithm will take input in the form of a set of flows to be routed. Each flow is specified in terms of a source and destination node, as well as a nominal bandwidth requirement. Furthermore, each flow will have a corresponding SLA specification as well as a priority value. The algorithm will sort the flows according to their priority and calculate a route. The calculated route will be applied on network elements so traffic can be routed. Then, the algorithm will proceed to the next flow, until the list of flow is empty. This procedure will be invoked when a network portion becomes unavailable. The flows that are currently using the aforementioned portion of the network will be passed to the orchestrator and re-routed.

5.1.1 On-going experimentation

Current activities are focused on evaluating the proposed solution. To this aim, it is necessary to determine an experimental protocol (i.e., test topologies and data) as well as state of the art algorithms for performances comparison.

Countermeasure optimization is most beneficial in highly redundant topologies. In this case multiple paths exist between two given nodes. In this context, human-based traffic engineering tends to be costly and error-prone. While one could design ad-hoc topologies to maximize the impact of the proposed solution, it is highly desirable to integrate well into existing topologies to improve the adoptability of the RESISTO approach.

In the first phase, countermeasure optimization will be tested on a simulated version of the GEANT topology [12]. A representation of the topology is shown in Figure 9.

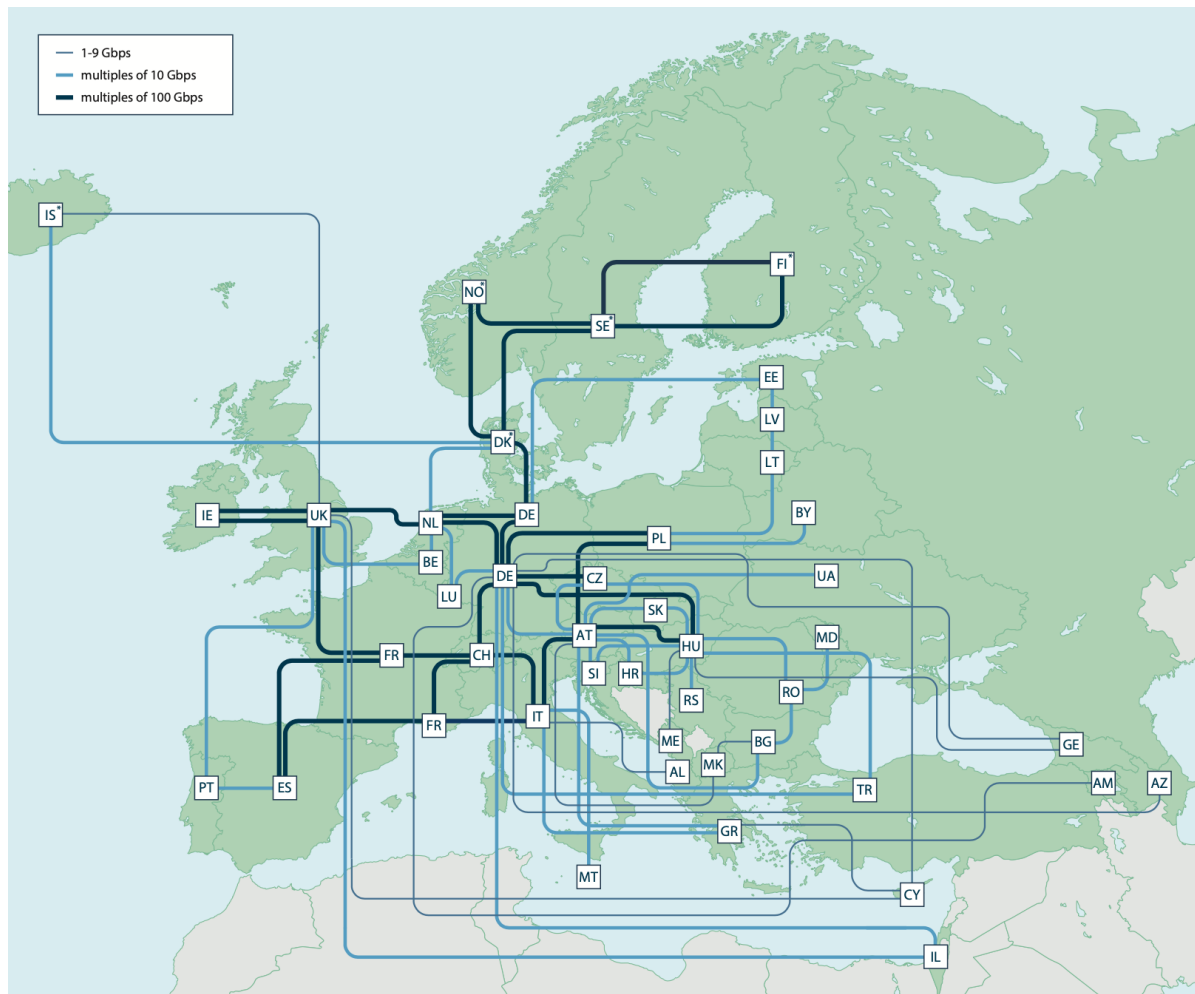


Figure 9: Representation of the GEANT network topology.

GEANT represents an interesting case study. First, it is a real, operating topology, thus yielding simulation results that are more realistic. Second, it offers numerous source-destination paths, thus allowing an evaluation of the countermeasure optimization capabilities. The COST 239 network topology [13] will also be considered in successive phases for analogous motivations and to improve comparability with other approaches, since it is widely used for evaluations in the state-of-the-art.

Selection of an appropriate traffic model for the evaluation is still ongoing. In the first phase, a Poisson process-based flow-level traffic model will be used. Thus, flows will be generated based on an exponential probability distribution controlled by a user-selected parameter, λ . Simulations with multiple λ (i.e. multiple traffic intensities) will be used in order to evaluate the proposed solution under a broad number of operating conditions.

The proposed solution will be compared to two algorithms: the first will be an ordinary shortest-path routing approach based on Dijkstra algorithm. This comparison will show the advantage of a routing algorithm that fully leverage SDN/NFV capabilities with respect to OSPF-like approaches, which represented the de facto standard in legacy networks.

To obtain data about the performances of the algorithm in comparison to modern approaches to routing, the algorithm introduced in **Errore. L'origine riferimento non è stata trovata.** will be implemented and tested. The algorithm considers the problem of energy saving beside networking constraints. Other approaches will also be considered in successive phases.

5.2 Software Defined Radio Security

In this section, an outline of the functionality and software-defined capabilities of RAN-MONITOR from the perspective of Software Defined Radio Security is given. RAN-MONITOR is one of the sensor-based tools being developed and used in RESISTO for Critical Infrastructure (CI) physical protection. This tool can be described as a cellular radio access threat detection and event generation system for massive deployment which allows all cells and operators to be monitored in real time in one target area.

RAN-MONITOR allows protecting cellular network resources in order to help the SDS platform to orchestrate and provide a mitigation response to a potential security attack to the Radio Access cellular Network.

In this context, the scenario is approached from two different perspectives according to the level of integration that the RAN-MONITOR tool has within the cellular network.

The first scenario represents the situation where RAN-MONITOR is monitoring an external cellular network, that is, the tool is not integrated with the network elements. In this case, RAN-MONITOR monitors the physical resources available in that network and determines the quality of the different frequency channels (bands) available for that operator based on metrics such as occupation and signal to noise levels.

The second scenario is the most extensive application of RAN-MONITOR, where the tool is able to integrate and communicate with cellular network elements in the infrastructure. In this case, information about the slicing or virtual resources and their mapping to physical resources can be monitored in order to protect the physical resources assigned to those slices and therefore detect any possible event/attack which degrades the quality of signal or performance, which is measured by a set of tool metrics.

Upon threat/attack detection and notification, an alarm is raised by the protection platform, in which case a response for mitigation can be coordinated with the network orchestrator. For example, if a jammer or DDoS attacker is targeting a cell specific channel where cell slices are allocated, the orchestrator based on the tool's monitored information about the network resources could instruct the different elements of the radio infrastructure to migrate a slice to another physical (frequency channel) resource which has better quality as measured by the RAN-MONITOR metrics

5.3 Machine Learning-based cell fault detection

5.3.1 Introduction

This section updates the information provided before in Deliverable D5.2 [1] (section 4.3.4). D5.2 presented the work methodology and key principles to be followed throughout the project, including the definition of the project stages, tasks, transitions and expected outputs. In the current Deliverable, the D5.2 work methodology is followed, and the problem setting is expanded with the following key advances:

- Business understanding description, regarding the current setting and expected outcomes
- Data understanding description, detailing data sources
- Initial take on modelling the core message presented by the data sources
- Presented a goal oriented description of the current approach to the use case
- Foreseen component integration communications, on expected inputs and outputs

This section also includes a brief description of how this work is planned to be integrated in RESISTO use case 9 “5G network response to a security breach”, to be deployed on Altice Labs (ALB) 5G testbed.

5.3.2 Overview

Alarm management systems are critical in today’s operations of network providers to enable the prompt resolution of network problems, therefore minimizing service interruption, impact on Quality of Service (QoS) and impact on Customer Experience (CeX).

From an operational perspective, existing alarm management solutions consume events from network elements (NEs) – in Radio Access Network (RAN), Passive Optical Network (PON) or other domains - and, based on a set of predefined human rules, convert those events into alarms. Typically, NEs are only able to report events when the problem is already affecting operations. This state of things defines the current fault management paradigm as a reactive one, based on a pipeline of diagnosis followed by damage mitigation and resolution actions.

Evolving from a reactive towards a proactive approach is paramount for operational management systems. Next generation operations will be mostly machine-based and human-assisted, relying on advanced mathematical algorithms and high-capacity computational systems to enable early detection of network problems and allowing immediate mitigation actions, therefore reducing the impact on the customer satisfaction.

Machine Learning (ML) technology provides the required toolset to evolve from a reactive paradigm to a proactive one. Applying ML techniques to available operational data makes possible to predict future problems and allows the implementation of new processes to prevent degradations from occurring, creating a new pipeline of precocious diagnosis followed by

preventive actions. This new paradigm will help enabling the nirvana of improved QoS and zero CeX impact due to operational issues.

The following subsections describe the cognitive challenge and technical approach to accommodate business requirements.

5.3.3 Business understanding

Alarm management today is typically addressed by a set of rules that can be very simple/direct (e.g. one network event mapping directly to one alarm) or more complex, involving several correlation levels to produce the alarms. These rules are made with expert knowledge and limited to the current understanding of the network dynamics. The constant evolution in software and hardware causes the manual rule creation approach to be both unpractical and inadequate.

The reaction to a network fault is supposed to fall into one of three categories:

1. Issues deemed automatically solvable
2. Issues requiring expert intervention and/or approval to solve
3. Issues requiring a team to be allocated to the site

An evolution in network fault management is expected to shift the balance of the first two categories. These are seen as correlated, where business seeks to reduce the need for expert intervention by increasing the scope of automatically solvable issues. The evolution of the third category advances the idea of proactive management, mitigating the impact on the network. The latter would also be expected to conform to additional business requirements, e.g. time constraints, thus increasing its complexity. All categories are expected to benefit from a shift to a proactive approach, either by advising or by acting.

Moving towards a cognition-based alarm management paradigm is paramount. This will enable evolving from a reactive to a proactive alarm management approach, in which Artificial Intelligence / Machine Learning (AI/ML) technologies and algorithms are fundamental to anticipate problems and pave the way for optimizing service operations. This is the cognition problem to be addressed - to predict an alarm. To this end, the available sources of information, of the current alarm management system, are to be explored.

5.3.4 Data Understanding

The available data sources supply the current Alarm management system of MEO, from Altice Portugal. These are characterized in Table 1, with greater insights detailed in subsequent subsections.

Table 11 - Source description

Source	Description
Alarm	Alarm state changes
Inventory	Equipment description
Trouble tickets (TTK)	Trouble ticket state changes

The data is ingested (via Apache Streamsets) by consuming events published by the alarm management platform in a Kafka bus. Thereafter, the retrieved alarms are stored in the data lake cluster, implemented through Hadoop.

Alarm data

The provided alarms represent a very wide network footprint in terms of the supported technology domains. Specifically, used alarm data includes RAN (e.g. 2G, 3G, 4G) and fixed (e.g. PON) access networks alarms, as well as backhaul and core alarmistic information. Besides the technology information, each alarm instance also includes the related inventory entry and the associated geographical area. Alongside spatial and domain information, alarms also include temporal information indicating all alarm instance state changes (e.g. start, update, end). Figure 10 illustrates the above described information.

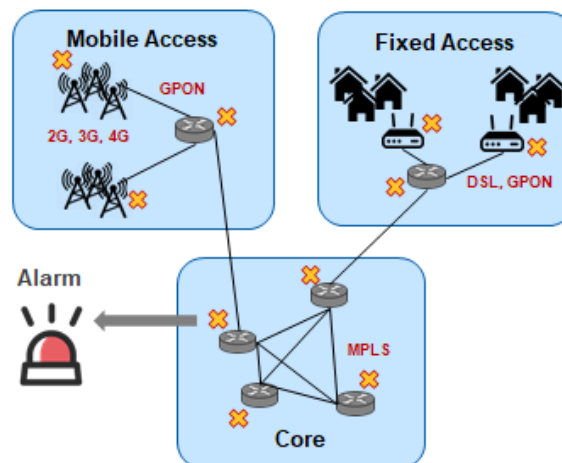


Figure 10: Alarm characterization – Spatial Perspective

The statement that current rules are too simplistic to capture the dynamic of the complex evolving network is a preconceived notion. This hypothesis was explored on Alarm events, as each possess a correlation identifier. The exploration targeted the inspection of simple rules, one of which was “Generator on” <-> “Air conditioner down”. This rule correlates Alarm problems and presents a simple issue, i.e. in case of a power outage, the generator must sustain core hardware needs only. The inspection of all other uncorrelated events, on the given days and locations, hinted at possible

extensions to said rule, e.g. reduced autonomy, affecting multiple technologies. This was then used to corroborate the initial hypothesis and highlight the need for data assisted rule discovery.

The key features of the Alarm events are shown in Table 12.

Table 12 - Alarm key features

Feature	Description
id	Alarm identifier
state	Alarm state, signaling whether it is open or closed
start_time	Timestamp of the initial Alarm event
end_time	Timestamp of the Alarm's closure, only available on the last event of an Alarm's lifecycle
location	Identifier for the geographic region of the occurrence
technology	Domain identifier
problem	Equipment specific problem description
ticket_id	Identifier for planned interventions
correlated_id	Alarm identifier, relating to its "parent"
equipment_id	Equipment component identifier

Upon further analysis, it was considered that a reshape of the available information could better convey the network dynamics. This is expanded in section 5.3.5 **Modelling**.

This data source is considered to be the most relevant in the use case, and might be enriched with information from the remaining sources, presented below.

Inventory data

The inventory maps a piece of equipment, in a given location, to an identifier. Its entries present a daily representation of the current equipment inventory, i.e. in an "UPSERT" fashion. This source is thought to be essential to the exploration process and, later on, solution interpretability. Its key features are shown in Table 13.

Table 13 - Inventory key features

Feature	Description
id	Equipment component identifier
location	Identifier for the geographic region where the Equipment is placed
installation_point	Identifier for the Equipment
equipment_name	Equipment component name

TTK data

This source, similarly to Alarm data, conveys the state changes of a given trouble ticket (TTK). The produced alarms can automatically open a new ticket on an external TTK management platform, by using predefined human rules to map the alarm into the TTK. The creation of a TTK may also map multiple uncorrelated alarms, given the context assessed by an expert. The TTK management platform works independently from the Alarm management system, not only containing tickets targeting alarms but also other network affecting events, e.g. planned interventions. It provides additional valuable expert information in the form of root cause and priority. The identified key fields are shown in Table 14.

Table 14 - Ticket key features

Feature	Description
id	Ticket identifier
state	Ticket state, signaling whether it is open or closed
location	Identifier for the geographic region of the occurrence
problem	Ticket specific problem description
priority	Ticket priority
root_cause	Identifier for the root cause of the problem
start_time	Timestamp of the initial Ticket event
end_time	Timestamp of the Ticket's closure, only available on the last event of an Ticket's lifecycle

The evaluation of the Alarm data enrichment process did not present a desirable coverage, i.e. few Alarm raise a trouble ticket. Although current processes do not use the referenced information, possible reshaping of the core message could still benefit from it.

5.3.5 Modelling

The Modelling stage assumes the existence of a dataset that represents the knowledge to be acquired, with as many examples as possible gathered from past observations so that it can be generalized to future events. In the alarm prediction use case, this data transformation phase converts alarm events into a new representation. Data is reshaped into network states, where it tracks the active alarm instances of a given set of equipment domain-problems occurring in a given location at a precise moment in time. Each network state results in a new contained and stateless snapshot capture on every change. This is further described in the following subsection.

Feature engineering

On the ongoing exploration, a set of features has been identified to transform the snapshots and its labels into a numeric matrix. The list of Alarm problems has been reduced to those of statistical significance and with expert knowledge. The feature list includes, but is not limited to, the following information assembled from the state:

1. If Alarm problem is active, for how long;
2. The time of the day of the snapshot;
3. The region of the snapshot.

A set of problem targets have been explored and the snapshot-to-event duration has been included in the new representation. This is thought to assist the learning process. Figure 11 presents an illustration of a snapshot.

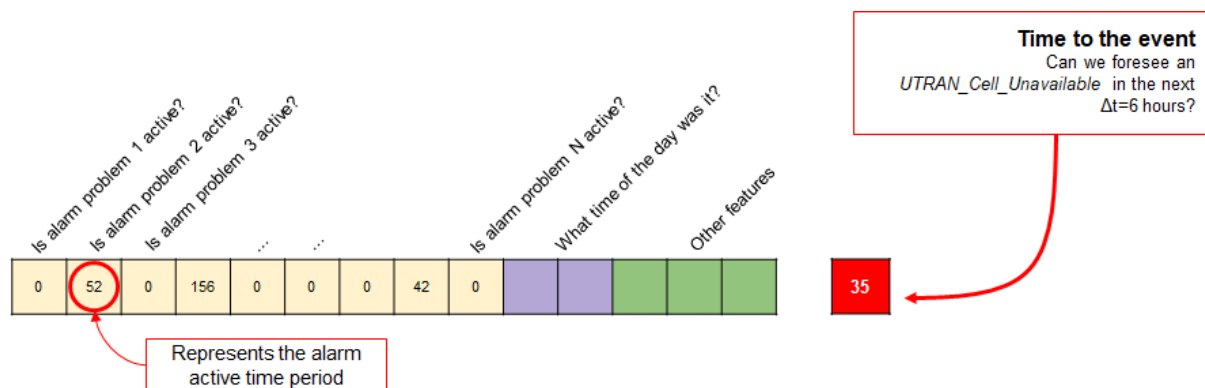


Figure 11: Network snapshot

In the current iteration, TTK information has not been included. Its inclusion on the new data representation and value of added insights must still be evaluated.

This reshaping of the core message is key to a successful learning process. Its ability to convey the network dynamics will continue to be evaluated and shaped accordingly.

5.3.6 Approaches

The use case relies on concise business understanding to shape its steps. The ongoing efforts must gather the needed insights and confront the previously stated business expectations, presented in Section 6.3.3 “Business Understanding”. To this end, the use case is following two approaches, described as follows:

1. Initial approach

- Focused on addressing RESISTO’s requirements
- Limited scope of descriptive and target features
- Expected to provide interpretable solutions to confront business experts
 - provide additional insights to grow the scope of automatically solvable issues

2. ALB Internal efforts approach

- Focused on addressing internal requirements
- Expected to provide a cell fault detection solution with time constraints

These approaches tackle the use case on different scopes and both insights are expected to shape the RESISTO cell fault detection solution.

5.3.7 Integration in RESISTO

The cell network fault detection is a component in the overarching RESISTO platform to be demonstrated in use case 9, as defined in D2.8 [2]. This led to the definition of communication interactions to enable future integration. In Figure 12, an illustration of the interactions between the ALB network testbed and the RESISTO platform, is provided.

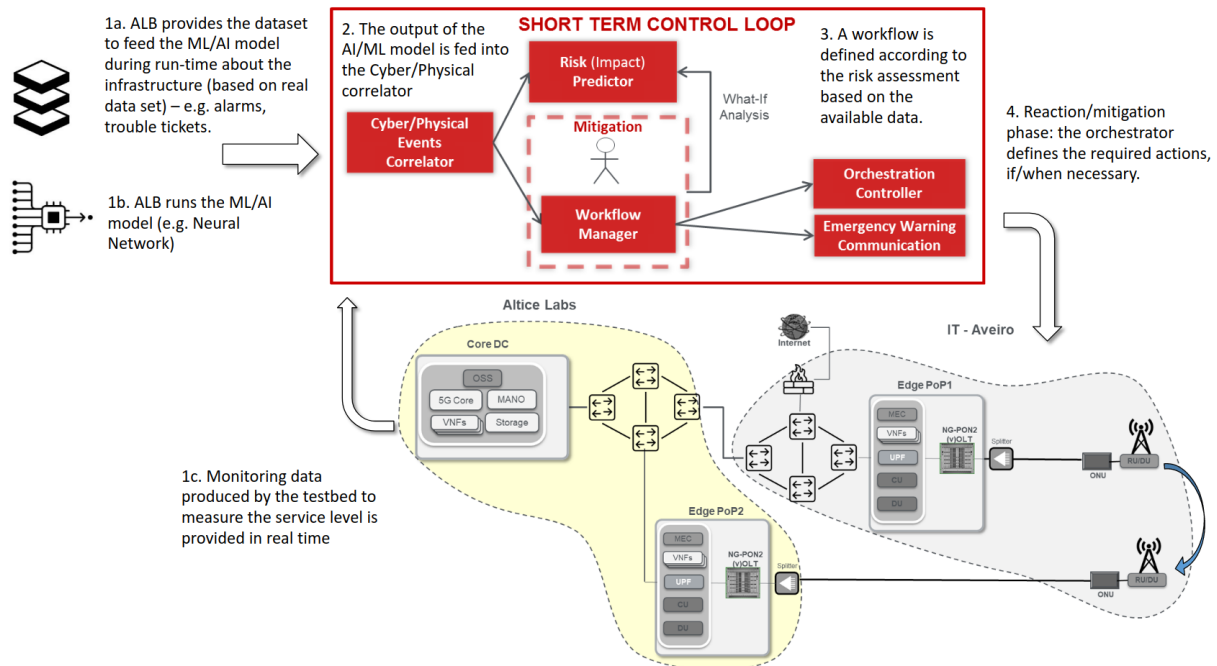


Figure 12: Cell fault detection integration with other RESISTO components

5.4 Machine Learning-based Positioning for Physical Security

In this section, a summary of the performance and capabilities of RADIOFILTER from the perspective of Machine Learning is given. RADIOFILTER is one of the sensor-based tools being developed and used in RESISTO for Critical Infrastructure (CI) physical protection. This tool detects and approximately locates unauthorized devices/ wireless access points using probabilistic techniques.

RADIOFILTER therefore features two functionalities: detection and localization. Detection is the main one. To provide this functionality, RADIOFILTER passively scans all traffic packets through the monitoring sensors from which identifying information and signal levels from devices and wireless access points is extracted.

The second functionality, location, is auxiliary to the detection of the devices, therefore when an unauthorized device or access point is detected, an estimation of the position is calculated. This is also of interest in scenarios where a device or access point is only authorized to be present in certain locations of a critical infrastructure building.

The method used to provide a location estimation of the device or access point is based on fingerprinting and machine learning techniques. The summarized process followed to obtain a location estimate consists of the following steps: A training phase is carried out when the tool is deployed in a critical infrastructure, where fingerprints are obtained by the monitoring sensors. Once the fingerprints are collected these are fed into the machine learning models (two main models are used here: K-Nearest Neighbors Classifier and Random Forest Classifier). After a validation and tuning phase, the most suitable model is selected to provide the best possible

location accuracy and finally this model is used in the on-line or operating phase where, the sensors measure fingerprints from a device or access point and this set of measurements is fed into the model which predicts the location of the device or access point. These results can be included in the event related information that is provided to the security platform upon threat/event detection.

6. CONCLUSIONS

This deliverable reports the last updates of the work performed in WP5. More specifically, following the work performed in other work packages (especially concerning the definition of the uses cases) and the comments received on D5.2 [1], the work previously performed has been refined. The possible threats and countermeasures have been tuned to the particular use case as well as the definition of the use cases. The SDS approach has been further improved and the emergency communication functionality fully implemented and tested. Based on the work performed in this WP, we may conclude that the use of SDS increase the possibility to effectively cope with the security challenges of a complex attack scenario. It will lead to further improvements in the future with the progressive use of SDN / NFV based systems which will allow faster and more effective reaction on systems, automatically or by even non-specialized operator through high-level orchestrator interfaces that hide the complexity of the underlying network.

The resilient routing algorithm proposed in T5.2 represent a meaningful improvement of the SDS framework. As a matter of fact, the SDS orchestrator will be able to perform intelligent re-routing based on the traffic requirements and constraints, accounting for modern threats to virtualization that cannot be addressed otherwise. It is worth to note that the proposed algorithm represents an approach to routing that can be used to address the problem of VNF placing and NS prototyping, a challenge for which no well accepted, automated solution is to this date available. This represent a strategic function for 5G slicing, that could otherwise be reliant on static NS prototypes, with all the associated lack of flexibility and resiliency to network conditions. Furthermore, the nature of multi-objective optimization allows for upgradability thorough the inclusion of novel constraints and that could arise in the future. The implementation of the RESISTO use cases, to be carried out in the scope of WPs 7-9 in the final year of the project, will allow the validation, assessment and practical demonstration of many of the outcomes of WP5. Thus, although WP5 formally closes with the present deliverable, activities related to the reaction/mitigation framework will be continued as needed, to ensure the successful accomplishment of the project goals, which will be ultimately validated through the WP 7-9 use cases.

7. REFERENCES

- [1] RESISTO Deliverable 5.2 - Interim Software Defined Security System And Decision Making Module, 2019
- [2] RESISTO Deliverable 2.8 - Table-top read teaming results of RESISTO architecture, scenarios and use cases, 2019
- [3] RESISTO Deliverable 5.1 - Countermeasures Draft Definition, 2019
- [4] RESISTO Deliverable 5.3 - Interim Workflow Definition and Emergency Warning Communication Function, 2019
- [5] Spectre vulnerability - <https://nvd.nist.gov/vuln/detail/CVE-2017-5754>,
<https://nvd.nist.gov/vuln/detail/CVE-2017-5715>
- [6] Meltdown vulnerability - <https://nvd.nist.gov/vuln/detail/CVE-2017-5753>
- [7] A. Barolli, E. Spaho, F. Xhafa, L. Barolli and M. Takizawa, "Application of GA and Multi-objective Optimization for QoS Routing in Ad-Hoc Networks," *2011 14th International Conference on Network-Based Information Systems*, Tirana, 2011, pp. 50-59.
- [8] B. Dey and S. Nandi, "Multi-objective routing optimizations in cluster based Sensor Networks," *2012 14th International Conference on Advanced Communication Technology (ICACT)*, PyeongChang, 2012, pp. 416-419.
- [9] X. Wei and L. Zhi, "The Multi-Objective Routing Optimization of WSNs Based on an Improved Ant Colony Algorithm," *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, Chengdu, 2010, pp. 1-4.
- [10] D. T. Hai, "Multi-objective genetic algorithm for solving routing and spectrum assignment problem," *2017 Seventh International Conference on Information Science and Technology (ICIST)*, Da Nang, 2017, pp. 177-180.
- [11] D. T. Hai, "Multi-objective genetic algorithm for solving routing and spectrum assignment problem," *2017 Seventh International Conference on Information Science and Technology (ICIST)*, Da Nang, 2017, pp. 177-180.
- [12] GEANT network topology - https://www.geant.org/Networks/Pan-European_network/Pages/GEANT_topology_map.aspx
- [13] M. J. O'Mahony, "Results from the COST 239 project. Ultra-High Capacity Optical Transmission Networks," *Proceedings of European Conference on Optical Communication*, Oslo, Norway, 1996, pp. 11-18 vol.2.
- [14] A. Cianfrani, V. Eramo, M. Listanti, M. Marazza and E. Vittorini, "An Energy Saving Routing Algorithm for a Green OSPF Protocol," *2010 INFOCOM IEEE Conference on Computer Communications Workshops*, San Diego, CA, 2010, pp. 1-5.
- [15] Marler, R. Timothy and Jasbir Singh Arora. "Survey of multi-objective optimization methods for engineering." *Structural and Multidisciplinary Optimization* 26 (2004): 369-395.

- [16] ITU-T Recommendation G.841, "Types and characteristics of SDH network protection architectures," ITU-T Standardization Organization, Approved 10/1998. Available at: www.itu.int. accessed 30 January 2020.
- [17] ITU-T Recommendation G.841, "Types and characteristics of SDH network protection architectures," ITU-T Standardization Organization, Approved 10/1998. Available at: www.itu.int. accessed 30 January 2020.
- [18] Vasseur, Jean-Philippe and Pickavet, Mario and Demeester, Piet - Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS, 2004, isbn = 012715051X, Morgan Kaufmann Publishers Inc., San Francisco, CA, USA
- [19] Rachel Kartch, Distributed Denial of Service Attacks: Four Best Practices for Prevention and Response, November 21, 2016, https://insights.sei.cmu.edu/sei_blog/2016/11/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response.html, Retrieved 28 January 2020
- [20] "Deep packet inspection: The smart person's guide". Techrepublic.com. Patterson, Dan (9 March 2017). Retrieved 28 January 2020
- [21] Choosing a DDoS mitigation solution ... the cloud based approach - By Media Team - June 10, 2013, <https://www.cyberdefensemagazine.com/choosing-a-ddos-mitigation-solution-the-cloud-based-approach/#sthash.XlwsFI8a.dpbs> Retrieved 28 January 2020
- [22] P. Wiatr, J. Chen, P. Monti, L. Wosinska and D. Yuan, "Device reliability performance awareness: Impact of RWA on EDFA failure reparation cost in optical networks," *2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM)*, Alghero, 2017
- [23] P. Wiatr, P. Monti and L. Wosinska, "Power savings versus network performance in dynamically provisioned WDM networks," in *IEEE Communications Magazine*, vol. 50, no. 5, pp. 48-55, May 2012.
- [24] P. Wiatr, J. Chen, P. Monti and L. Wosinska, "Energy saving in access networks: Gain or loss from the cost perspective?," *2013 15th International Conference on Transparent Optical Networks (ICTON)*, Cartagena, 2013, pp. 1-6.