# Product Sheets

Partners

Co-financed by:

Product Sheets

5GO.pt

# Patrol Drone

PDM&FC

Instituto de Telecomunicações

**Provides remote monitoring of areas of interest.**

## Goals

- Remote monitoring of areas of interest.
- Early situational assessment in many situations (accident, riots, risks, etc.).
- Overseeing regions to assure vigilance.

## Description

Solution to control areas and early situational assessment, moving itself quickly to a designated point, dynamically positioned according to the monitored scenario, and delivering high quality images to the specialist team (using multiple coordinated drones and monitoring if needed).

A Patrol Drone provides remote monitoring of areas of interest.

Moving itself quickly to a designated point and delivering high quality images to the specialist team. It can help with early situational assessment and pre-planning before a team even arrives.

Among other applications, Drones can be used in accident situations, sites security, riots, areas supervision, etc.

In the case of a large area, drones can be used as relays of communication.

Patrol Drones have fast travel capability, above average flight autonomy, and allow for routine missions or manual control by an operator.

They can automatically be positioned with respect to the monitoring requirements and ground forces location.

In addition, they are capable of transmitting high resolution real time images by 5G links, with adaptive quality and performance.

## Contacts

info@5go.pt

in @5Go.pt

@5go_pt

@5GO.PT

## Co-financed

COMPETE 2020 · PORTUGAL 2020 · Lisb@20[20]

5GO.pt

Product Sheets

5GO.pt

# Smart-Healing

efacec

PDM

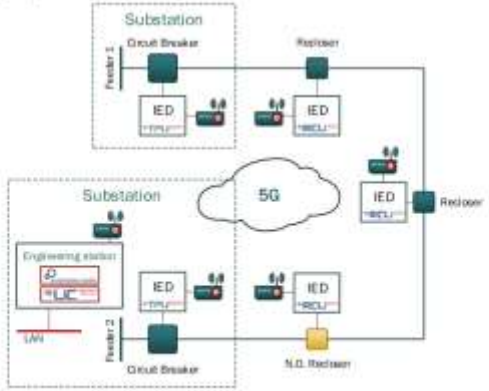
## Self-Healing solution based on 5G for enhanced power distribution grids

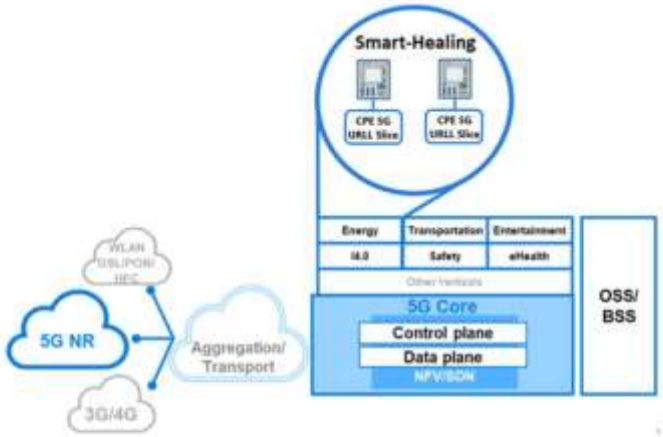
## Goals

- High-speed coordinated protection in case of unexpected electrical fault on power grids;
- Grid reconfiguration in few milliseconds;
- Enhanced quality of service on power grids.

## Description

Traditional self-healing solutions are solely based on voltage level analysis over extended periods of time and typically take tens of seconds to reconfigure power grids. This new approach, called Smart-Healing, takes advantage of 5G communication networks to perform healing in few milliseconds, which brings a notorious improvement on the quality of service.




Overhead medium voltage power distribution grids are prone to unexpected faults – These faults can be temporary or permanent. For instance, branches of trees may fall over the power lines. In such cases, it is mandatory to automatically clear the electrical fault for protecting the integrity of the entire electric system. Fault clearance can be done by an Intelligent Electronic Device (IED) that temporarily opens the closest upstream circuit breaker. IEC61850 RGOOSE messages are exchanged between IEDs in order to ensure selectivity (i.e., in order to ensure that other upstream devices further from the fault do not interrupt the circuit as well). To ensure the viability of this coordination, such messages must reach other upstream IEDs as fast as possible, ideally in few milliseconds. Although there are similar solutions implemented in high-speed "legacy" communication networks such as LTE, 5G will allow meaningful gains in latency, reliability, availability and security, bringing forth significant improvements in coordinated protection and power grid self-healing solutions.


**Contacts**

info@5go.pt

@5Go.pt

@5go_pt

@5GO.PT



**Co-financed**

Lisb@20[20] COMPETE 2020 P2020


5GO.pt

Product Sheets

5GO.pt

# VR Gladiator

PDM&FC

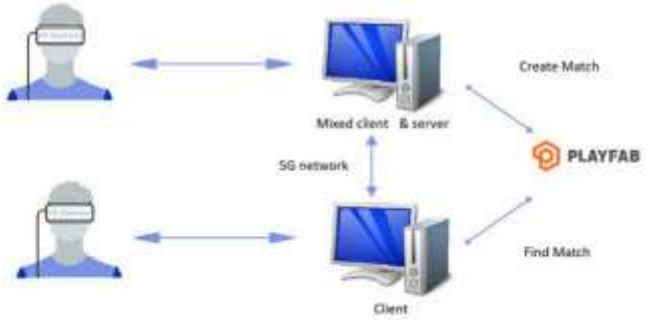
**Virtual reality game that allows each player instant reactions assured by 5G technology.**

## Goals

- Real time combat between players.
- Enhanced game experience.
- High immersion game perception.

## Description

Virtual reality game that allows each player to simulate character's arms movement, giving more realism and enhanced user experience, through instant reactions assured by 5G technology.





VR Gladiators is a game played using virtual reality equipment, where each player moves the motion controllers to simulate character's arms movement.

In the headset is presented the virtual environment that, together with sensors that detect hand's position, give more realism to the scene, providing enhanced user experience and perception.

The agility between the players is assured by 5G technology, which allows on time reaction inside the game.

## Contacts

info@5go.pt

@5Go.pt

@5go_pt

@5GO.PT

## Co-financed

COMPETE 2020 | PORTUGAL 2020 | UNIÃO EUROPEIA

Lisb@20[20]

5GO.pt

Product Sheets

5GO.pt

# Policy Management (PCF)

altice labs

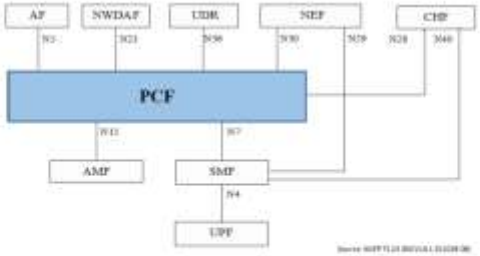
***Policy Control Function* is at the heart of the 5G core network where decides on how to handle user data sessions.**

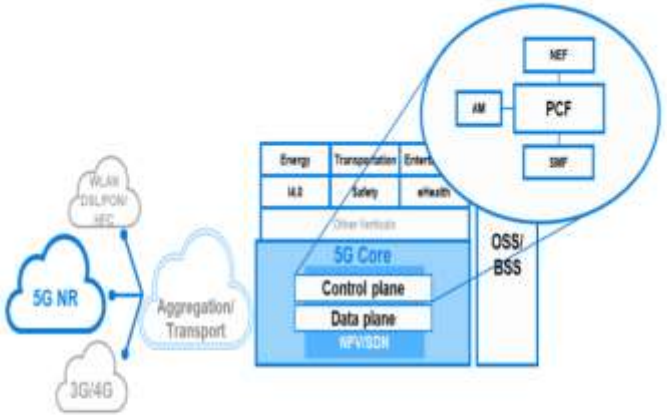
## Goals

- Decide gating and QoS control policies.
- Decide traffic steering policies.
- Decide access and mobility policies.

## Description

Policy management is paramount to allow all the stakeholders to extract the best out of the 5G network. At the center of the 5G system resides the PCF (Policy Control Function) which plays the pivotal role of deciding how each data session should be treated and handled by the entire 5G network. This allows different handling methods (e.g.: QoS, gating, traffic steering) depending on customer, service and contextual awareness.




In the context of the 5Go mobilizer, the policy management component is included in the core functions and it plays the role of the PCF in the 5G network. In this ecosystem, the PCF is responsible for informing the SMF of the gating and QoS policies for each new data session necessary for a good service experience.

Through its integration with the NEF, the PCF processes requests from 3rd party service platforms, external to the operator network, that require specific network resources to correctly deliver the service.

Two separate instances of PCF are deployed in association to the existing slices and are used to control the data sessions in the respective network slice.

The solution is also taking advantage of the integration with a machine learning component for identification of behavior patterns and enhanced adjustment of policies.

In this project, is possible to demonstrate the central role that the PCF has on the entire 5G ecosystem being the authority that enables the best conditions for unique service delivery.

## Contacts

info@5go.pt
@5Go.pt
@5go_pt
@5GO.PT

## Co-financed

Lisb@20[20] COMPETE 2020 P2020

5GO.pt

Product Sheets

5GO.pt

# 5G CPE (Wavecom-5G)

wavecom

INESCTEC

## 5G based CPE for characteristic scenarios

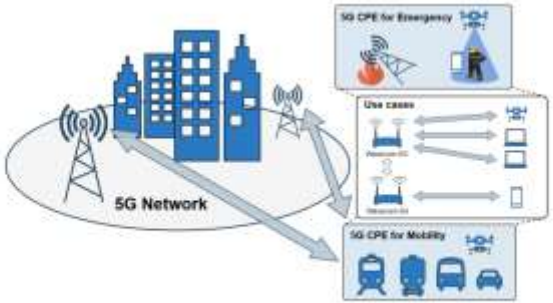
### Goals

- Provide 5G network in vehicles allowing new types of services and applications.
- Providing WiFi internet access through a 5G gateway.
- Providing critical communications.

### Description

It's intended to develop a 5G CPE with specifications for use mainly in the transportation scenario, namely buses and autonomous vehicles, where the existence of a 5G gateway will be serving a Wi-Fi network.

With the advantages that a 5G brings, it will be possible to provide a broadband communications service on these vehicles, serving the purpose of various applications: critical communications, multimedia, Internet, etc.





**Use cases**

The use cases defined for CPE focus on three components: safety, entertainment and transportation.

**First Responders Use case**

- Group communications for First Responders;
- Replace damaged or overloaded communications infrastructures;
- Traffic-aware topology control and routing.

**Crowded Events Use case**

- Broadband Internet Access in Temporary Crowded Events;
- Reinforce capacity of existing networks;
- Traffic-aware topology control and routing.

**Vehicular Use case**

- Vehicular communications;
- Alert and control messages;
- Internet connectivity.

**Contacts**

info@5go.pt

@5Go.pt

@5go_pt

@5GO.PT

**Co-financed**

Lisb@20[20] COMPETE 2020 P2020

5GO.pt

Product Sheets

5GO.pt

# 5GOpenclasses (5GOc)

**A platform to support online classes, exploring 5G eMBB & MEC capabilities.**

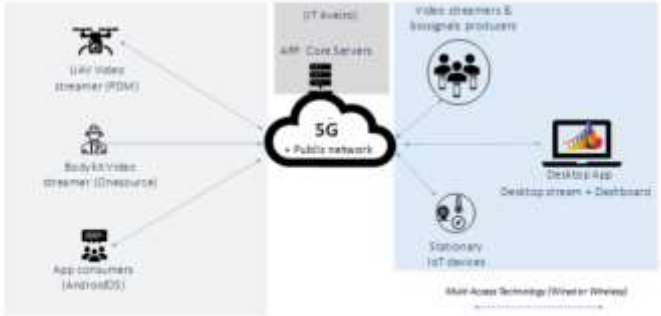
## Goals

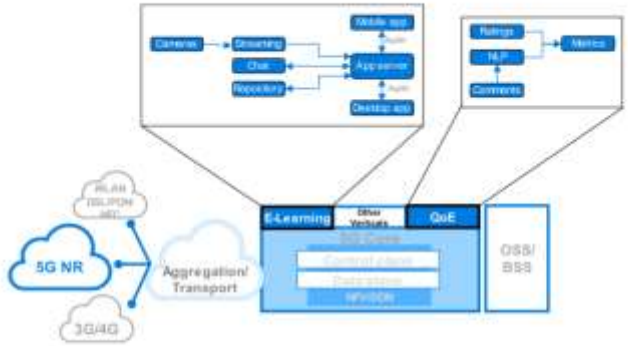
- Develop an online teaching-facility.
- Purpose a process for QoE measurement
- Compare QoS/QoE performances of the application when running OTT (over the top) on 4G and 5G networks.

## Description

Our goal is to develop an online teaching-facility and a Quality of Experience (QoE) process.

Besides the mobile app to serve the students, a desktop app allows teachers to create, manage and close the class sessions where students can chat, view live streams and download materials from a repository. An array of live video streams serving several students is an ideal scenario to leverage the 5G enhanced Mobile Broadband capability (**eMBB**).




The **evaluation of the QoE** will be done based on two inputs, namely comments and rating from the users, via a questionnaire in the mobile app. The former input will feed a Natural Language Processing module, to produce a list of the main topics throughout the text.

Benefiting from the **5G edge computing capability (MEC)**, the data collected in the questionnaire can be summarized as early as possible in the network.

**On-the-fly differentiated services** will be ensured. A UE inside the class premises should not be able to chat, ask questions and watch the live streams. On the other hand, if the UE is outside of the class premises, its users should not be able to provide biosignals sensed values neither stream videos.

**Privacy-Preservation Protocol**

The authentication (Auth) process in the product will be powered by the Privacy-Preservation Protocol solution from IT Aveiro.


## Contacts

info@5go.pt
@5Go.pt
@5go_pt
@5GO.PT



## Co-financed

Lisb@20[20] COMPETE 2020 2020


5GO.pt

Product Sheets

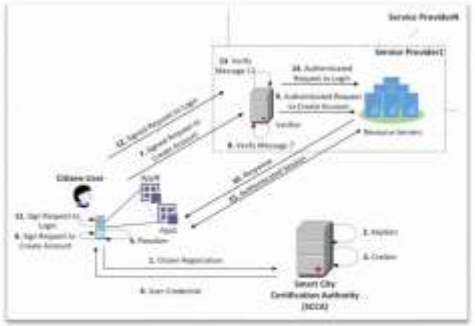
5GO.pt

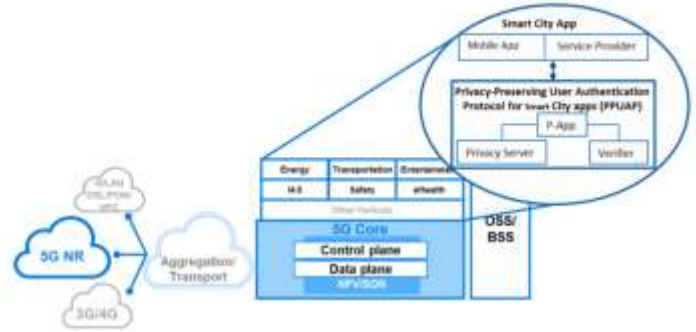
# PPUAP for Smart City Apps

## Privacy-preserving user authentication protocol for Smart City apps

### Goals

- To provide mobile users with efficient and effective means to authenticate towards Service Providers, while preventing user identification and tracking.
- To allow anonymity revocation in case of user misbehavior.
- To avoid multiple user profiles creation on the Service Provider side.
- To enable easy integration in current mobile application implementations.






### Description

We propose the design and implementation of a privacy-preserving authentication protocol for Smart City apps. The target of the proposed protocol is to provide mobile users with efficient and effective means to authenticate towards Service Providers, while preventing user identification and tracking. The proposed protocol integrates a pseudonym-based signature scheme that can provide privacy-preserving authentication, since pseudonyms can serve as identifiers for entities while still preserving the entities' anonymous state (i.e., a state in which the users cannot be distinguished from other entities in the set of users).

Previous research efforts have already provided a number of efficient mechanisms that enable conditional privacy through pseudonym systems, either based on Public Key Infrastructure (PKI) or Group Signature (GS) schemes. However, these mechanisms do not allow users to self-generate an unlimited number of pseudonyms per user so as to enable users to make use of different apps simultaneously, while preventing the users from participating in the same task under different pseudonyms, which is referred to as Sybil attack.

Finally, the proposed privacy-preserving authentication protocol will also prevent malicious users from creating multiple profiles for a specific mobile application at the Service Provider side.


### Contacts

info@5go.pt
@5Go.pt
@5go_pt
@5GO.PT



### Co-financed

Lisb@20[20] COMPETE 2020 P2020


5GO.pt

Product Sheets

5GO.pt

# Nokia Assurance Center

NOKIA

## Zero-Touch Operations with Automated Assurance in the digital era

## Goals

- Decrease mean time to detect and mean time to repair
- Automated operations for services, network and processes
- E2E close loop service lifecycle management with fulfillment

## Description

Nokia Assurance Center provides a Single Pane of Glass across Network Vendors and domains, connecting Network with Service. It supports an intuitive work flow UI and engines that guides to RCA and Service Impact Analysis, enabling to identify in an automated manner the affected service by the underlying network and taking the necessary prioritization and/or actions. It plays a very important role in 5G slice Management and B2B2X Digital world.



Nokia Assurance Center is a Cloud Native, Microservices based and Automation-native product that will be collecting the 5G Network and slice metrics. It will allow to perform correlation through the collected metrics. In the new era of cloud, 5G and digitalization it is critical to provide E2E lifecycle management of the Network and the Network Slices. It is needed to ensure multiple levels of close loop.

Powerful proactive monitoring ensuring E2E view and QoS SLAs with network, service and slice insights over PM, FM, CM and virtual Probes.

Preventive healing based on forecasting, what if scenarios and Machine learning techniques.

In 5GO project, Nokia Assurance center will play the role of assurance solution being the main functions:

- Collect 5G Network and Slice Metrics
- Calculate the needed KPIs
- Perform prediction based on ML
- Feed Policy modules with all the needed data for correct decision making

Co-financed

COMPETE 2020 PORTUGAL 2020

Lisb@20^20

5GO.pt

Product Sheets

5GO.pt

# Applicational Intrusion Detection and Prevention System (AppIDPS)

OneSource

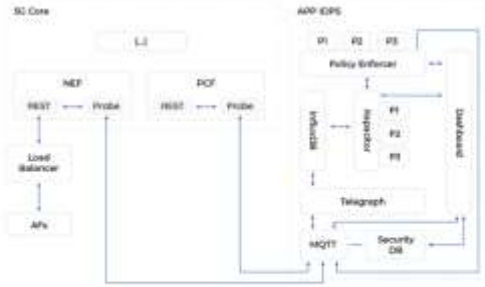
## Securing 5G Core services.

### Goals

- Detect threats to 5G Core services.
- Analyze patterns to learn how to detect new threats.
- Prevent attacks by taking actions against threat events.

### Description

AppIDPS serves the purpose of securing the service-based architecture of the 5G Core, providing security at the application layer where API communication takes place. AppIDPS combines an Intrusion Detection and Protection System (IDPS) with Security Information Event Management (SIEM), with enhanced tools and specifically tailored for 5G networks. This allows security probes in essential components, namely those exposed to the exterior (e.g. NEF).





Security probes monitor diverse parameters of each system, with the information of the probes being sent to the centralized components of the APP IDPS. The analysis process runs continuously as events arrive from the data sources. Events may be primary events, such as access control information, or can take the form of a pre-processed events such as the case of the detection of an ongoing attack where a pattern is analyzed by another tool and the contents of the analysis are indicative of an attack.

Common attack vectors for 5G Core services are:

Denial of Service (DoS); Malformed Requests; Bad Parameters; and exploring Lack of Rate Limiting.

After the detection of such an event, an action is taken automatically or taking into account human input. This action is sent back to the secured service and normal operation of its system is resumed as the ongoing attack is prevented.


**Contacts**

info@5go.pt

@5Go.pt

@5go_pt

@5go.pt



**Co-financed**

Lisb@20[20] COMPETE 2020 P2020


5GO.pt

Product Sheets

5GO.pt

# BodyKit Situational Awareness Platform (BodyKit)

OneSource

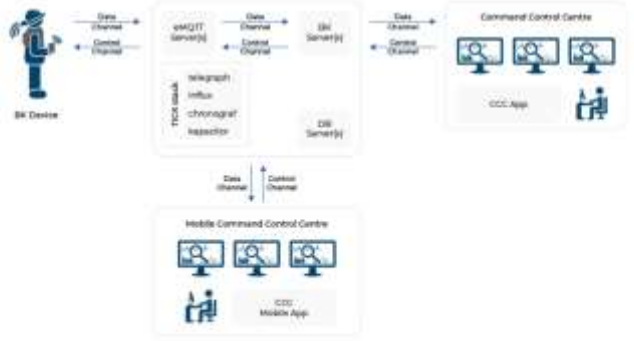
## Situational Awareness Platform over 5G.

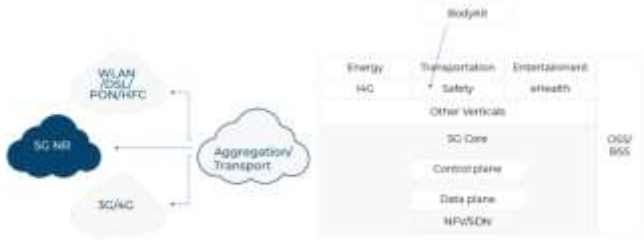
### Goals

- Collect data from multiple types of sensors and multimedia equipment over 5G.
- Provide a flexible situational awareness to enhance field operations and personnel safety.

### Description

The BodyKit Situational Awareness Platform (BodyKit) enhances current Command and Control Center (CCC) capabilities by increasing situational awareness for emergency response situations, including advanced 2-way voice and video communications and a large array of data collected from environmental and biosensors. All the information can be sent over the 5G network, thus contributing to the vertical of Safety.




BodyKit can integrate with a very wide range of sensors. The current list includes but is not limited to:

- Biosensors: Electrocardiogram (ECG), Respiration Rate (RR), Blood Pressure (BP), Heart Rate (HR), Body Temperature;
- Environmental sensors: gas (e.g. CH4, CO, Benzine, etc.), smoke, temperature, humidity, location and position.

BodyKit also has automated alarms that include the detection of man-down events, or even the presence of adverse and dangerous atmospheric environmental conditions like high temperatures and toxic levels of gases. All the information sent to the 5G network is prioritized according to its Quality of Service (QoS) profile. In order to accomplish that, the BodyKit server interacts with the 5G Core via Network Exposure Function (NEF), requesting the desired QoS profile for each flow at the Policy Control Function (PCF).


**Contacts**

info@5go.pt

@5Go.pt

@5go_pt

@5go.pt



**Co-financed**

Lisb@20[20] COMPETE 2020 P2020


5GO.pt

Product Sheets

5GO.pt

# Network Exposure Function (NEF)

OneSource

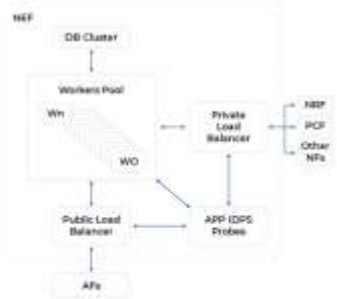
## Exposing 5G Core services to the world.

### Goals

- Fully compliant interfaces in line with 3GPP standards.
- Secure access as main entry point for 5G Core.
- Scalable and flexible service for cloud deployment.

### Description

In-line with the 3GPP Service-Based Architecture (SBA), NEF is one of the modular Network Functions (NFs) in the 5G Core. As NEF becomes a Virtual Network Function (VNF), we have the capability of deploying distributed and flexible NEFs that enable multiple entry points in the network for Application Functions (AFs) and very low latencies for distributed NFs reporting and communicating with NEF.





NEF, specified in 3GPP Release 15 [3GPP TS 23.501] [3GPP TS 23.502] [3GPP TS 23.503] is instrumental in providing an open 5G platform that can be leveraged for several players and services, providing the means for customers to interact with the network. It constitutes an evolution of the Service Capability Exposure Function (SCEF), which was originally defined as a node in the Evolved Packet Core specifications (according to 3GPP Release 13 [3GPP TS 23.682]).

NEF is essentially an API gateway designed to interact with the network functions, designed to provide third parties (such as a service or partner operators) to provision, enforce and monitor application-level policies within the operator network. Therefore, a requirement for NEF is to be scalable, secure and flexible enough to have multiple instances in the 5G Core. Multiple instances are a key part of enabling scalability, but also a benefit towards isolation when several network slices exist.


**Contacts**

info@5go.pt

@5Go.pt

@5go_pt

@5go.pt



**Co-financed**

Lisb@20[20] COMPETE 2020 P2020


5GO.pt

Product Sheets

5GO.pt

# E2E Orchestrator

ALTRAN

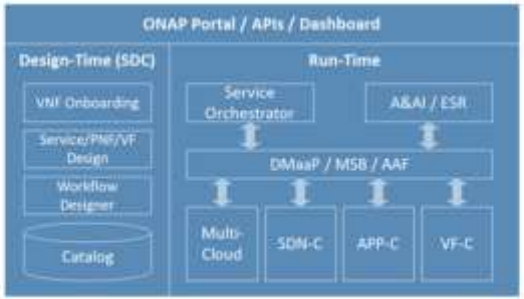
## ONAP IS AN OPEN-SOURCE PLATFORM FOR NEXT-GEN 5G SERVICE MANAGEMENT

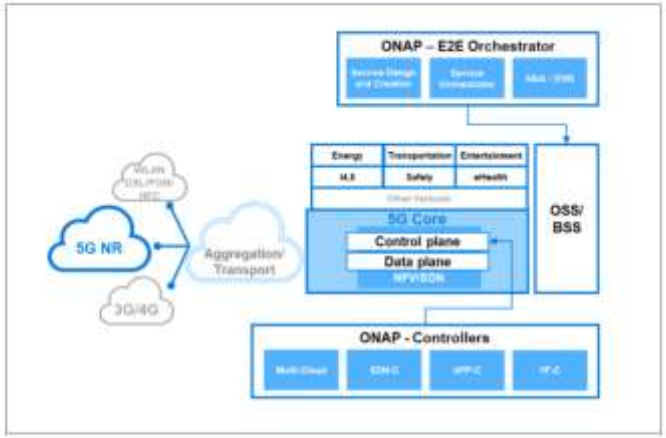
## GOALS

- Provide model-driven agile service design and fulfilment for cloud-native applications;
- Support closed-loop service management;
- Validate 5G services readiness.

## DESCRIPTION

ONAP is an open-source platform for real-time, policy-driven orchestration and automation of network functions (VNFs and PNFs) targeting all domains (fixed, mobile / 5G and enterprise). With a strong involvement of Telecom Industry (Operators, Vendors, Cloud and Software companies) it is becoming the reference platform in Operation Support Systems.




To unleash the 5G potential current systems need to be smarter and ONAP provides operators with:

- Model-driven agile service design;
- Workflow engine for multi-domain Orchestration;
- Legacy and virtualized resource management;
- ETSI, MEF and TM Forum compliance;
- Cloud-native application;
- NFV Marketplace enabler.

In 5Go.pt, Altran will showcase ONAP Orchestration capabilities in closed-loop control and prediction scenarios. With ONAP, application and service developers can use model-driven capabilities for a fast-time-to-market availability. While operators take advantage of ONAP automation features for complete product lifecycle management. Additionally, the enhanced infrastructure awareness enables optimized resource placement and efficiency.

## CONTACTS

info@5go.pt

@5Go.pt

@5go_pt

@5GO.PT

## Co-financed

Lisb@20[20] COMPETE 2020 PT2020

5GO.pt

Product Sheets

5GO.pt

# Railway 5G Level Crossing

efacec

PDM

## Supporting Railways signaling operations through 5G networks

## Goals

- Use 5G communications to support railway signaling operations, in particular to meet railway level crossing communication requirements (M2M) – Figure /Scenario #1.
- Allow maintenance agents to monitor (status and alarm event transmission) and manage the level crossing controller, through a tablet device (5G communications)-Figure/Scenario #2

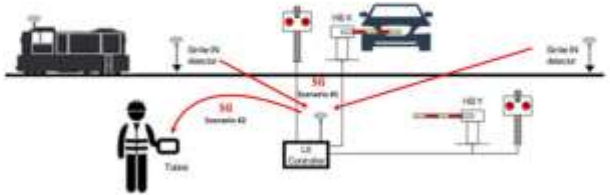
## Description

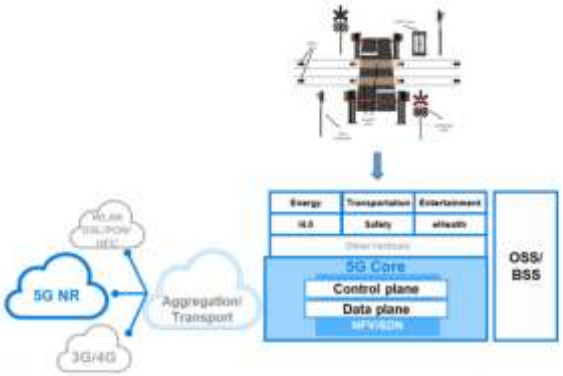
The system uses 5G to exchange data information with the Level Crossing Controller whenever a train is approaching the Level Crossing (LX) area (Fix permanent communications between Strike in detectors and Lx Controller or mobile communications between the train and the LX controller) to trigger the railways operation.

Additionally, the 5G will support remote maintenance of the Level Crossing equipment's, allowing maintenance agents to monitor and manage the LX, through tablet devices connect to the level Crossing controller.

The solution has a huge impact regarding business indicators allowing the reduction of system capex, system installation cost, installation time, cable cost, maintenance efficiency and service response time.

**Level Crossing Area**






The Railway 5G Level Crossing will take advantage of the capabilities of the 5G network to support the railways service requests concerning Availability/Reliability (uRLLC), Latency (uRLLC) and Mobility (eMBB) to provide an End-to-End safety solution.

This solution includes a cybersecurity framework able to support all the safety critical communications and also all the security mechanisms of wireless networks in compliance with safety and security railways standards providing this way the capability to replace the existing cable infrastructure by a secure wireless network.

## Contacts

info@5go.pt
@5Go.pt
@5go_pt
@5GO.PT

## Co-financed

Lisb@20[20] COMPETE 2020 P2020

5GO.pt

Product Sheets

5GO.pt

# Railway 5G Mobile CCTV

efacec

ubiwhere PDM

## 5G to Reinforce safety at Level Crossing area

### Goals

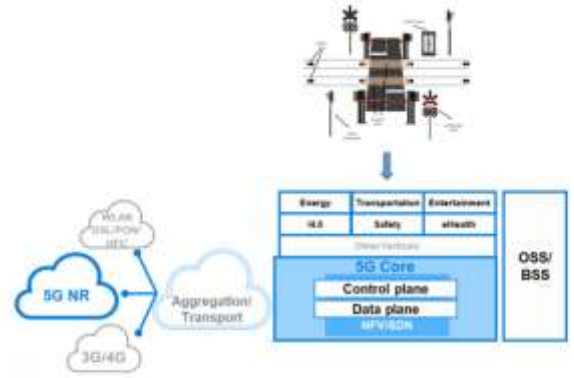
- Use 5G communications to transmit HD video images of level crossing area to approaching trains, to maintenance agents and Command Centre.
- Prevent accidents caused by cars trapped between the level crossing gates

### Description

The system uses 5G to transmit HD real time video images to Tablet devices (train and maintenance agents) and Command Centre.

The images, of the next level crossing area will be transmitted whenever the train is approaching. The system uses GPS and onboard software algorithms for localization purposes and to trigger or interrupt the video transmission.

The solution has a huge impact regarding business indicators reinforcing safety conditions at Level Crossing area and reducing traffic accidents and damages.


The Railway 5G Mobile CCTV will take advantage of the capabilities of the 5G network to support the railways service requests concerning Availability/Reliability (uRLLC), Latency (uRLLC), High Bandwidth and Mobility (eMBB) to provide an End-to-End solution.

This solution includes a cybersecurity framework able to support all the security mechanisms of wireless networks in compliance with security railways standards providing this way the capability to a secure wireless network.

## Contacts

info@5go.pt

@5Go.pt

@5go_pt

@5GO.PT

## Co-financed

Lisb@20[20] COMPETE 2020 P2020

5GO.pt

Product Sheets

5GO.pt

# 5G Probe (rNode-5G)

wavecom

ubiwhere

## 5G radio spectrum monitoring probe

## Goals

- Identification of 5G channels in the analyzed spectrum.
- Estimation of transmitted and received power.
- Auxiliary tool in coverage tests.
- Spectrum interference detection.
- Logging of 5G transmissions for later analysis in a centralized system.

## Description

The fifth generation introduces a new form of radio management, allowing a more efficient allocation of the bandwidth available to the users.

With a new technology it is important to have tools that allow to evaluate its performance. The probe's main objective is to monitor the 5G communications spectrum, collecting metrics and sending them to a centralized service for further analysis.



**Use cases**

The measures will allow to evaluate and validate communications between 5G equipment such as the CPE and gNodeB which are also being developed in this project.

**Coverage tests**

It can be used to plan the best arrangement for the different network components by measuring the received signal.

**Network troubleshooting**

Through 5G signal analysis the probe can be used to detect problems in the cellular network.

**Permanent 5G signal monitoring**

Using the logging system, it is intended to implement the signal quality monitoring at strategic points of the network, thus measuring the signal quality over time and identifying potential constraints.

**Contacts**

info@5go.pt

@5Go.pt

@5go_pt

@5GO.PT

**Co-financed**

Lisb@20[20] COMPETE 2020 P2020

5GO.pt

Product Sheets

5GO.pt

# Honeynet

ubiwhere

## Preventing and mitigating attacks on 5G services

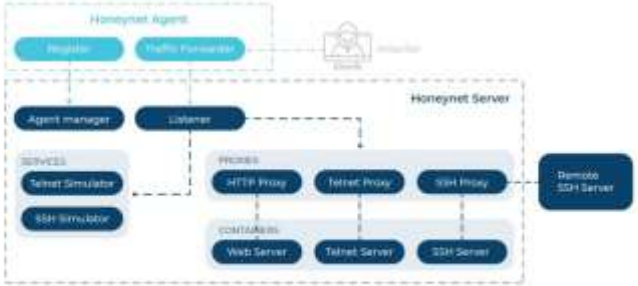
## Goals

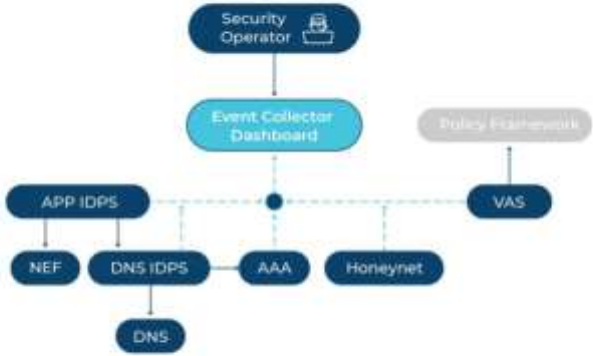
- Prevent attacks by detecting abnormal activity around service entry points
- Mitigate impact after 5G service has been compromised
- Monitor and learn attacker's methodologies to improve network protection

## Description

The Honeynet module has the purpose of detecting illicit activity on two main fronts. The first, as a preventive measure, consists of detecting abnormal activity, such as probing, around network entry points. The seconds aims to detect attackers after a machine has been compromised.

A typical Honeynet deployment is composed by multiple Honeynet Agents (HA) and a single Honeynet Server (HS).




The HAs are lightweight servers that forward all incoming traffic to the HS. The honeypots, i.e. services, simulators, proxies and containers are running in the Honeynet Server which accepts incoming connections from its HAs. The HS can provide simulated services or real services deployed on containers or VMs.

Looking at the project security ecosystem, all security modules, including Honeynet, report events to the Event Collector.

The Event Collector is responsible to aggregate all security-related events and present them in a user-friendly dashboard which is shown to the network security administrator.

## Contacts

+351 234 484 466

@ubiwhere

@ubiwhere

## Co-financed

COMPETE 2020

PORTUGAL 2020

Lisb@20[20]

5GO.pt

Product Sheets

5GO.pt

# Intelligent Video Surveillance System (IVS)

ubiwhere

**Autonomous computer vision system to monitor and prevent hazards on railroad level crossings**

## Goals

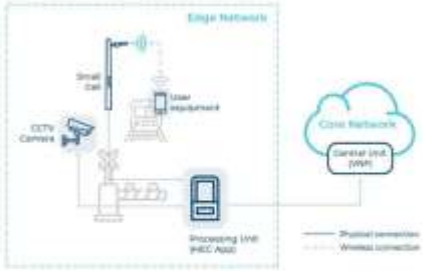
- Obstacle detection and classification on railroad level crossings
- Broadcast real-time video of level crossings to train conductor
- Global alert system to contact authorities

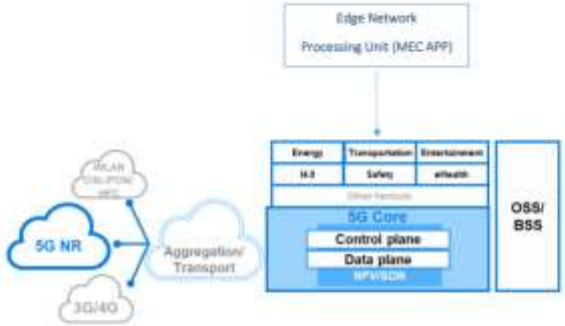
## Description

The IVS solution leverages network edge computational resources to enable real-time processing of images from cameras, targeting the detection and classification of foreign objects in railroad crossings.

At railroad crossings there will be a camera pointing to the crossroad. The Processing Unit (PU) will analyze the real-time video feed from the camera in order to autonomously detect and classify objects in the area that are prone to provoke hazards. Once potentially hazard objects are detected an alert is sent to the Central Unit (CU) and to the train conductor. In addition, a live feed of the video with overlay tags of classified objects is broadcasted in the network edge, to reach the user equipment of the train conductor, and to the network core, to reach the CU operator.

From this point, the CU operator has the responsibility of accessing the severity of the situation and perform actions, such as ordering the immobilization of the train and dispatch emergency authorities to the site.




## Contacts

+351 234 484 466
@ubiwhere
@ubiwhere

## Co-financed

COMPETE 2020
PORTUGAL 2020
Lisb@20[20]

5GO.pt

Product Sheets

5GO.pt

# Vulnerability Assessment System (VAS)

ubiwhere

## Scanning for vulnerabilities on 5G services

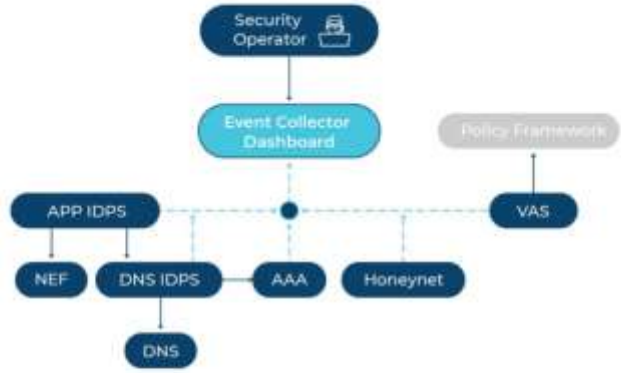
### Goals

- Periodic scan of function vulnerabilities inside 5G services
- Automatic update of database with the latest vulnerabilities
- Report detected anomalies and vulnerabilities to a central system

### Description

The Vulnerability Assessment System (VAS) intents to actively protect a 5G service by periodically scanning its functions against vulnerabilities known up to date.

Along with the service required functions, an additional function, namely the VAS Slave will be deployed within the service, thus allowing vulnerability scans of all functions. Once vulnerabilities are detected,


The VAS Slave will register itself in its corresponding VAS Master, retrieve the latest known vulnerabilities and begin the scanning process of the functions in the service. Detected vulnerabilities are reported back to the Master, which will analyze their severity and act accordingly. Afterwards, vulnerabilities are aggregated and reported to the Event Collector dashboard.

Typically, in a telecommunications operator network it is expected to have multiple instances of VAS Slaves (one per each service) and one VAS Master responsible to coordinate and update its Slaves.

Both VAS Master and Slaves use OpenVAS resources to leverage opensource collaboration, together with Network Vulnerability Test (NVT) synchronization. In the open source community, there is a significant amount of NVT databases compatible with OpenVAS, so it is fairly simple to maintain scanners up to date.


**Contacts**

+351 234 484 466

@ubiwhere

@ubiwhere



**Co-financed**

COMPETE 2020 | PORTUGAL 2020 | Lisboa2020

5GO.pt

Product Sheets

5GO.pt

# Mobile Video vCDN

ALTRAN

## DISTRIBUTED AND MOBILITY-AWARE EDGE CACHING

## GOALS

- Reduce video delivery latency on the move;
- 5G Core compliance;
- Context-awareness (user, network and video).

## DESCRIPTION

A **5G-enabled** approach leveraging Operator's context-aware operational systems to fulfil next-generation multimedia (and other) services requirements and end-user expectations: any content, anywhere, anytime.


Targeting the optimization of video provisioning to mobile users, the integration of vCDN system with 5G Core and MEC capabilities, as well as virtualization of supportive network functions (NFV) and programmable traffic control (SDN) are leveraged.

The instantiation of content replicas in vCDN Nodes, closer to the users, dismisses the need for video to be retrieved from centralized locations, achieving lower latencies and conserving resources throughout the backhaul.

Moreover, the framework has access to multiple user context (e.g. location), for dynamically placing expected content across distributed caches at edge sites along the user's or vehicle's itinerary in mobile scenarios.

### SYSTEM COMPONENTS

vCDN Node: distributed element used to store (caching function) and deliver (streaming function) the video sessions to mobile users.

Monitoring Manager: integrates monitoring sources and context (e.g. Network, User or vCDN System-related), storing it on the databases.

User Location Predictor: embeds algorithms for predicting user's location and/or path based on UE and MEC location services.

Request Router: provides content discovery capabilities, responding to requests for video or VR / AR content by providing the location of the local cache best suited to deliver it to the UE.

Content Placement Planner: this component uses analytical capabilities to provide recommendations to the vCDN Engine regarding the target caches where the content should be replicated. It is through this component that the CDN infrastructure realizes the predictive caching and buffering mechanisms.

vCDN Engine: this component realizes the logic of the vCDN platform:

- Enforces operations according to recommendations from the CPP;
- Responds to requests made through northbound API;
- Registers Data Sources on the databases;


Co-financed

COMPETE 2020 PORTUGAL 2020

Lisb@20[20]

5GO.pt

Product Sheets

5GO.pt

# Autonomic Manager (AM)

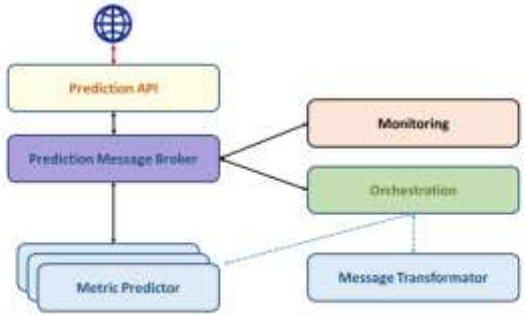
## Real-time forecasting for improve network management.

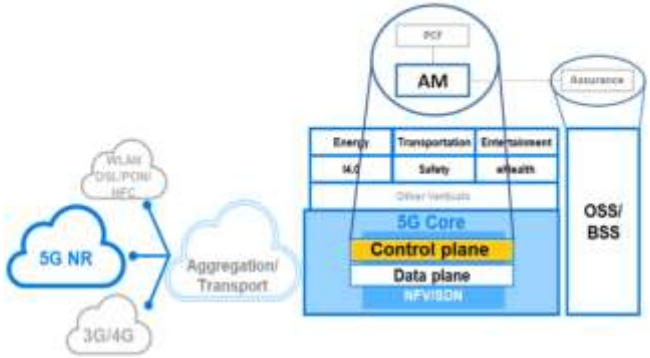
## Goals

- Real-time predictions of different performance metrics;
- Dynamic threshold algorithm to adapt network resources in an inter-slice 5G management;
- Proactive congestion management.

## Description

**Autonomic Manager (AM)** makes simultaneous real-time predictions of different network performance metrics through different forecasting algorithms. AM uses information from Assurance to identify and predict anomalies in network slices and alerts PCF to adjust the network control policies.




The Prediction API allows: train the predictor for a given metric; predict a value for a time series system/metric; save new time series data for later training; and change the training parameters.

The broker component enables to build several prediction components for the same metric, each one with a different prediction model. These predictions can be combined to build an ensemble predictor that performs better than the individual prediction components.

**AM** instances can be used in a slice and in slice groups being managed by orchestrator component.

**AM** is simple, flexible to the needs of the domain, and scalable to be incorporated in big data architectures. It can be used in a 5G scenarios, with different parallel prediction approaches for and different metrics/KPIs in different slices.

info@5go.pt
@5Go.pt
@5go_pt
@5GO.PT

Co-financed
Lisb@20[20] COMPETE 2020 P2020

5GO.pt

Product Sheets

5GO.pt

# Security Dashboard & Event Collector

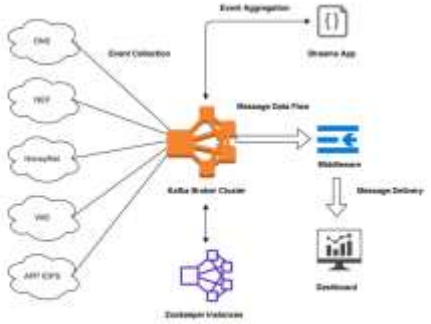
## Security visualization tool

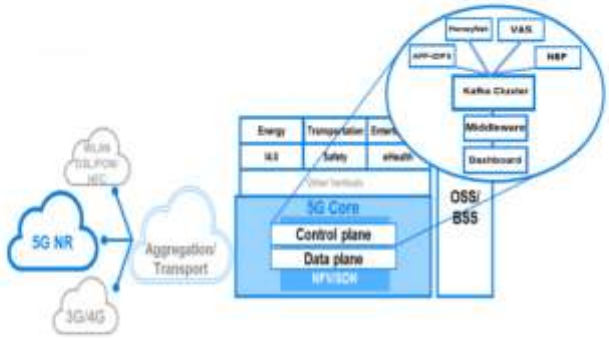
### Goals

- Collect security events from the different components of a 5G network core;
- Support a distributed event transport topology capable of leveraging edge processing;
- A middleware that validates and processes security events;
- Easy real-time monitoring of security events by using a user-friendly visualization tool.

### Description

The Security Dashboard & Event Collector was designed to be used as a component of the security framework of a 5G network core. It is composed by a dashboard that displays security information, a middleware that collects, validates and processes security events, and a message broker that centralizes all the messages received from multiple components. This visual tool will help network administrators to monitor and secure, in real-time, the services supporting the 5G core.




The multiple security events generated by 5G network components demand a careful real-time analysis from the network administrators. To ease their task, a **message broker**, composed by a Kafka cluster, prioritizes the events, provides the scalability needed and assures the necessary performance. These messages are pre-processed in a first stage recurring to Kafka streams, where the first information is aggregated.

A **middleware** will get the events for a second level processing. It calculates all the specific metrics required and adapts the information to be displayed in the dashboard. The **dashboard**, which is directly connected to the middleware, displays all the information in a simple and intuitive way. Multiple views are available, from a general overview of the network security events to a detailed event log. Broker activity is also monitored and shown.


## Contacts

info@5go.pt

@5Go.pt

@5go_pt

@5GO.PT



## Co-financed

Lisb@20[20] COMPETE 2020 P2020


5GO.pt