SMART ROAD

"The intelligent road that runs with progress"

By the Direction for Operation and Territorial Coordination
Technological Infrastructure and Facilities

SMART ROAD

"The intelligent road that runs with progress"

By the Operation Division and Territorial Coordination
Technological Infrastructure and Facilities

anas
GRUPPO FS ITALIANE

TABLE OF CONTENTS

INDEX OF FIGURES

INDEX OF TABLES

SMART ROAD DESIGN FOR SMART MOBILITY

The new season of infrastructure planning and design in our Country entrusts Anas with an important role in promoting and supporting enforcement policies of new works, in preserving infrastructural heritage and in technological innovation. Intelligent mobility is one of our main objectives: roads that can respond to road user's modern needs and to the functionality of the Smart Road. For this reason, an International Scientific Technical Committee has been set up to flank Anas in the realization of the "Smart Mobility" project, oriented toward the construction of an advanced model of intelligent mobility able to better manage traffic flows and improve road safety. A teamwork of experts will direct the development of the executive design for technological infrastructure and services dedicated to users. The project, which initially sees the access road to Cortina as protagonist on occasion of the 2021 World Ski Championships, represents the first "Smart Mobility" prototype in Europe for mobility management, starting from services and technologies offered by Anas Smart Road, aimed at ensuring greater safety, traffic fluidity and driving comfort. This is a decisive step towards connected and autonomous driving of the future.

In Italian history, Anas played a fundamental role in national modernization, influencing its economic and cultural development. A strategic role that the company has preserved and developed over the years as a multiplier of investments. Today we want to continue to unite the Country with passion, efficiency, sustainability and technological innovation to prepare Italy for tomorrow's challenges.

Ennio Cascetta, Presidente de Anas

DIGITAL TRANSFORMATION OF INFRASTRUCTURES

Anas aims to become "an excellence" at European level and a reference model in road innovation that will become "smart". The objective is to provide the Country with an efficient road network, in progressive improvement and open to new challenges in the future: from electric supply to a driver assistance system and beyond, as in the case of self-driving vehicles.

The company has launched the Smart Road program with the aim of progressively extending it to the main arteries of Anas road and motorway network, leading the Country towards the digital transformation of our infrastructures, in order to generate services that facilitate mobility and monitoring of works. The intent is to turn about 3,000 kilometers of roads and motorways into Smart Roads, including the new A2 "Autostrada del Mediterraneo", which will be the first Italian infrastructure able to interact with users, allowing a more comfortable and safe journey.

New technologies offer us the opportunity to further develop our mission and enhance Anas roads and motorways, improving the quality of the service offered through traffic control, road safety increase, more efficient mobility management and infrastructure control.

This is a know-how that, thanks to the presence of Anas on foreign markets, can be exported along with the 'culture of the road', obtained over 90 years of activity in road and motorway infrastructure sector.

Gianni Vittorio Armani, CEO de Anas

FOREWORD

This technical book aims to be the first guide in the Italian road industry, and one of the firsts internationally, to define the concept of "Smart Road". According to Anas' vision, a Smart road is capable of "talking to users and to itself". Through in-motion connectivity systems, it erases distances, widens spaces and can automatically include and recognize users. The Smart Road extends road infrastructures, improving, through technology, their operational capability. With this vision, modern road arteries will become "Green", provided with data communication channels and energy, fully integrated in the transport and information multi-modal network.

The solutions proposed in this text are particularly innovative and take into consideration the latest Internet of Things, Open and Big data technological developments, in order to address the demanding challenge of bringing these issues to the road.

Anas Smart Road's digital systems and platforms will enable Vehicle To Infrastructure (V2I) exchange and facilitate Vehicle To Vehicle (V2V) communications, thus accelerating the introduction of driving assistance systems and the circulation of Self Driving Cars.

The strength of this project stems from the interdisciplinary vision and from being sure that the "digital shift" is the key to revive the transport infrastructural sector. The digital shift is what identifies a sustainable growth, capable of creating safer, more functional infrastructures and generating new services and information for a better "travel experience" for users, goods and self-driving transport systems. This way, it will contribute to the country's development.

Thanks to Anas' structure technicians for their valuable effort in drafting this technical book and to Mr. Luigi Carrarini for coordinating and developing this complex project.

Moreover, a special thank goes to prof. Carlo Ratti's studio for their valuable help.

To conclude, recent references to Smart Roads at national level, which were included in the 2018 budget law approved by the Italian Parliament at the end of 2017, "in order to support the dissemination of technological good practices in the road network digital shift process...", highlight even more the need for a document like this.

Therefore, we hope that this work can be useful to those who research, plan, build and test complex systems to be used in future Smart Roads and that this Italian vision will also be appreciated abroad.

Ugo Dibennardo

1 THE SMART ROAD

1.1 Transport Systems: From the European Strategy to the Smart Road

Transports play a major role in a country's economic and social development. An efficient transport system enables the creation of new markets and the improvement of those that already exist; therefore, it is fundamental to support steady economic growth, employment and wealth. At a time in which, for any production system, winning the challenge of the "global" competitive market is fundamental, an inefficient transport system reduces the chance to reach new markets, the scope of trades, the production capacity and the potential for economic and social growth.

In facts, societies are becoming increasingly structurally dependent from their own transport systems and, at the same time, in the last few decades the demand for mobility has skyrocketed in developed countries.

In the last few years, trading needs have deeply changed. People and goods' mobility needs and habits led to a radical change in the way we see transport systems and, accordingly, in the visions and strategies that must inspire policies in this sector.

As the traditional model, in which people and goods transportation is considered as a group of "mono-modal" movements, land transport is giving way to the multi-modal paradigm. This means that one trip consists of a group of linked transfers. This supposes a rise in people and goods movement time, road accidents and congestions. Such events compromise transport networks capacity. This way, the risk is that networks will not be able to sustain future vehicle flows.

To win mobility-related challenges, not only the number of infrastructures is to beincreased, it is also necessary to optimize and improve transport systems' efficiency by making the most of current potential.

Transport must be reshaped into an integrated and dynamic system, in which data, management and control work together to optimize infrastructures' use and mobility organization. For this purpose, "Intelligent Transportation Systems" - ITS have been introduced with the Directive 2010/40/EU. It contains ITS standards and specifications that are shared throughout the EU, establishing the following priorities:

- Optimal use of data about roads, traffic and goods transportation;
- Continuity of ITS traffic management and goods transportation services;
- Implementation of ITS for road safety and transport security;
- Vehicle to Infrastructure communication;

Standards, regulations and actions to elaborate are planned in priority sectors:

- Implementation, throughout the EU, of multi-modal mobility information services;
- Implementation, throughout the EU, of real-time traffic information services;
- Data and procedures to share road safety related minimum universal traffic information free of charge to users, where possible;
- The harmonized implementation, throughout the EU, of an interoperation emergency call electronic service (eCall);
- The implementation of information services in safe parking areas for heavy goods and commercial vehicles;

- The implementation of reservation services in safe parking areas for heavy goods and commercial vehicles.

The use of intelligent systems around the world, both in and out of urban areas, enabled the concrete assessment of ITS benefits in different countries, both in the USA and in Europe, such as:

- Transportation times decreased by around +20%;
- Network's capacity increased by between +5 and +10%;
- Number of accidents decreased by -10/15%;
- Congestions decreased by -15%;
- Polluting emissions decreased by -10%;
- Energy use decreased by -12%.

For the ITS to be determining in a more efficient use of infrastructures, vehicles and logistic platforms, they must undergo a process of *digital transformation* and be integrated with technologies that can support information exchange among the different actors of transport systems. For this purpose, the European Commission is devising strategies for the C-ITS (Cooperative Intelligent Transport Systems) oriented to bidirectional cooperative mobility, both Vehicle-To-Vehicle (V2V) and Vehicle-To-Infrastructure (V2I).

Right now, many car manufacturers are launching new vehicle models that can interact with one another, as well as with road infrastructures. Such interactions are at the basis of C-ITS models, which enable users and infrastructure operators to share real-time information in order to increase road safety, optimize traffic management and improve driving comfort. Likewise, on the infrastructure side, the *digital transformation* enables a country to have a sustainable, smart and inclusive growth that can create safer, better and simpler infrastructures that generate data and services for a better travel experience. The *digital transformation* can also be useful for *decision-makers* to devise transport policies and manage traffic flows.

For this purpose, the guidelines on the Cooperative-Intelligent Transport System set out the creation of a unified network that will be available for those companies that work in the field, in order to avoid divisions caused by the adoption of different standards. This way, both drivers and road-operating companies will be able to share useful information to coordinate actions and decisions. Such technological trends, in the *automotive* industry, are driven by future scenarios in which vehicles will be provided with an increasing number of driving assistance systems, rapidly evolving towards the last step: self-driving.

The infrastructures' *digital transformation* is a driver for the country's entire economy, given that infrastructures serving the transport industry, due to their ability to connect different manufacturing bodies and industries, are a real opportunity to draw important investments. In this sense, the *digital transformation* is a huge opportunity for Italy, because it enables to make the best of all the existing assets through technological *upgrades*, which times and costs are averagely lower than upgrades on material infrastructures.

The Ministry of Infrastructure and Transport (MIT) took on the challenge of digital innovation, creating a national *vision* which considers technology as fundamental for the development of the country's infrastructures serving transports, with direct benefits for citizens and companies.

With this vision, on the 22 June 2016, the MIT presented a preliminary study: "Functional standards" for Smart Roads, dealing with the evolution of roads digitalization process at a national level.

The Smart Road initiative aims at introducing the ITS nationally by creating a technological system that can facilitate the exchange between infrastructures and new-generation vehicles, adapt infrastructures to new transport modalities and set out innovative services for users and infrastructure managers, in order to increase safety levels.

However, the transport and logistics infrastructures industry is extremely divided due to the existence of many and different regulation instruments. ITS were implemented for the first time, to promote sustainable mobility, in 2001's Piano Generale dei Trasporti e della Logistica (Transport and Logistics General Plan) and then in 2007's Linee Guida del Piano della Mobilità (Mobility Plan Guidelines).

The Directive 2010/40/EU was implemented in the Italian legislation with law no.221/2012, which sets out the requirements for ITS dissemination, planning and manufacturing. Such requirements were adopted by the MIT on the 1 February 2013 with the Decree for the Dissemination of Intelligent Transportation Systems in Italy, and they address:

- Actions and fields in which to act to facilitate the development of ITS nationally;
- Continuity of ITS traffic management and goods transportation services;
- Online database of vehicles not covered by the mandatory insurance and ITS Applications for safety (eCall);
- V2I connection;
- Creation of the Comitato di indirizzo e coordinamento tecnico delle iniziative in materia ITS (ITS-related intiatives technical coordination and steering committee).

The inter-ministerial decree no.446/2014 sets the MIT as the national body responsible for the implementation of the "Piano nazionale per lo sviluppo dei sistemi ITS" (National plan for the development of ITS sytems), adopted on the 12 February 2014.

Despite the high level of regulation in the field, the targets set by the EU remain unmet. Therefore, it is clear that there is the need to adopt specifications on technological standards, in order to implement the recommendations of the reference common framework, and to clarify Smart Road-related functions and services to enable by proposing performance standards to implement in order to follow through with the *digital transformation*.

To set out reference technological performance standards for Italian Smart Roads, the MIT decided, consistently with the concrete nature of new infrastructure policies, to create a well-defined roadmap. Particularly, the approach focuses on logical and functional aspects, which include the determination of data and information that can be exchanged between functions and with central-level collection and analysis systems.

This way, the person in charge for the implementation will have more freedom of choice, thus avoiding the risk of quick obsolescence should technological standards be defined. As a matter of fact, the same functions, services and performances can be carried out even implementing different technologies. The aim is that of defining the order of priority for those standards that cannot be postponed, considering the management of infrastructures and data and the direction that the private sector is taking.

Note also that important references to Smart Roads at a national level have been added in the 2018 budget law, approved by the Italian Parliament at the end of 2017.

1.2 Anas' Vision

The Smart Road is a set of technological infrastructures aiming at sustainability and improving roads safety and availability through the Digital Transformation (DT), which is a dynamic process that offers modern services and solutions.

The basis of the DT process is the creation of adequate enabling structures and platforms to implement in Smart Roads, in order to carry out many functions and to provide services that can meet the modern needs of road users.

An integrated and evolving framework, as far as mobility is concerned, is only possible if innovative technologies are embedded in an open and comprehensive "*system architecture*". This system architecture is constituted by enabling structures (platforms). These may even be invisible to users, but they are the real, effective foundations for all the applications.

Common features of these "platforms" are:

- The **"enabling"** nature for different kinds of functions and services.
- To be **"open"** to third parties. Information that could be made available to third parties to develop market-oriented applications. The combination of these two features ("enabling" and "open") enables digital roads to become the "development promoters" for the country.
- The **"evolving"** nature: as time goes by, enabling structures will be adapted to new technological offers.

The Smart Road that Anas wants to develop is focused on users and their safety and the goals that Anas wants to reach are to ensure:

- A safe trip, without difficulties, with driving assistance and/or self-driving; Safe roads, with adequate levels of maintenance;
- Timely action in emergencies and alerts from users' mobiles; Real-time information on mobility;
- Services to users since the first installations and with possible future implementations;
- An increase in efficiency through raising existing roads' operation factor by using modern technology;
- Intelligent monitoring, through IoT (Internet of Things) systems, of road infrastructures, traffic and goods transport, as well as environment and climate;
- Monitoring of vehicle flows with Multi Function Smart Camera; Tunnels management and monitoring with the "Smart Tunnel" method;
- Network management and increase in infrastructure transport capacity by increasing traffic volumes through dynamic lanes;
- Real-time check of vehicles mass with Weigh in Motion systems (WIM);
- Full integration of existing technologies and databases on one digital platform.

Figure 1 - Anas' Smart Road

The Smart Road is the evolution of the concept of road: from mere public work to technological infrastructure. Technology overcomes spatial and functional limits of roads to increase their operational capacity.

The core of the Vision is the connectivity with users, vehicles and goods.

All of this is made possible by the connectivity with users and between vehicles and infrastructure. In facts, two wireless systems will be implemented, which will connect users in motion and vehicles with systems along the infrastructure.

The first will take advantage of the extensive dissemination of "personal mobile devices", that is to say all those electronic devices that can be used in motion, such as mobile phones, PDAs, smartphones and tablets, using the information produced by their sensors (accelerometer, gyroscope, magnetometer, proximity sensor, barometer, brightness, thermometer, humidity, pedometer, etc.) and, particularly, the very functions of the device, such as loudspeaking telephone and messages, through apps that provide information on mobility and road safety services.

Anas' choice is to create a dedicated Wi-Fi network, working up to a vehicle speed of 130 km/h (~81mph), which enables users' mobile devices to connect to an intranet network dedicated only to Smart Road services.

Road users will receive the information requested, safely and without distracting them, on their mobile device's loudspeaker: this way, **mobile devices turn into an On Board Unit (OBU)**. Other functions that may be available on the Wi-Fi network will be only allowed when vehicles are stationary.

The second Vehicle to Infrastructure (V2I) wireless system for Safety services will quickly disseminate semi-self or self-driving systems; the technology implemented is the G5 ITS ETSI wave system, through the IEEE 802.11p physical layer, already chosen by the US FCC ((Federal Communications

Commission), by many American road operators and by the European Community through ITS Directives.

Anas' Smart Road has been devised modular, that is standalone and independent; a module is a physical road or motorway segment that is operational and is served by the Green Island, energy core of the Smart Road.

The Green Island is an area that contains mainly renewable energy generation and distribution systems, capable of independently powering all of Smart Roads' systems in its module, which is generally a road segment of 30 km (~19mi).

Another feature of the Smart Road is the creation of an infrastructure to monitor constantly and in real time all the work of arts and the state of the road. The infrastructure will be based on IoT (Internet of Things) networks, through Low Power, easily installed, Wide Area and Long Range sensors.

To sum up, the Smart Road project implements enabling platforms based on the following main elements:

- Communication system
- Energy system
- Dynamic lane
- Smart Tunnel method
- Internet of Things (IoT)
- Open data and Big data

The communication system is implemented through "seamless" communication networks, which efficiently connect people and vehicles: this is a necessary and fundamental condition for digital roads to happen. For this purpose, the Smart Road lays down the conditions to ensure:

- Connectivity between people and digital instruments (serving travelers, road operators and third parties) with WI-FI in motion technology, standard IEEE 802.11 a/b/g/n, ensuring fast roaming in order to have continuous communication service with users;
- Vehicle-to-Infrastructure connectivity (V2I), provided with communication integrated platforms based on ETSI G5 DSRC WAVE (Wireless Access Vehicle Environment) - IEEE 802.11p standards;
- Monitoring system based on the "Wearable" concept:
  - Easy to install
  - Low cost
  - Extensive connectivity
  - Addressable devices (internet-native and as all-in-one as possible).

Energy system

The energy system's architecture is made up of, in dedicated areas called Green Islands, renewable energy generators, a connection to the national grid and energy transformation and distribution systems.

The energy system carries out the following tasks:

  - Generation: mainly with photovoltaic systems and, if necessary, with small wind turbines with variable power output, based on which available source can be best harnessed. They will be coupled with an energy storage system that can guarantee continuous power supply during those times in which energy is not generated.

- Technological core: a room that stores all energy transformation, conversion, control or distribution systems.
- Distribution: divided into local, for devices inside the Green Island, and in itinere, that is powering devices along the road/motorway module considered.

Dynamic lane

The increase in Italy's stock of cars and the subsequent increase in road transport proportionally and negatively affects traffic congestions, road accidents and polluting emissions.

On Anas' main arteries, the growth of land transport exceeds the capacity of existing road infrastructures, with evident negative effects both on safety and the environment. As far as ITS (Intelligent Transport System) technology development is concerned, the introduction of the dynamic lane could be an effective way of improving traffic flows and optimizing services in main motorways during congestion peak times.

The dynamic lane consists in the use of the carriageway's far-right lane as the slow or emergency lane, based on necessity or traffic volume.

The impossibility to widen carriageways leads to the construction of the dynamic lane, built based on the width of carriageways and on exceptions made to the Codice della Strada (Road Traffic Regulations)[1].

The Smart Tunnel

The added value for tunnels' safety depends on the nature of installed technologies, sensors and an efficient management system, both during normal operation and emergency situations.

The smart tunnel is an instrument aimed at developing and implementing solutions that can improve management and safety factors, that is to say:

- that can prevent and control dangerous situations,
- constantly and remotely monitor operational
- conditions and optimize maintenance
- that have a system that can predict dangerous events

The SMART TUNNEL platform implements dynamic risk analysis, an improvement of risk analysis already set out in the Directive 2004/54/EC and in the Legislative Decree 264/06, for a swift, accurate and real-time response on risk.

The Internet of Things (IoT)

The Smart Road is provided with multiple sensors, with durable performances and extension. A number of monitoring systems will be implemented on road infrastructures. Think, for instance, about all the existing types of traffic sensors, to monitor devices' stress, ground conditions, local climate, environment, bridges, viaducts, tunnels, road barriers, hydrogeological conditions: IoT technology already offers (and will even more in the future) low-cost solutions for specific needs.

The market of both sensors and their applications is expected to rocket in the short term.

Roads are clearly deemed to become one of the hot industries, both for cities' connectivity direct applications and as enabling bodies for applications serving the areas covered.

[1] NCds, Article 13, paragraph 2, functional rules for the construction of roads provided for by the Highway Code,art.3

Open data and Big data

The Smart Road is a digital road which is deemed to produce a great deal of interesting data for infrastructures operators, travelers, authorities and for digital world planning bodies in general; data that can enable the development of new business areas. The data, in order to fulfill their dual task of making transports more efficient and promote development, will have to be:

- **"Open"**, according to known and well-established terms;
- **"Available"**, with known conditions.

The first condition will be devised according to existing regulations (national and European), while the second will be complied with through an adequate data filing, research and processing platform, based on advanced technologies and such that researching, processing and transferring data will be made simple and effective, both for internal use (services for Anas S.p.A.) and for third parties use with permissions.

To guarantee a balance between Big Data and Privacy, ANAS believes that the implementation of the privacy-by-design principle is fundamental: a transparent approach that will enable users to understand why their data are collected and how they will be used, as well as to have extensive control on their data.

As for personal data management, ANAS will collect, treat and use data in compliance with the laws on privacy in force, without the possibility of transferring them to third parties, thus ensuring their confidentiality.

Traffic and statistical data and events needed to manage the network and the information on mobility will be also made available on existing interoperational channels with the CCISS (Italy's National Information and Road Safety Coordination Centre). Moreover, there will be a discussion on the possibility to transfer, to third parties, only aggregated data to be used, anonymously, for statistical purposes (traffic data, travel time, times, events, etc.) and on the possibility to sell advertising spaces (solely related to added value services for Smart Road users, such as information and offers about service stations along the route) and access to specific services for third companies. However, those services are not to be activated during the first phase of the project, which focus is to guarantee greater land transport safety and to improve/enhance information services on mobility for road users.

1.1 Communication system

Personal devices and vehicles efficient connectivity is an essential condition for digital roads.

In this sense, the communication system plays a fundamental role to ensure:

- Connectivity between people and digital instruments;
- Vehicles connectivity;
- Infrastructures connectivity.

The Smart Road provides operators and users with a set of services aimed at efficiently using road infrastructures and consistently increasing the safety and efficiency levels of service.

The goal of this action is to create an advanced technological infrastructure that can support modern state-of-the-art Smart Road services and sustain the levels of growth that new services and new applications will require.

Therefore, the immediate guaranteed levels of performance and future growth potential will be fundamental requirements. The solution will be modular and scalable. This means having the possibility to expand the solution, in the future, to new road segments or new road infrastructures and the possibility to connect with technological systems on a wider scale, in order to create an integrated geographical network, consistent for technologies used and management and maintenance methods. For this purpose, we chose, as a prerequisite, to fit the solution to the most popular market standards and to those that are expected to spread in the future.

As for the new G5 system, the technological network planned will be based on the principles of a telecommunication network for its reliability, resilience to failures, performance level and transport capability. Besides these features, it will be improved with high flexibility and multiple connection standards and modes, which will be, particularly during wireless services provision, where maximum coverage is needed, compatible with multiple standards, efficient in radio spectrum use, flexible and capable of growth.

In developing the Smart Road, the telecommunication network, seen as a connectivity integrated system, is a fundamental part.

The planned network will be created with two types of communication systems and control centers:

- Label system; fiber optic, through a IP-MPLS (Multi Protocol Switching) wired network
- Two wireless systems:
  - Wi-Fi in Motion with IEEE 802.11 a/b/g/n standard in unlicensed frequencies 2.4/5 GHz to connect infrastructures and personal devices (i.e.: mobiles, tablets, etc.).
  - Wi-Fi with ETSI ITS-G5 standard for V2I (Vehicle to Infrastructure) connectivity.
- Local processing and control system and a central control system.

The network infrastructure described here is designed to provide modules, called Green Island segments, which are both independent and connected:

- **Independent**, each one can work regardless of the connection with other network segments and is provided with all the components for a stand-alone functioning, where needed;
- **Connected**, that can communicate with other green islands or with the control centre both to transfer data to support the Wi-Fi client communications and to coordinate and collect information flows generated by the system.

The expected size of a Wi-Fi segment ranges between 25 and 35 km (⊠16-22 mi): therefore, performance standards for the infrastructures provided must guarantee the levels of effectiveness for the expected size.

The network infrastructure requires two processing systems: a local one and one from the control centre.

The local system is based on a dedicated server infrastructure. Such infrastructure must be arranged so as to create a multi-centre system, which is resilient and can work independently from the central system.

The central infrastructure is designed to collect traffic coming from the outside network segments and to provide a central system that controls and connects with the company's IT systems.

The intelligent road that runs along with progress

Each server infrastructure must have the following base functionalities:

- **Gateway IP - Wireless network controller**: it is the link between the existing network and the Wi-Fi network and the node through which to implement routing, security, caching or address mapping (NAT) policies and collect information on client's position in the served segment. It is also useful to adequately sequence the Wi-Fi IP network;
- **Positioning Server**: it collects information on single clients signals compared to single network nodes trough gateway devices and gives back information on clients positions in relation with the served road segment;
- **Provisioning Server**: it is the system that dynamically provides configurations to wireless network nodes. Admin platform for O&M (Operation and Maintenance) activities;

- **Network Management**: system's monitoring, diagnostics and reporting platform. Each segment's diagnostic system will be integrated in the centre in order to provide a unified point of connection between the outside systems and the management platforms.

System architecture

The overview on system architecture takes into account different levels of data switching, routing, transfer, collection and service provision:

- first level of peripheral switching (Centre level) in every section of Anas S.p.A.'s roads or motorways;
- a second level of routing designed to connect the different first-level switching levels with the transmission backbone (Green Island segment nodes);
- a third level of connection between second-level nodes (secondary nodes) that can integrate with the transmission backbone and offer new or next-generation services.

Figure 2 - Smart Road concept

The following is a block diagram of the Smart Road's transmission systems architecture:

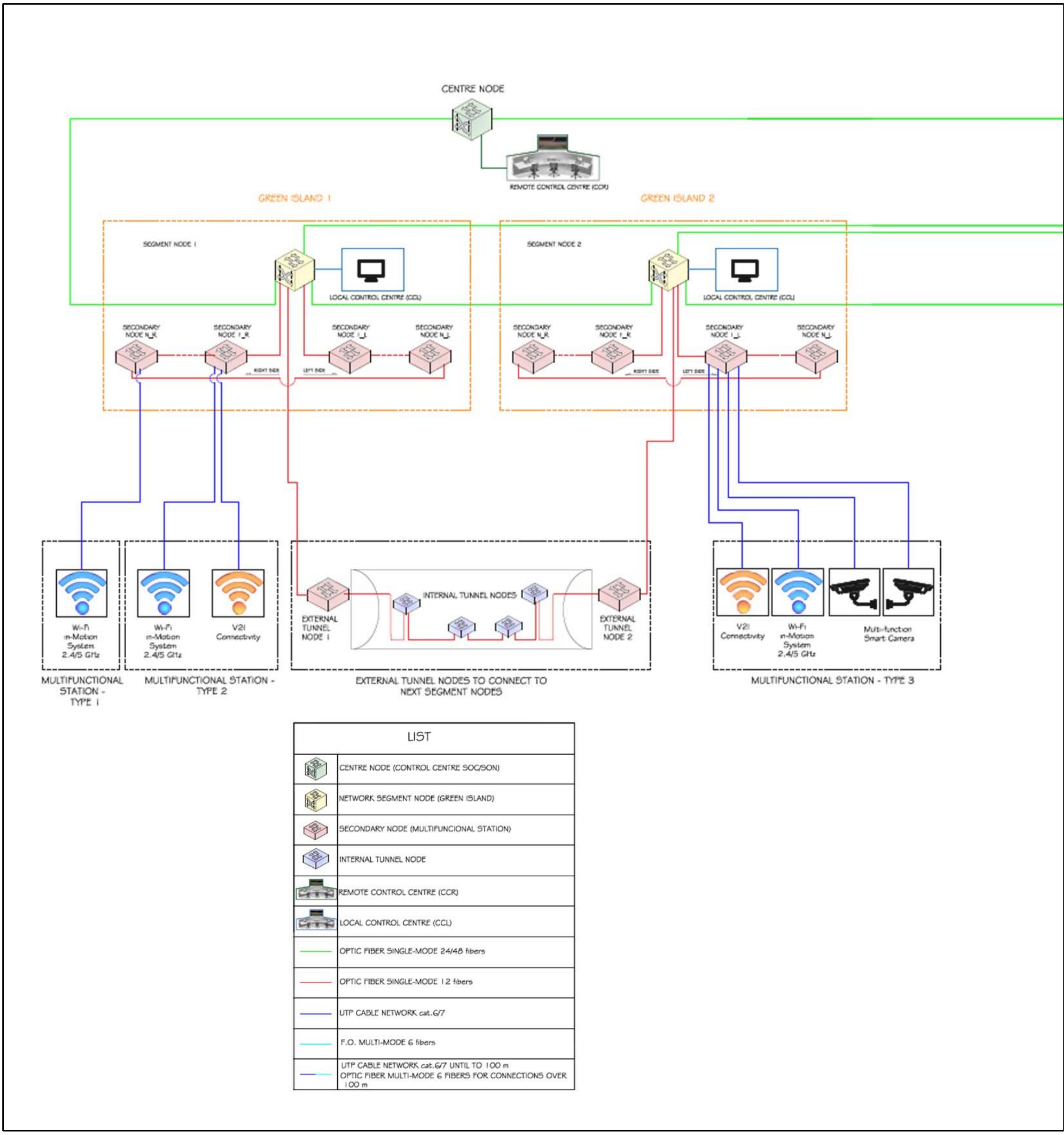
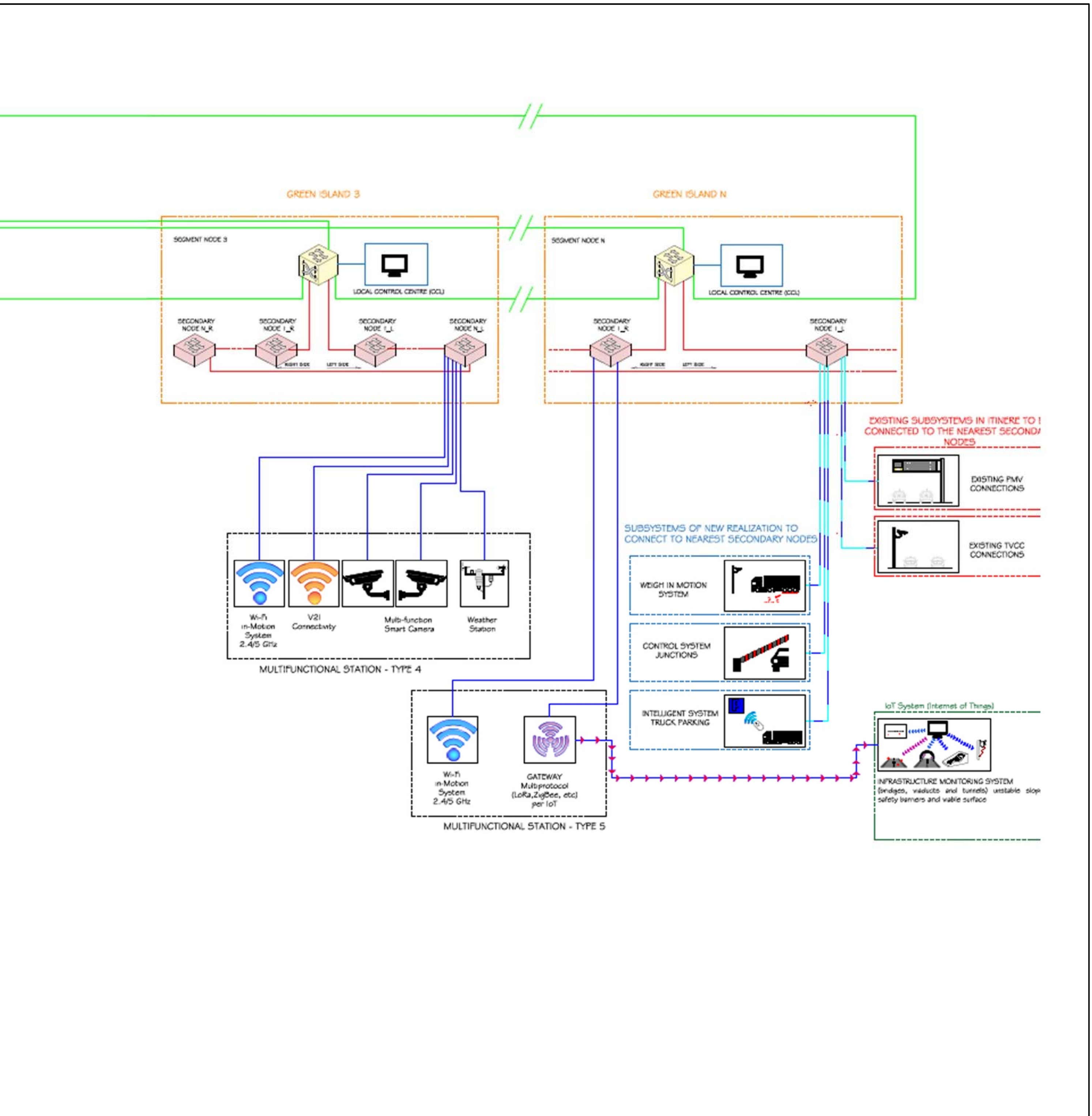


Figure 3 - Communication system diagram



GREEN ISLAND 3
GREEN ISLAND N
SEGMENT NODE 3
SEGMENT NODE N
LOCAL CONTROL CENTRE (CCL)
LOCAL CONTROL CENTRE (CCL)
SECONDARY NODE N_R
SECONDARY NODE I_R
SECONDARY NODE I_L
SECONDARY NODE N_L
SECONDARY NODE I_R
SECONDARY NODE I_L
Wi-Fi in-Motion System 2.4/5 GHz
V2I Connectivity
Multi-function Smart Camera
Weather Station
MULTIFUNCTIONAL STATION - TYPE 4
Wi-Fi in-Motion System 2.4/5 GHz
GATEWAY Multiprotocol (LoRa,ZigBee, etc) per IoT
MULTIFUNCTIONAL STATION - TYPE 5
SUBSYSTEMS OF NEW REALIZATION TO CONNECT TO NEAREST SECONDARY NODES
WEIGH IN MOTION SYSTEM
CONTROL SYSTEM JUNCTIONS
INTELLIGENT SYSTEM TRUCK PARKING
EXISTING SUBSYSTEMS IN ITINERE TO I
CONNECTED TO THE NEAREST SECONDA
NODES
EXISTING PMV CONNECTIONS
EXISTING TVCC CONNECTIONS
IoT System (Internet of Things)
INFRASTRUCTURE MONITORING SYSTEM
(bridges, viaducts and tunnels) unstable slop
safety barriers and viable surface

The network infrastructure is a multi-service type, that is, it can guarantee the transmission of advanced services even in triple play environments (voice, video and data), prioritize single types of traffic, configure queueing, enable traffic coloring, reserve bandwidth and implement security policies.

The main goal is to give the possibility to connect any-to-any in order to guarantee to each service its own features and apply the right design and traffic engineering rules to define service classes that can meet the described needs and those expressed during the creation of the new infrastructure.

Minimum transmission bands planned, unless further detailed in following paragraphs, will have to be:

- 10Gbps on the first level of peripheral switching (segment network);
- 100Gbps on other levels.

The architecture must have a 1:1 redundancy on all levels so that, if one element should be unavailable, the correct functioning of both the element's relevant level and the architecture in general is not hindered.

The central level carries out traffic collection from previously described levels and connects with the company's IT systems.

The architecture could be centralized or distributed ("Multi-center") and must have minimum performance standards to support the traffic generated in lower levels.

At this level, outside devices and network status diagnostic functionalities will be held. Information must be available for the integration of the RMT (Road Management Tools) system or other infrastructure management systems.

1.1.1 Wired System

The data transmission system is the physical infrastructure designed to connect devices installed along the motorway segment in full-duplex mode with the Remote Control Centre (RCC), ensuring information transmission (data, video, voice). Given the nature of transmitted data and the goal of Smart Roads in Anas' vision, the physical infrastructure ensures a high level of reliability for the connection.

The network architecture consists of a Centre Node (CN), located in the RCC, connected through a fiber-optic multi-ring backbone with each "Green Island" Segment Node (SN). Each SN consists of a redundant Segment Router (SR), which enables the connection between the segment and the backbone, and of a number of switches connected to one another with a fiber optic ring (segment ring).

The SR is also the beginning and the end of the segment ring. Each switch is connected to a number of outside devices, such as Infrastructure Monitoring Systems, VMS, Acces Monitoring Systems, Multi-function Stations, etc.

This system is divided into two logical blocks, formed by:

- Passive infrastructure, that is the physical means of transmission (fiber optic);
- Active infrastructure, that is the electronic components that collect relevant data from outside devices and send them to destination according to communication standards. Routers, switches and servers with gateway function make up the active infrastructure.

The backbone will be implemented with a multi-ring configuration in order to provide at least two alternative connection paths to the RCC, located at the Anas headquarter in charge of the area. Rings must also be closed with the wireless technology implemented in SMART ROADS. Moreover, immunity from possible SR failures must be ensured through SR redundancy.

Such an architecture enables to avoid malfunctioning caused by SR failures or by the interruption of the means of transmission.

As for rings wired closure, the two fiber optic cable branches could be trunked in separate positions (i.e. in motorways, on the opposite sides of the carriageway). This way, in case of interruption of one fiber ring branch, continuity will be ensured. Moreover, segment nodes could also be placed so as to create multiple rings that can bypass possible out-of-order Routers and also be path redundant.

The cabling system is designed so that information on racks status is sent to a software installed in the RCC. With this software, operators can check passive infrastructure connection status without physically going there. This enables the creation of a so-called intelligent cabling, which, acting at patch panel level, can detect the correct status of the cable on each patch panel port.

This way, troubleshooting operations are made easier, because it is possible to remotely check whether the interruption of a connection is caused by cabling issues. By cross-referencing data from the structured cabling with data from the active network management system, the type of failure can be identified more accurately, thus going on the field only when strictly necessary.

The cabling intelligent management system must be embedded in the connection hardware. It gives an automated and accurate solution to fully register and manage the physical level in real time from remote control stations. The system must be able to report real-time connectivity status and network's automatic documentation to the admin.

1.1.1.1 Network infrastructure

The whole infrastructure is designed by dividing, from a logical standpoint, the network into two different and separate types:

- Backbone;
- Segment or "Green Island" network.

Backbone

The backbone, with 100 Gigabit Ethernet (GE), connects all Segment Nodes with the Centre Node through fiber optic cables. The backbone is designed for a future upgrade to a multi-ring configuration, which gives a high level of reliability (as seen in Figure 3). The network must meet IEEE 802.3-2015 standard specifications.

The network is the 3rd layer of the ISO/OSI diagram and uses a Multi-Protocol Label Switching (MPLS) architecture.

MPLS, besides ensuring consistently better switching and throughput times than TCP/IP architecture, has a set of advanced functionalities:

- **Service quality support**. MPLS enables the creation, compared to TCP/IP, of connection-oriented network that can easily manage different levels of priority.
- **Traffic engineering**. It is possible to optimize the use of network resources by using a number of different paths between two points. Traffic can be routed using all the available paths in order to distribute it evenly on network resources, thus improving performances.
- **Path reconfiguration in case of failures**. When setting a network path, it is possible to define alternative (protection) paths to be used in case of failure of one or more sections of the main path. This way, path reconfiguration times will be much shorter than with IP routing.
- **Advanced services**. MPLS enables the creation of Virtual Private Networks - VPN. This way, between two remote points of the network, data can be transparently transmitted, fully separate from other traffic flows, thus generally improving network performances in terms of both quality management and security of information transmitted.

MPLS means basically addressing data packets by creating a switching label. Procedures for the distribution of labels will be defined by a non-proprietary LDP (Label Distribution Protocol).

Centre Node

The Centre Node consists of a modular, compact, non-blocking router with a full-duplex switching capacity of at least 1 Tbps. The device supports redundant mode with GPS and BITS (Building Integrated Timing Supply) signals inputs to meet needs of online sync, management console port. It also must be able to integrate up to four redundant power supply units supporting power supply voltage and the forced ventilation module. A solution with two power supply units for each device can also be accepted, considering however at least two devices for each node. It must provide at least two 100 Gb/s (GE) Ethernet interfaces with full feature parity on integrated interfaces on one single module slot.

It must be a carrier-class device, capable of ensuring service flexibility, scalability, performance and high availability to Ethernet Carrier transport networks, such as that described in this specification, and enable them for end-to-end services scalable, intelligent, flexible and converged transport.

It must be a highly reliable IP router that can support: clustering functionalities, capable of providing full sync of the Control and Forwarding Plane between two separate physical chassis and make them visible as a single logic element with only one Control and Forwarding Plane, with non-stop forwarding and non-stop routing functionalities. Carrying out this functionality with MC-LAG protocols is considered equivalent.

The device must support local or remote management and configuration, SNMP protocol and browser management and configuration. For this purpose, we request to provide a client-side application platform which is compatible with a large number of marketed devices, that can ensure communication between users and host and that can be used during the operation of the "Smart Road" technological platform.

We also request the same for the server side, integrated in the RMT system.

Fiber optic backbone

For the backbone network, fiber optic cables are used with metal protection and double coating, with Low Smoke Zero Halogen (LSZH) features. Fiber optic cables used must be CE marked and comply with regulations in force on safety and electromagnetic compatibility and with the ITU-G.655 standard. Fiber optic cables wiring must comply with the recommendations provided in the ISO/IEC 11801 2nd edition, EN 50173-1 2nd edition and EIA/TIA 568 C standards.

At each segment router location, 24 fibers from the backbone cable fibers are stripped through closures.

Segment Node

Each "Green Island" is connected to the backbone through a redundant SR, which must be:

- compatible with both protocol (L2/L3) and I level rings band management;
- enable functionalities planned for the backbone level;
- ensure a redundant 100Gbps towards the backbone and its redundancy peer device;

The device considered must have compact shape factor, low energy consumption, high throughput and enable the following base functionalities:

- L2VPN;
- L3VPN;
- MPLS-based;
- VPN;
- VRF.

Segment nodes will be lodged in special shelters or cabins provided with A/C units in order to ensure the best possible operational environmental conditions.

If a segment is isolated without the possibility to be connected to the backbone, then it must be connected to the Remote Control Centre, preferably through Anas' network, where available, or to a commercial provider through adequate Firewalls and Gateways to protect the segment network.

Firewall

The Firewall, if requested, will be lodged in a rack provided with redundant power supply units and at least 10 slots for future expansions. It will be lodged in special shelters or cabins provided with A/C units in order to ensure that it works in the adequate temperature range.

Segment Network

At the logical level, the segment network can be divided into two separate networks:

- Secondary switches network (SS);
- Switch - device link.

The switches network consists of a ring (secondary ring) that, through a 24 single-mode fibers optical fiber, connects SSs to the SR. The secondary ring implements a ISO/OSI layer 3 connection and uses a 10 Gigabit Ethernet MPLS architecture. Labels distribution procedures will be defined by a non-proprietary LDP.

Secondary switches must meet the following specifications:

- It must be an industrial, managed device, capable of supporting Ethernet connections with minimum speed 10/100 Mbit/s in PoE/PoE+ mode and must be provided with SFP and SFP+ slots for copper and fiber optic Fast Ethernet, Gigabit Ethernet and 10 Gigabit Ethernet transceivers;
- It must provide Fast Ethernet, Gigabit Ethernet e 10 Gigabit Ethernet wirespeed connectivity, advanced and intelligent switching services as security in network access, network performances check, traffic multi-cast management and QoS (Quality of Service) for critical control traffic performances;
- It must be compact and passively cooled without the aid of ventilation/cooling systems and must be provided with relay output signals and alarm signals inputs.

Secondary switches are connected to devices along the segment and will be lodged near those.

The connection between switch and device is an ISO/OSI layer 2 type, with a TCP/IP architecture and can be made either with fiber or copper.

Copper cables

The copper cable we are planning to use for the connection between network peripherals and relevant secondary switches is a Cat 6 UTP, which supports Fast Ethernet, Gigabit Ethernet and 10 Gigabit Ethernet protocols transmission. The 8 cables are divided into 4 pairs; each cable pair is twisted. Each cable has a 0.57mm (23 AWG) diameter and a coating; the 4 pairs are separated by a cross-filler. Copper cables must comply with regulations in force.

1.1.2 Wireless systems

Smart Road's wireless system is divided into two separate systems:

- The first one is the Wi-Fi in Motion with IEEE 802.11 a/b/g/n standard in unlicensed frequencies 2.4/5 GHz to connect infrastructures and personal devices.
- The second one is the Wi-Fi DSRC (Dedicated Short Range Communication) with ETSI ITS-G5 standard in the frequency band dedicated to V2I (Vehicle to Infrastructure) connectivity.

1.1.2.1 2.4/5 GHz Wi Fi in Motion system (Standard IEEE 802.11 a/b/g/n)

The Wi-Fi in motion system will be used for C-ITS applications and will connect road users' mobile devices, who will receive the information requested, **safely and without distracting them**, on their mobile device's loudspeaker. Other functions that may be available on the Wi-Fi network will be only allowed **when vehicles are stationary**.

WI-FI in motion network features and requirements

The Wi-Fi IEEE 802.11 a/b/g/n wireless network goal, in unlicensed frequency bands 2.4 Ghz and 5 Ghz, serving Smart Roads, is to enable wireless access to services offered by the procuring authority (Anas S.p.A.) for users owning devices with IEEE 802.11 a/b/g/n connectivity (hereafter, the "client"), such as mobile devices, VoIP phones and barcode readers. The aim is to make available all the services that the procuring authority wants to implement with systems and methods, not described in this project, which do not distract drivers.

The Wi-Fi will consist of:

- **Local Network Control Centre (LCC)**: the Network Control Centre (WIRELESS CONTROLLER), located in each Green Island, is a central node to manage and check the whole Wi-Fi network.
- **Wi-Fi Access Point**: the Access Point is the device that enables users to connect to the wireless network. The Access Point must be fitted to connect to the fiber optic wired network (AP wired) through the secondary node or, via radio frequencies, to other Access Points (AP mesh); the Access Point is the network element that carries out the Wi-Fi radio coverage in the 2.4 Ghz band (IEEE 802.11 b/g/n standard).

  The 5 Ghz frequency band (IEEE 802.11 a/n standard), besides reducing the risk of interference from other Wi-Fi networks which coverage extends, even partly, on the motorway, can be also used for the backhaul mesh in order to connect wireless Access Points to one another and ensure their redundancy on the segment backbone.

  Interference is highly likely, particularly in those motorway sections that cross cities in which there are facilities near the carriageway. The number of products which use the 5 Ghz frequency band is much lower that those that work with the 2.4 Ghz band.

  Near all domestic Access Points work in 2.4 Ghz. A simple domestic Access Point near the carriageway is highly likely to interfere with the backup point-to-point protocol along the motorway, thus notably hindering the reliability of the very backup. By using the 5 Ghz band instead, the radio space is much freer and the likeliness of interference is reduced to a minimum.

Wi-Fi network architecture

The proposed Wi-Fi network architecture must comply with requirements of flexibility, expansibility and resilience. Elements of resilience must be based on:

1. Self Healing: the proposed Wi-Fi network must be able to dynamically and automatically adapt Access Points' radio resources (radio channels and/or transmitted power levels) so as to optimize the radio frequency signal when interference is present or to restore a road section's optimal radio levels following the loss of an Access Point.
2. Site Survivability: Access Points must be able to communicate even without the Control Centre. The Wi-Fi network architecture is designed so that Access Points generally establish a communication under the control of the Control Centre. This is called the dependent mode and is the network's normal working mode. Access Points, to be installed for the creation of the wireless network dedicated to the Smart Road system, must be able to work even

without the Control Centre, carrying out locally the functions of the Control Centre. This is called the independent (or stand-alone) mode. The switch between one mode to the other (depending on the circumstances) must be automatically and seamlessly carried out, without hindering the clients' connectivity. This ability is called "Site Survivability". The Access Point adoption process by the Control Centre must be available both in Layer 2 and in Layer 3. Access Points must therefore work in adaptive mode, that is automatically adapting their working mode (dependent or stand-alone) depending on the situation.

As for routing, the proposed architecture must be able to avoid bottlenecks (or "single points of failure"), which are common in a traditional centralized network, and be highly scalable: it must be able to distribute the network intelligence and the traffic routing and security functionalities all over the network, while keeping the central management role in the Control Centre.

Each Access Point must be able to independently decide on security matters and local traffic routing, optimizing network resources. The result will be a safe, reliable and highly-performing network. Therefore, we request that local traffic is locally routed, without going through the Control Centre, in a dynamic and intelligent way. This way, the best of both a distributed and a centralized architecture is kept, because Access Point are centrally managed by the Control Centre.

This architecture type becomes fundamental in case of high traffic density stemming from a high number of clients connected to the same Access Point. Particularly, the Control Centre is prevented from quickly becoming a bottleneck for the whole network, voice applications and video traffic jitter-related issues are reduced and the network is more flexible and more capable. The local Control Centre remains the single Access Point anagement point, providing centralized configuration, check and troubleshooting functions.

1.1.2.1.1 WI-FI in Motion Access Points

Performance features

Access Points must be highly performing both in terms of radio signal and in terms of clients management functionalities, routing and available bandwidth. They must support the following features:

1. Compliant with IEEE 802.11a, 802.11b, 802.11g, 802.11n standards.
2. Fitted to support Power-over-Ethernet (PoE) powering mode, according to the IEEE 802.3af standard, without consistent loss in performance.
3. Have at least one Gigabit Ethernet port and LED warning lights.
4. Support the "VLAN tagging" mechanism, according to the 802.1q standard. APs must be managed on a "tagged VLAN".
5. Capable of being automatically updated with the proper software online, without actions at the location, remotely from the Control Centre.
6. Dual Radio (Band Unlocked) / Dual Band type, capable of granting access both in the 2.4 GHz and 5 GHz bands, or to support Mesh-type 5 GHz connectivity to connect wireless Access Points (called Mesha Access Points or MAPs) to wired Access Points (called Root Access Points or RAPs).
7. To support, in IEEE 802.11n standard, 20MHz and 40Mhz channels and up to 300Mbit/s Data Rate.
8. Each access point must ensure a capability of at least 100 simultaneous clients connected.
9. To support at least 8 SSID (Service Set Identifiers) for each radio; for each SSID, it must be possible to define specific security and authentication policies.
10. To support advanced RF (Radio Frequency) functions, such as:

- Mesh multi-top connectivity: the routing mesh algorithm used in Access Points must be a dynamic type, in order to ensure efficient routing, mesh-level low latency, low overhead routing, high-speed hand-over even with clients moving at motorway project speed (130 Km/h or ≈81 mph) and great scalability. Moreover, it must be possible, from a RAP node (Root Access Point), to reach not only adjoining nodes but also remote nodes through consecutive "hops" from one MAP (Mesh Access Point) to another: multi-hop technology limits the use of wired connections.
- MIMO 2x2 or higher antenna systems: the MIMO technology consists in the use of multiple antennas, both when transmitting and receiving, in order to consistently reduce interference, even in particularly hostile radio propagation environments (high interference from other devices or systems, obstacles which obstruct direct visual between APs or between AP and client, multipath fading, etc.).
- Spatial Multiplexing: Spatial Multiplexing enables the transmission of 2 or more data streams using 2 or more antennas in order to double the throughput of a wireless channel, not only for IEEE 802.11n but also for IEEE 802.11a/b/g clients
- Frame Aggregation: the Frame Aggregation function increases throughput by sending two or more data frames in a single transmission, thus reducing the impact of overheads on bandwidth consume.

11. The possibility to be managed both by the Control Centre and separately, through a CLI (Command Line Interface) or GUI (Graphical User Interface) access type.

Security functions

Each Access Points must include, locally, the following security functions:

1. Integrated firewall (Wired & Wireless). Firewall features must include:
   a. L2 / L3 stateful type, role-based and IP Filtering functionalities: no traffic towards the wired network shall be permitted without going through the Access Point role-based inspection.
   b. Wireless clients protection from « Man in the Middle » (MITM) type attacks through Access Points ARP dynamic inspections («ARP cache poisoning» prevention).
   c. Enable a safe optimization of the network flow by inspecting Access Points traffic before sending it to a local VLAN and without going through the Control Centre.
   d. Prevent «Denial of Service» (DoS) and «storm» broadcast/multicast type attacks from spreading towards the wired network without going through the Control Centre.
2. Native wireless anti-intrusion functions (Wireless Intrusion Detection System, or WIDS, and Wireless Intrusion Prevention System, or WIPS).
3. Authentication server (AAA).
4. Encryption systems:

64 and 128-bit WEP, WPA-TKIP

- WPA-PSK-TKIP
- WPA-AES WPA-
- PSK-AES WPA-
- IEEE 802.11i WPA2- AES
- WPA2-PSK-AES
- WPA2-TKIP
- WPA2-PSK-TKIP

Networking functions

Each Access Points must include, locally, the following networking functions:

1. Integrated DHCP server.
2. NAT (Network Address Translation) integrated functionality.
3. Quality of Service (QoS) management integrated functionality: WMM- PS/SIP CAC, WMM-UAPSD, IEEE 802.1p, Diffserv and TOS.
4. Firmware configuration and updates management local functionality (that is, integrated in Access Points).
5. Layer 3 routing and 802.1q/p, DHCP server/client, BOOTP Client, PPPoE e LLDP protocols. Traffic load-balancing with Rate Limiting and Bandwidth Management.
6. Layer 2 and 3 mobility functions (stateful roaming).
7. Fast roaming functionalities: generally, clients' fast roaming capacity between Access Points is managed by the Control Centre; however, even without it, Access Points must be able to share clients' authentication credentials with other Access Points of the network. This will enable clients to switch from one Access Point to another without the need to re-enter their credentials.
8. Wired/Wireless extended VLAN: at VLAN level, Access Points must enable the extension of the wired network VLANs to the wireless network, without the need to reconfigure VLANs at the wired level. This prevents the introduction of the Wi-Fi network from modifying existing wired networks and enables wireless clients to access wired VLANs and to switch between wired and wireless VLANs.

1.1.2.1.1 Mobile Edge Computing (MEC)

Multi-access Edge Computing (MEC) is a platform that can process data and information near the radio infrastructure (regardless of the access technology used, i.e. 4G or Wi-Fi), with a consistently reduced latency. MEC enables Virtualized Network Functions for private and public multi-technology radio networks. Thanks to the virtualized software nature, MEC is a flexible, scalable and efficient technology. Multi-access Edge Computing technology is a ETSI Industry Specification Group standard (ETSI GS MEC 003 V1.1.1 (2016-03, see http://www.etsi.org/technologies-clusters/technologies/multi-access-edge-computing). The main functionality of MEC technologies is to introduce ultra-low latency and high bandwidth, that can make available real-time services for multiple applications in ANAS' Smart Road project. The most common use-cases for MEC technologies are:

- Video analytics
- Location services
- Internet-of-Things (IoT)
- Local and optimized distribution of contents

In ANAS' Smart Road vision, MEC technologies, paired with a wireless access network based on WIFI technology (that can also support key standards for in-motion connectivity, such as the 802.11r/k), serve to enable content distribution and collection from smartphones through TCP sessions as local and stable (thanks to low latency) as possible. This will enable to transfer a significant amount of data in a short period of time, that is the period the WIFI client, which is moving at motorway speed, remains connected to an Access Point. For each 30 Km motorway segment, a platform with Mec technology, installed on a dedicated server, must be planned; such server will be lodged inside the racks hosting fiber optic transmission devices.

1.1.2.2 System for V2I connectivity

The following paragraphs indicate the main standards relating to V2I connectivity, the IEEE standard 802.11p and the communication architecture in the ITS (Intelligent Transportation System) indicated in the ETSI standards.

ITS (Intelligent Transportation Systems) are systems that have advanced information and communication technologies in order to improve the safety of driving and the safety of people, the safety and protection of vehicles and goods, the quality, as well as the efficiency of the transport systems for passengers and goods. ITS follow standards both internationally and nationally.

V2I (Vehicle to Infrastructure) technologies have the main objective of preventing road accidents caused by driver errors and distractions, thanks to the ability to recognize situations of possible collision and potential hazards sooner than the driver can do. The V2I is based on the exchange of information between vehicles and infrastructure, communication exploits DSRC technology (Dedicated Short Range Communications) for the exchange of data such as location of each vehicle, its speed, direction and possible deceleration. The devices that allow communication with the road user can be installed directly on board in the case of new vehicles or may be the subject of "aftermarket" in the case of vehicles already existing or, again, personal communication devices may be used (for example: mobile devices, tablets, etc.).

Wireless DSRC communication is bidirectional and enables fast and secure messaging for road safety applications, where the "short range" is dependent on the surrounding environment.

DSRC technology guarantees:

- Rapid Network Acquisition: communications must be fast and updated in real time;
- Low Transmission Latency: road safety applications must be able to recognize and transmit messages without temporal delays with transmission latencies less than 50 ms;
- High Reliability: road safety applications must guarantee the operation also at high speed and in any weather condition;
- Priority: security-related applications take priority over applications not related to road safety;
- Security and Privacy: DSRC guarantees authentication and privacy systems.

Some applications of DSRC communications can be listed as follows:

- Visualization of vehicles presence in blind spots (blind spots); Indication of next collision;
- Indication of sudden braking of the previous vehicle;
- Indication of the impossibility of overtaking (blind spots);
- Indication of rescue vehicles approaching;
- Indication of vehicle tipping;
- Signage on board;
- Authorization and reporting of the presence of heavy transport vehicles;
- Indication of vehicle next to lane change;
- Indication of vehicle in the wrong direction.

ITS communications, on the basis of what is established by the National Plan of Frequencies Distribution take place in a dedicated band that guarantees minimal interference since pre-existing operators operating in the intron of this frequency do not exist.

The ETSI (European Telecommunications Standards Institute) also compiles standards at European level in the Information and Communications Technologies (ICT) area.

Within the ITS, ETSI published two standards for messages exchanged between vehicles and infrastructure or between vehicle and vehicle:

1. The specifications of the Cooperative Awareness Basic Service: this standard describes the specifications of the CAM (Cooperative Awareness Message) that is the messages exchanged between the vehicle and infrastructure (see ETSI EN 302 637-2).
2. The specifications of the Decentralized Environmental Notification Basic Service: this standard describes the specifications of the DENM (Decentralized Environmental Notification Message) that is messages sent to vehicles related to alarm events occurring in the road as per excessive traffic (see ETSI EN 302 637-3).

To support the V2I and/or V2V communication and therefore the exchange of information, the Ministry of Infrastructure and Transport indicated, in particular, the need to have integrated communication platforms based on ETSI G5 DSRC standards.

The ETSI G5 technology describes the frequency bands for communication between V2V or V2I as indicated in the following table (see ETSI EN 302 663):

Table 1 - Frequency bands for V2V and V2I communication

	Frequency range (MHz)	Applications
ITS-G5D	From 5 905 to 5 925	Future ITS Applications
ITS-G5A	From 5 875 to 5 905	Applications related to road safety
ITS-G5B	From 5 855 to 5 875	Non-safety ITS Applications
ITS-G5C	From 5 470 to 5 725	RLAN (WLAN)
CEN DSRC	From 5 795 to 5815	Collection of electronic toll

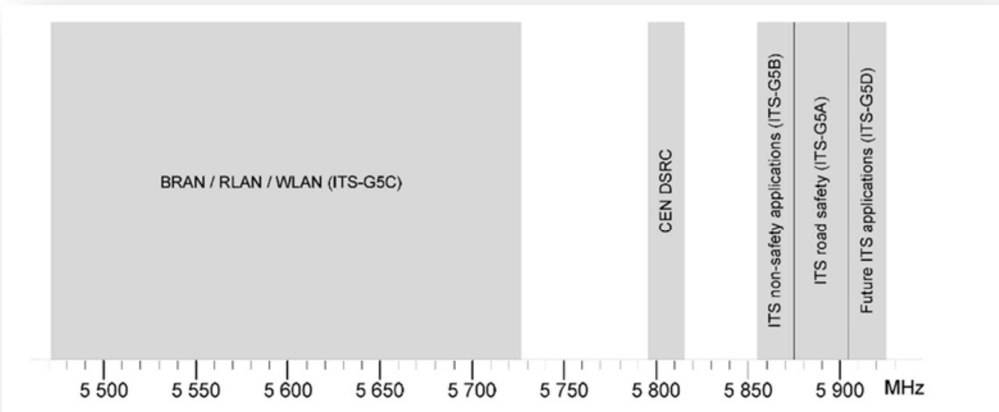


Figure 4 - Frequency bands for communication between V2V or V2I

The figure above shows the European frequency band identified by the ETSI G5 and by the Dedicated Short Range Comunication (DSRC) used for electronic toll collection.

The DSRC includes the following units:

- OBU (On Board Unit): equipment provided with an antenna intended for use in vehicles on road or railways (see ETSI standard EN 300 647-2-2);
- RSU (Road Side Unit): equipment provided with an antenna intended for use in road and motorway infrastructures (see ETSI EN 300 647-2-1).

The introduction of the frequency band of the DSRC has led to the development of the 802.11p standard used in V2V and V2I communication.

The IEEE 802.11p is an amendment to the 802.11 standard that adds some modalities and modifies parameters of the MAC (Medium Access Control) and PHY (Physical layer) level to allow and regulate communication in vehicular environments. The changes mainly concern the 802.11a standard that operates on 5GHz, the frequency used by the PHY 802.11p level is in fact 5.9 GHz.

Communication architecture in ITS (ITSC)

ITSC (Intelligent Transportation System Communication) is the communication system dedicated to transport as shown in the following figure (see ETSI EN 302 665):

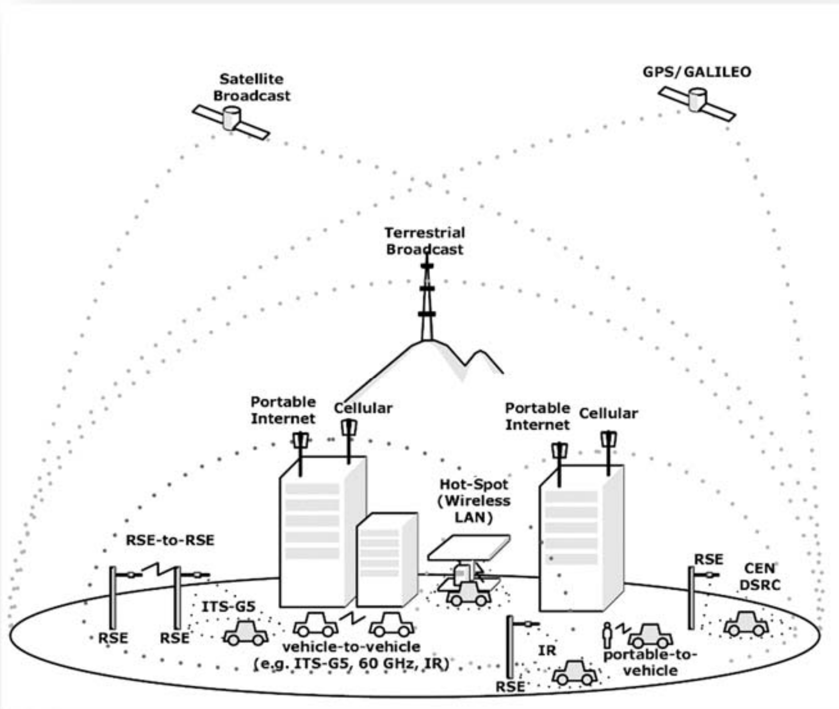


Figure 5 - Simplification of the ITS communication scenario

The main sub-systems involved in ITSC are:

- The mobile devices of users who travel the road;
- Vehicles (cars, trucks, etc.);
- Road infrastructures (tunnels, portals, etc.);
- The Central System that manages and monitors road infrastructures. In the case of Anas the central system is the RMT system.

Each of the sub-systems indicated above contains an ITS station which, depending on the context, can have one or more functional components as shown in the following figure:

The detailed figures of the ITS stations of the "Vehicle" sub-system, of the "Infrastructure" sub-system and of the "Central Sustem" sub-sustem are shown below:

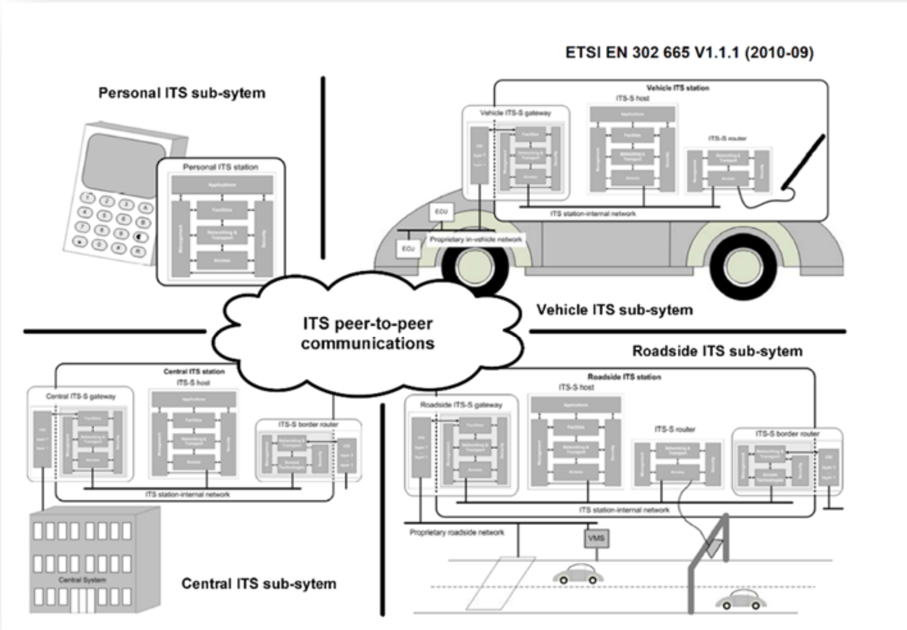


Figure 6 - Simplification of ITS systems

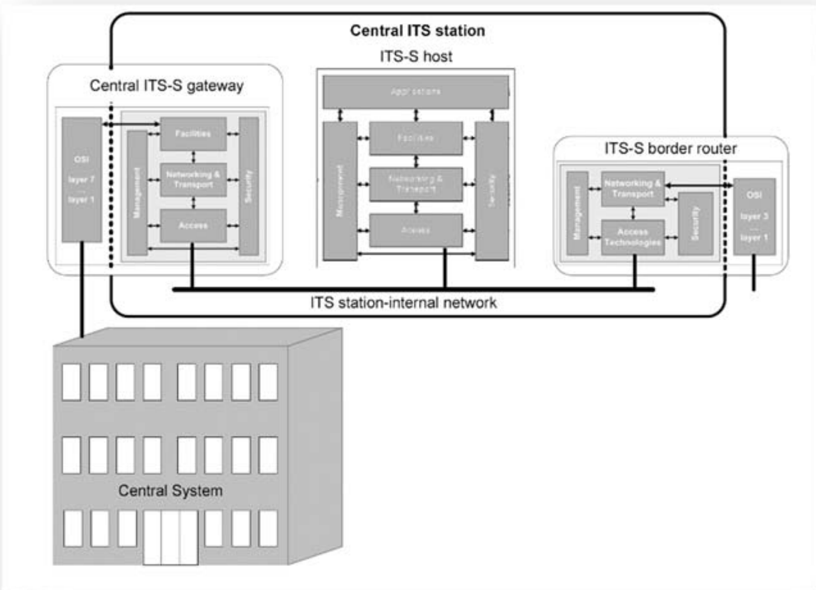


Figure 7 - Simplification of the ITS "Central System" station

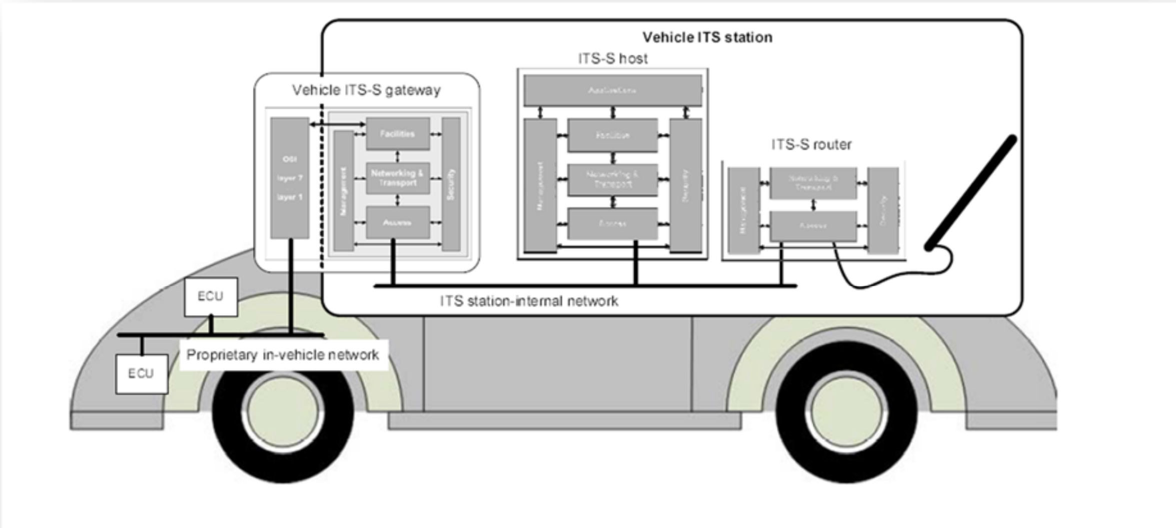


Figure 8 - Simplification of ITS "Vehicle" station

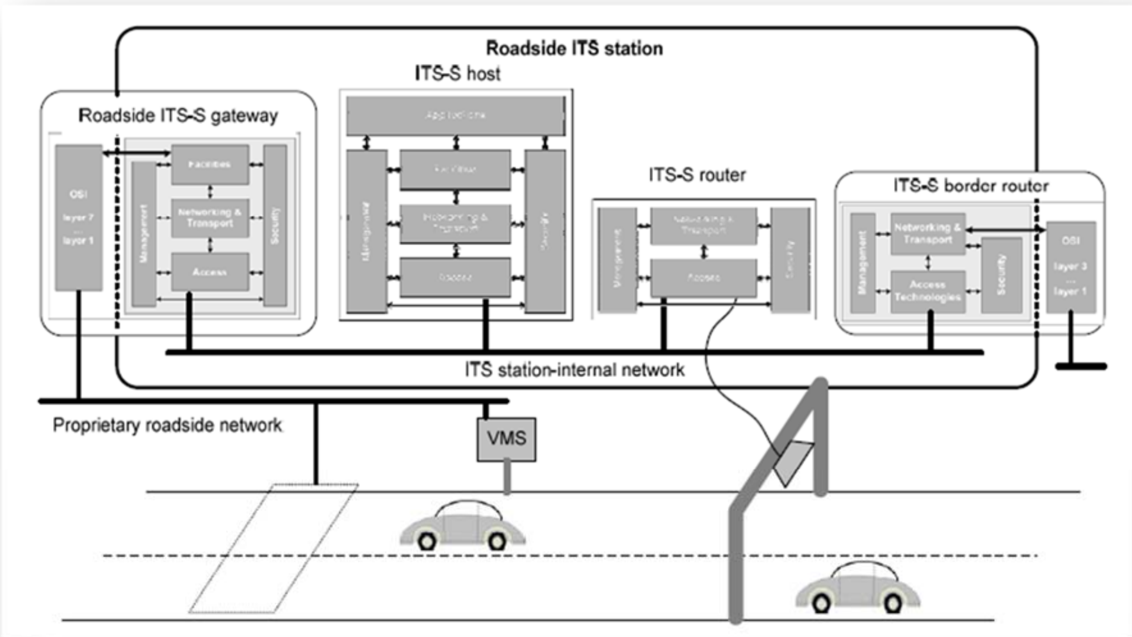


Figure 9 - Simplification of ITS "Infrastructure" station

The functional components present in the ITS stations indicated above are:

- **ITS-S host**: contains ITS applications and the functionalities necessary for them;
- **ITS-S gateway**: connects the sub-system (vehicle, infrastructure, central system) to its internal ITS network;
- **ITS-S router**: connects two ITS protocols, ie the ITS internal network of the ITS station and a ITS external network;

- **ITS-S border router**: used to manage and connect all the systems and equipment present in the infrastructure manager's network. In particular, the manager's network could follow communication standards different from those typical of ITS, for example MPLS or Internet. The plant park belonging to the infrastructure manager also includes "Infrastructure" sub-systems involved in ITSC.

The functional components of ITS stations (ITS-S host, ITS-S gateway, ITS-S router and ITS-S border routers) have a general architecture that **follows the principles of the Open System Interconnection (OSI) model**. With the exception of the ITS-S host, each functional component has sections specific of the general architecture shown in the following figure (see ETSI EN 302 665):

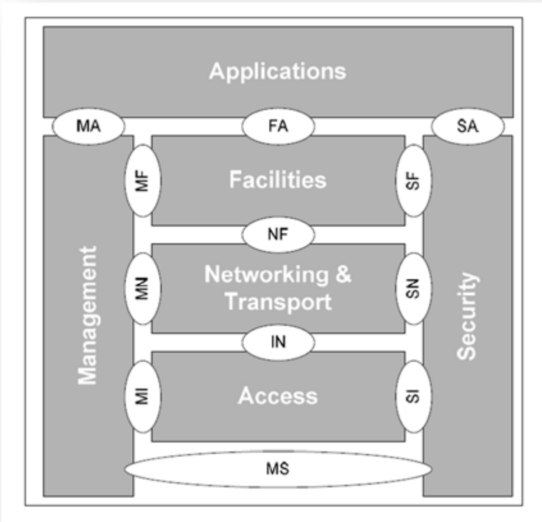


Figure 10 - Architecture of ITS stations

The three central blocks of the architecture reflect the functions of the OSI model, in particular:

- The "**Access**" block represents layers 1 and 2 of the OSI model;
- The "**Networking & Trasport**" block represents layers 3 and 4 of the OSI model;
- The "**Facilities**" block represents layers 5, 6 and 7 of the OSI model.

The blocks identified by the architecture are interconnected by interfaces or by means of "Service Access Point (SAP)" (eg MI, MN, MF, etc.).

Although the concept of layers within the OSI model is based on individual layers, in the architecture of the ITS stations each layer contains within it an additional set of functions referred to as "Cross-layer functionality" (see ETSI EN 302 665):

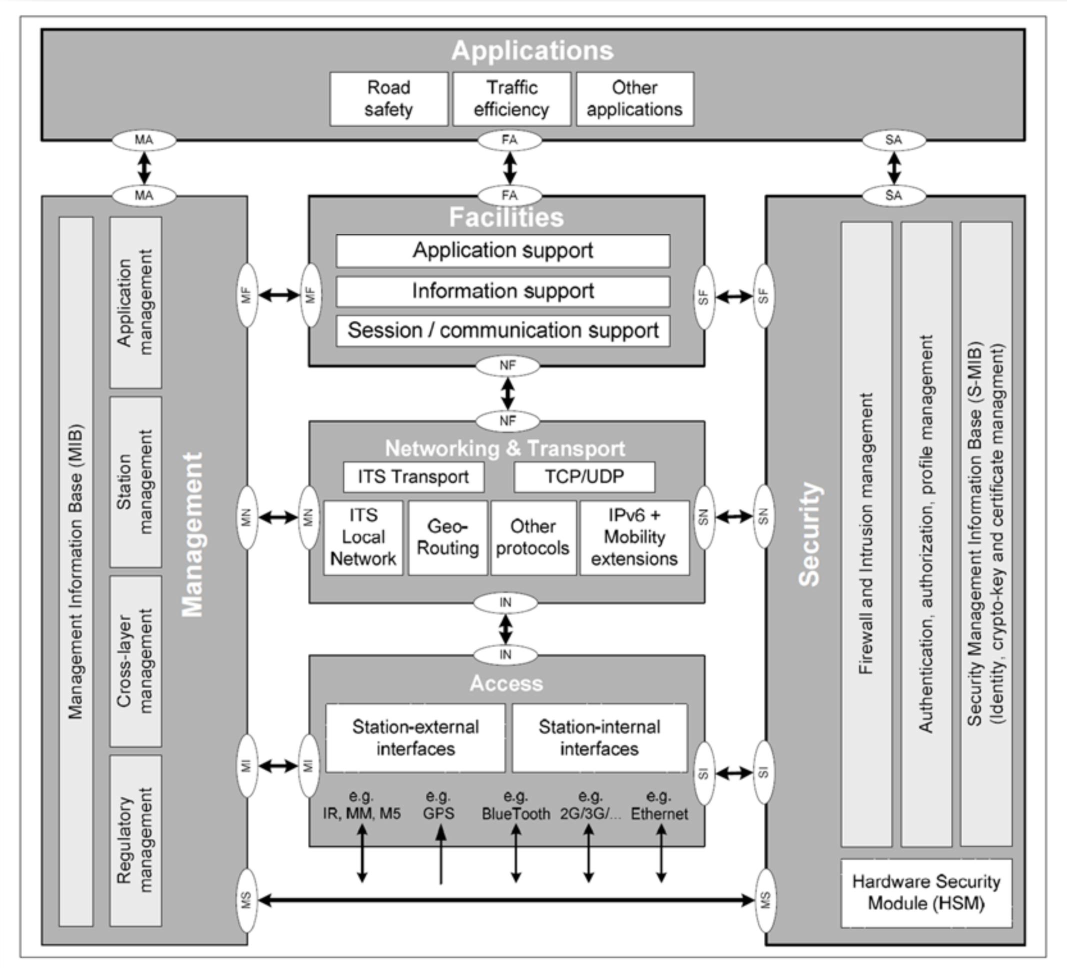


Figure 11 - ITS stations architecture functions

The following paragraphs show the detailed structures of the six blocks of the ITS stations architecture.

Applications Layer

The Applications Layer represents the ITS applications used to provide ITS services from a user to another, for example, the exchange of information between vehicle and vehicle or between vehicle and infrastructure.

The details of the Application Layer are shown below (see ETSI EN 302 665):

Figure 12 - Detailed functions of the Application Layer

The Applications Layer includes three classes of applications: **Other Applications**.

The following table shows the relevant use cases for each application class (see ETSI TR 102 638):

Table 2 - Application classes and related use cases

Applications Category	Applications	Uses	Day C-ITS Services List
Active Road Safety	Assisted driving/ Safety Information	Warning of presence of rescue vehicles	Day 1 C-ITS Services List
		Warning of slow vehicle	Day 1 C-ITS Services List
		Collision alert near Inter	Day 1 C-ITS Services List
		Motorcyclist Reporting	
	Assisted driving/ Reportin g of Dangers	Electronic emergency stop light when braking	Day 1 C-ITS Services List
		Alert of driving in the wrong direction	
		Warning of vehicle stationary due to accident	Day 1 C-ITS Services List
		Warning of vehicle stationary due to breakdown	Day 1 C-ITS Services List
		Reporting Traffic Conditions	Day 1 C-ITS Services List
		Reporting violation of road signs	Day 1 C-ITS Services List
		Reporting of the presence of road works	Day 1 C-ITS Services List
		Risk of accident alert	Day 1 C-ITS Services List
		Data coming from the risky vehicle/place	
		Data coming from vehicle/ atmospheric precipitation	
		Data coming from vehicle/road surface adhesion	
		Data coming from vehicle/visibility	
		Data coming from vehicle/wind	
Traffic Efficiency	Speed management	Speed limit notification	Day 1 C-ITS Services List
		Recommended speed near traffic light	
	Cooperative Navigation	Traffic information and recommended itineraries	Day 1.5 C-ITS Services List
		Signaling closed sections / alternative routes	Day 1.5 C-ITS Services List
		Assisted navigation	
		Repetition of road signs on board	Day 1.5 C-ITS Services List
Local Cooperative Services	Service Based On localization	Notification of Points of Interest	Day 1.5 C-ITS Services List
		Automatic access control and parking management	Day 1.5 C-ITS Services List
		ITS for electronic commerce	
		Media Downloading	
Internet Services	Service for connectivity	Insurance / finance services	Day 1.5 C-ITS Services List
		Fleet management	
		Loading areas management	
	Life cycle management ITS stations	Vehicle software/data collection and updating	
		Vehicle database calibration	

The European strategy on C-ITS systems, published in Brussels on 30/11/2016, identifies one list of services that intelligent transport systems must provide to users along European road networks. The set of services provided to the user by the Smart Road is shown in the previous table subdivided by category of applications, with reference to the list of C-ITS services indicated by aforementioned European strategy.

The list of services provided by already technologically mature C-ITS systems should be implemented quickly, so that end users and society in general can benefit from it as soon as possible. This list of services already available is defined as a list of C-ITS Day 1 services.

In a second phase, the services belonging to a second list of services, called Day 1.5, must be provided for the commission, the latter list includes a set of services for which the specifications or complete standards may not yet be technologically available for the large-scale distribution from 2019, even though they are generally considered to be already existing.

Facilities Layer

The Facilities Layer provides support to ITS Applications in particular it is structured in such a way as to provide generic functions identified by applications and their use cases. The details of the Facilities Layer are shown below (see ETSI TR 102 638):

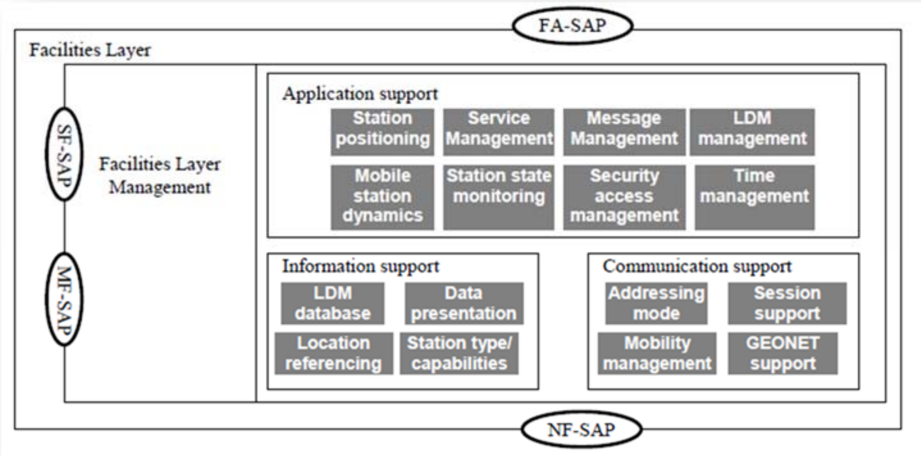


Figure 13 - Detailed Functions of the Facilities

Layer The Facility Layer consists of three main sections:

1. Application Support: kernel of the common functions supporting the Application Layer;
2. Information Support: repository of static and dynamic information used by the Facilities Layer and accessible from applications;
3. Communication support: manager of the different communication modes.

Networking & Transport Layer

The Networking & Transport Layer contains the network and transport protocols and their management.

The details of the Networking & Transport Layer are shown below (see ETSI EN 302 665):

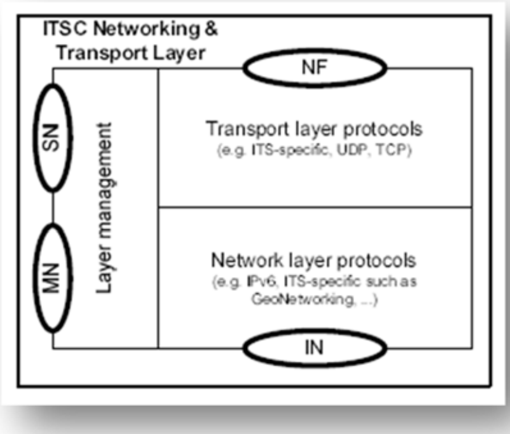


Figure 14 - Detailed functions of the Networking & Transport Layer

Access Layer

The Access Layer consists of three main sections:

1. **Physical Layer (PHY):** physically connected to the means of communication;
2. **Data Link Layer (DLL):** divided into Medium Access Control (MAC) that manages access to the means of communication and the Logical Link Control (LLC);
3. **Layer Management** that directly manages the Physical Layer and the Data Link Layer.

The details of the Access Layer are shown below (see ETSI EN 302 665 ETSI EN 302 663):

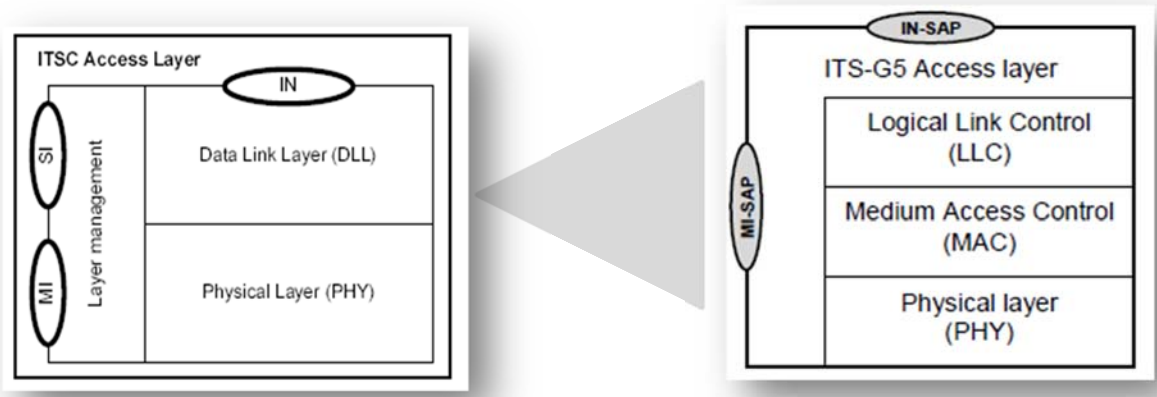


Figure 15 - Detailed functions of the Access Layer

Physical Layer

The Physical Layer is closely related to the transmission of the message between ITS stations (vehicle, users' mobile infrastructure and systems).

The figure and the explanatory table of the Protocol Data Unit of the Physical Layer are shown below (see ETSI EN 302 663):

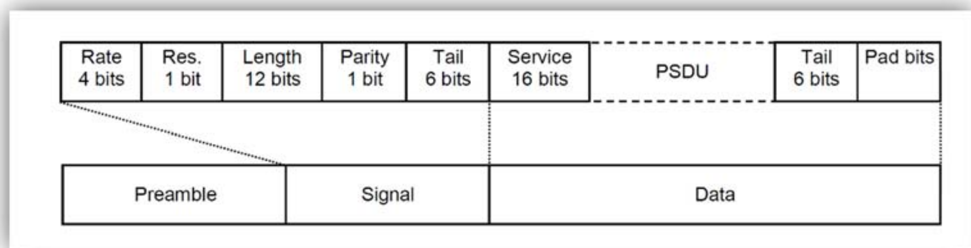


Figure 16 - Protocol Data Unit of the Physical Layer

Table 3 - Protocol Data Unit of the Physical Layer

Field	Subfield	Description	Duration [µs]
Preamble	N/A	Synchronizing receiver. Consists of a short and a long training sequence.	32
Signal	Rate	Specifies the transfer rate at which the data field in the PPDU will be transmitted.	8
	Reserved	For future use.	
	Length	The length of the packet.	
	Parity	Parity bit.	
	Tail	Used for facilitate decoding and calculation of rate and length subfields.	
Data	Service	Used for synchronizing the descrambler at receiver.	Depending on selected transfer rate and packet length.
	PSDU	The data from the MAC layer including header and trailer, i.e. MPDU.	
	Tail	Used for putting the convolutional encoder to zero state.	
	Pad bits	Bits added to reach a multiple of coded bits per OFDM symbol (i.e. 48, 96, 192, 288, see Table B.1).	

Medium Access Control

The Medium Access Control (MAC) manages the flow of sending and receiving the message in order to minimize interference in the system and increase the probability of receiving the whole message.

The diagram of the message sending and receiving flow is shown below (see ETSI standard EN 302 663):

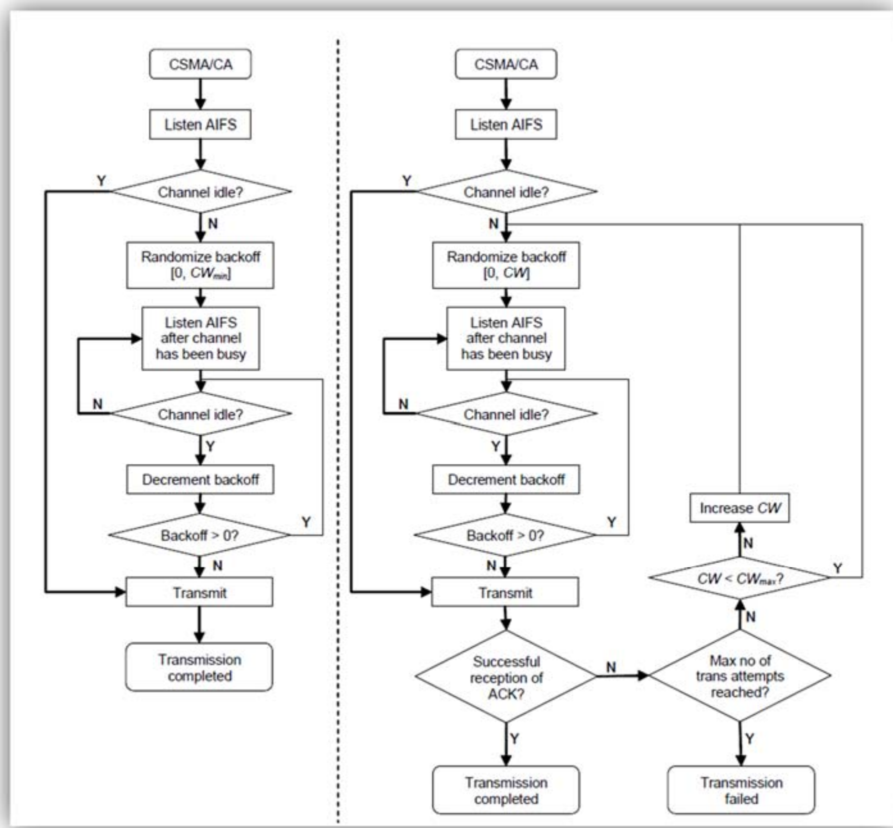


Figure 17 - Message reception flow

Management Layer

The Management Layer manages the transversal communication of the ITS station, in particular it deals with the management of the network, communication services and advertising services. The details of the Management Layer are shown below (see ETSI EN 302 665):

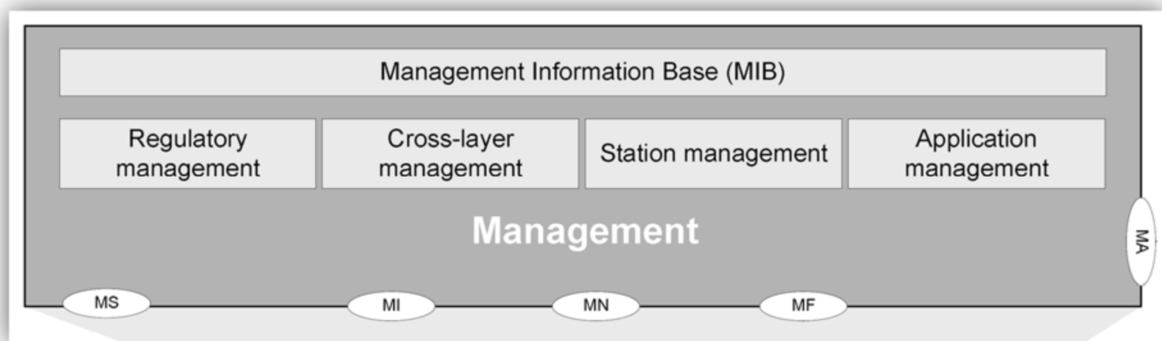


Figure 18 - Management Layer

Security Layer

The Security Layer contains the functions related to computer security in particular deals with the management of intrusion, authentication, authorization, certificates, security of information and hardware security modules.

The details of the Security Layer are shown below (see ETSI EN 302 665):

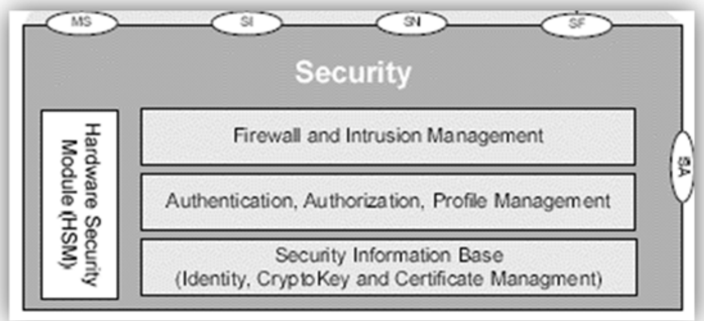


Figure 19 - Detailed functions of the Security Layer

1.1.2.2.1 Road Side Unit

This paragraph defines the technical specifications of the Road Side Units (RSU), radio modules based on industrial WLAN technology used for communication between infrastructure and On Board Unit (OBU) devices installed on vehicles. Each RSU as well as having transmitter and receiver functions, processes and sends data to the system control center.

The RSU must be prepared for mounting on a support and must be installed at a height of more than 4 m. The RSU must transmit local and selective information to the road users in real time through DSRC (Dedicated Short Range Communication) to ETSI ITS-G5 standards. They must also be equipped with further communication interfaces such as Ethernet, LTE and WLAN standards.

The RSUs must have Layer 2 and Layer 3 functions and must be updated automatically through the wired network and without the need for interventions on the ground through the control center. The RSU must guarantee a Data Rate in transmission and in reception of 6 Mbit per second both for the information channel and for the service channel with an overall data rate of not lower than 12 Mbit/s. The information channel is standardized according to the ETSI ITS-G5 specifications while the service channel will be used by the system operator according to the standard communication protocols for dedicated uses.

The RSU must have characteristics of robustness such as to guarantee high performances in all environmental conditions and must have an IP67 degree of protection and be able to operate at a range of temperature between -20 ° C and +65 ° C. All connections of the RSU must be accessible from the outside of the enclosure whose closure, for security reasons, must be guaranteed by appropriate seals for the visual indication of its illicit opening.

1.1.3 Additional data communication technologies that can be implemented in the Smart Road

In order to safeguard and enhance over time the investment made on Smart Road systems, ANAS look carefully at the evolution of cellular technology-based connectivity systems also in the experimental phase and not yet available on an industrial scale. In fact, in addition to the two expected systems of wireless connectivity, the highly scalable architecture of the Smart Road data infrastructure, will give the possibility of opening also to the development of a possible cellular type infrastructure based on small cells through an easy installation of small telecommunications equipment used both in a complementary way and independently of the radio cells of the mobile phones. This will allow the Smart Road to accommodate a hybrid data communication system also implementing systems based first on the 14th release of 3GPP LTE-V (3rd Generation Partnership Project), which includes Vehicle-to-Everything communication (V2X) with direct focus on Vehicle-to-Infrastructure communication (V2I) Vehicle-to-Vehicle (V2V), as well as the area of Vehicle-to-Network communications (V2N), up to the next most advanced 5G standard, characterized by an ultra-low latency and high data flow (throughput).

1.1.4 Site Survey

For a more performing arrangement of the AP and the RSU the Site survey must be carried out regardless of the solution and the number of AP Wi-Fi and the RSU, the coverage of the zones requested must be complete. A planning study of the positioning of the AP Wi-Fi and RSU in the affected road route using a radiofrequency coverage simulation software tool is appropriate.

The software tool will have to use 2D / 3D digital maps that accurately model the areas and the obstacles to propagation and report on the same maps the RF signal level (RSSI) with areas of different colors, in order to predict the behavior of the proposed Wi-Fi system from the RF point of view. It is required that the minimum RF signal level received from a client is not less than -65 dBm and that the ratio between the useful signal and the interference and noise level is sufficiently high, in order to guarantee the correct functioning also of the Voice Over IP (VoIP) service.

A site survey is also required after the installation and activation of the new AP and the RSU so that discrepancies between the initial software simulation and the actual state of affairs can be highlighted.

In all cases, the site survey must be complete with reports and visual mappings for the following parameters:

- positioning and coverage of Access Points and RSUs;
- signal distribution and power;
- signal/noise ratio;
- interference;
- data rate.

1.1.5 Smart Road Control Center

For the management of the entire infrastructure there are two different levels of Control Center:

- Remote Control Center (CCR) which corresponds to the RMT functions supplied either centrally or at the territorial offices where the software platform is installed for the management and control of the backbone IP-MPLS wired network;
- Local Control Center (CCL) where the data center and the equipment and the devices for the production, distribution, transformation and storage of electricity are located.

The Local Control Center Data Center will consist of multiple server platforms (hardware), on which the management and control software platforms of the various technological systems present in the field will be installed, in particular the following platforms will be present:

- Software platform for the management of charging stations for electric vehicles installed on dedicated industrial PC;
- Software platform for monitoring and controlling energy data installed on dedicated personal computer;
- Software platform for monitoring and controlling the electrical system installed on dedicated industrial PC;
- Software platform for the management of Multi Funcion Smart Cameras installed on dedicated server;
- Software platform for managing and controlling the in-motion WiFi system installed on dedicated server;
- Software platform for the management and control of the ETSI ITS G5 DSRC system installed on dedicated server;
- Software platform for the management and control of the segment IP-MPLS wired network installed on a dedicated server;
- Software platform for the management and control of the "Smart Tunnel" system tunnels installed on a dedicated server;
- Software platform for the management and control of the IoT monitoring system installed on dedicated server.

To increase the scalability and reliability of the architecture as a whole the environment of virtualization must be based on an architecture whose physical servers have load balancing and redundancy capacity.

The virtualization platform must allow "live" migration of virtual machines to allow maximum availability of services during O & M operations.

In support of each system a Storage Area Network platform must be provided on I-SCSI protocol for sharing virtual disks and a Network Attached Storage for functions of backup.

All the software applications of the various devices present in the field will have to communicate with the CCR and with the RMT system so as to make it possible to remotely manage the various systems such as, for example:

- Radio system;
- Internet of Things system (IoT);
- Smart Tunnel System
- Dynamic lane management system
- Infrastructure monitoring system;
- Traffic and Freight Monitoring system;
- Environmental monitoring system;
- Drone monitoring and intervention system;
- Energy production system;
- Technological center;
- Energy distribution system.

In each "Green Island" a CCL will be established, interconnected with the CCR and the RMT system.

1.1.5.1 Wired network management software platform

The MPLS backbone and the segment one will be managed by a high reliability platform, installed on 2 dedicated servers, each of which must provide the following features:

- support of a variety of services including VLL, VPLS, H-VPLS and IP VPN;
- end-to-end service provisioning with point & click methodology, in a centralized way;
- GUI of user friendly type, based on an interface with predefined "Service Templates";
- centralized management of alarms, with intelligent correlation of them with the network elements and service instances involved;
- diagnosis and troubleshooting in a centralized and automatic way on the levels of network infrastructure and single service (Service OAM);
- discovery and graphical view of level 2 and 3 of the wired network;
- management of IP routing and access ACLs;
- carrier-class resilience and synchronization between the management system database and the managed devices;
- security features that involve the use of accurate control policies of access privileges of operators by defining detailed profiles, optionally with assignment of user-id and password and through User Authentication protocols. All the loggings to the system and the operations performed are tracked for security reasons;
- possibility of obtaining real-time or historical traffic statistics at any point in the network;
- possibility to have information on the packages offered / forwarded / discarded at gate and service;
- level loss, jitter and delay measurements;
- possibility to define thresholds on the values of losses, jitter and delays whose exceeding generate alarms;
- collection of statistics for thousands of simultaneous services without negative impacts on the CPUs of nodes and management systems.
- QoS support;
- time detail of the traffic sent;
- all information regarding the status of each segment node;
- centralized firmware update of each node with indication of possible errors and faults and possibility of restoring the initial conditions;
- alarms and reported alerts, such as:
    - Problems on updating the firmware;
    - Hardware faults to the infrastructure;
    - Security alarms;
    - Capacity problems;

The results of monitoring the various parameters of the infrastructure will have to be made available on visual and customizable supports (graphs, tables, charts, etc.) to visualize the progress in real time.

1.1.5.2 Local control center WiFi in Motion system

The CCL of the Wi-Fi network, installed on a dedicated server, must allow control and configuration and management of the Wi-Fi network from a single centralized point. The features and capabilities of the Network Control Center required are summarized below:

1. Centralized management of initial and subsequent configurations of Wi-Fi access points; the Control Center must have the capacity to manage at least 300 Access Points, also of different vendors.
2. Hierarchical and simplified management of the infrastructure user and device policies and profiles infrastructure (Access Point).
3. Access by the network administrator through a GUI user friendly graphical interface (Graphical User Interface) or Command Line Interface (CLI), based on Web UI, SSH technologies.
4. Centralized firmware update of the Access Points: the Control Center will also have to support the creation of profiles for the various types of system devices in order to send firmware updates for groups of devices or for the entire network. The process of update must report any errors and faults; the equipment must have the possibility to keep the previous firmware version and eventually return to the previous firmware in case of problems with the new firmware version.
5. It should also be possible to schedule the update process, for example in night hours.
6. Management of Quality of Service (QoS) policies on the various WLANs (Wireless LAN) to allow the prioritization of traffic on multiple WLANs, depending on the type of traffic supported (navigation, VoIP, etc.); the QoS of a WLAN will have to support:
   a. WMM (Wi-Fi Multimedia) protocol with WMM Power Save capability;
   b. WMM classification of the wireless client, which will have to include different profiles of the following type on the WLAN:
      - Voice traffic;
      - Video traffic;
      - Normal traffic (best effort);
      - Low Priority traffic.
   c. SpectraLink Voice Priority (SVP) type prioritization
7. Support of the IEEE 802.11k and IEEE 802.11r protocols
8. Support of Multicast Frames to support higher data rates
9. Support for Layer 2 and Layer 3 roaming and for client mobility from an Access Point to another
10. Integrated DHCP server
11. Support of centralized security features:
    a. Integrated Stateful Layer 2-7 Firewall
    d. Support of NAT functionality
    e. Support of IEEE 802.11i protocol
    f. Support of WPA2-CCMP (AES) encryption
    g. Support of WPA2-TKIP encryption
    h. Support of WPA-TKIP encryption

i. Support of the TACACS protocol

12. Support of centralized authentication functionality;
13. IEEE 802.1x/EAP protocols - transport layer security (TLS), tunneled transport layer security (TTLS), protected EAP
14. Support of SNMP v1, 2 and 3 protocols.
15. Integrated server for managing Voice over IP (VoIP) client communications (for future developments).
16. The Control Center will have to include functions and tools for analysis and resolution of the problems (troubleshooting).
17. The troubleshooting tools can be used for discovery, analysis and proactive resolution of problems such as:
    a. Connectivity problems.
    b. Roaming problems.
    c. Insufficient performance.
    d. Security issues or policy violations.

The capture of the data packages to be analyzed can be defined both at the Control Center level and at that of Access Point, both through physical interfaces (Ethernet ports, radio interface) and through the logical interfaces (VLAN, Wireless LAN, etc.). Data can be saved locally or exported via email or FTP and be exported in commonly used formats such as PDF, HTML or Excel/CSV.

Access Points must be able to generate and manage large amounts of log data, which can then be aggregated and sent to the Control Center or managed directly by the Access Points, if there is no connection with the Control Center itself. The capture of the traffic packets for a single wireless client that roams from one access point to another must be distributed among all the Access Points involved in the passage of the packages, whether they are traveling from the wired network to the wireless network or vice versa, with the aim of carrying out the analysis of the behavior of every single client.

The troubleshooting tools should include both historical analysis and reporting. The Control Center must allow the collection of statistical data, to support the historical analysis of the performance, alarms and critical issues found on the system, through customizable reports.

Among the data collected in the historical reports, the following elements should be considered:

Which device has communicated with whom:

- All the associations between Access Point and client;
- Metrics regarding the number of clients.

When a communication has occurred:

- Beginning and end of each association;
- Time detail of the traffic sent.

What has been observed historically:

- All information regarding the status of the devices;
- Indicators of the used data rate, type of traffic, SSID;
- Signal and coverage level, types of encryption and authentication;
- Amount of traffic: number of bytes and frames transmitted and received.
- Alarms and reported alerts, such as:

- Problems on operability and connectivity, association and client status;
- Problems on updating the firmware;
- Hardware faults to the infrastructure;
- Coverage and interference problems;
- Security alarms;
- Capacity problems;
- Roaming problems.

The system must allow a dynamic analysis of data in real time. Visual and customizable tools (graphs, tables, charts, etc.) to view the trend in real time of the monitored parameters will have to be available.

The system will have to support spectral analysis, in the 2.4 and 5 GHz bands. The spectrum analysis of the WiFi network, must allow real-time display of potential sources of RF spectrum interference (Radio Frequency), their identification and classification, through spectrograms and tables. The Spectral analysis tool will have to behave in all respects like a spectrum analyzer.

1.1.5.3 Management and control platform WI Fi V2I system

The platform, installed on a dedicated server, must allow control, configuration and management of the RSU from a single centralized point. The required features and capabilities of the LMS related to the WI Fi V2I system are summarized below:

1. Centralized management of the initial and subsequent configurations of the RSU: the LMS must have the ability to manage at least 100 RSUs also from different suppliers.
2. Access by the network administrator through a user friendly interface of type GUI (Graphical User Interface) or CLI (Command Line Interface), based on Web UI, SSH technologies.
3. Centralized firmware update of the RSU: the LMS must send firmware updates for groups of devices or for the whole network. The update process will have to report any errors and allow the equipment to maintain the previous firmware version and eventually return to the previous firmware in case of problems with the new firmware version. It will also need to be able to make one scheduling of individual update processes.
4. Support of centralized security features:
    a. Firewall with integrated Stateful filtering of packets
    b. Support of the Network Address Translation (NAT) functionality
    c. Support of the IEEE 802.11i protocol
    d. Support of WPA2-CCMP (AES) encryption is.
    e. Support of WPA2-TKIP/MIC encryption
5. The Control Center shall include functions and tools for analysis and resolution of the problems (troubleshooting).
6. The troubleshooting tools can be used for discovery, analysis and proactive resolution of problems such as:
    a. Problems of communication with the RSU.
    b. Insufficient performance.
    c. Security or Policy Violation Alert.
7. Introducing GPS positioning and RSU mapping

The capture of the data packets to be analyzed can be defined both at the LMS and the RSU level, both through the physical interfaces (Ethernet ports, radio interface) and through the logical interfaces (VLAN). The data can be saved locally or exported via email or FTP and be exported to commonly used formats such as PDF, HTML or Excel/CSV. Troubleshooting tools will have to include both historical analysis and reporting. The LMS must allow data collection statistics, to support the historical analysis of the performances, of the alarms and the criticalities found on the system, through customizable reports. Among the data collected in the historical reports the following elements will have to be considered:

Which OBU have communicated:

- All the associations between the RSU and the OBU;
- Metrics regarding the number of OBUs.

When a communication has occurred:

- Beginning and end of each association;
- Time detail of the traffic sent.

What has been observed historically:

- All information regarding the status of the OBUs;
- Indicators of the data rates used;
- Signal level;
- Amount of traffic: number of bytes and frames transmitted and received.
- Alarms and reported alerts, such as:
    - Problems on operability and connectivity, association and client status;
    - Problems on updating the firmware;
    - Coverage and interference problems;
    - Security alarms;
    - Capacity problems;

The system must allow a dynamic analysis of data in real time. Visual and customizable tools (graphs, tables, charts, etc.) to view the trend in real time of the monitored parameters will have to be available.

1.1.5.4 Smart Tunnel Software Platform

The software platform of management and control of the smart tunnel system must be programmed and customized for management and control related to the single Gallery. The software platform will have to be prepared both for communication with the Local Control Center (CCL) of the Smart Road segment to which the Gallery belongs and with the Road Management Tool (RMT) System. The platform must be equipped with all the appropriate software testing certifications provided for by the National, European and International sector regulations. The software platform must be scalable, prepared for tunnels of any length, with single or double arches and must be installed on dedicated management server. The platform must be able to allow the manager to verify the level of safety (dynamic and static risk analysis) of their galleries in real time for emergency management.

The platform must also guarantee the management of the maintenance in a predictive manner according to the actual operating conditions, the current state of the work and the installations installed, with information management in a dedicated database.

1.1.5.5 Software platform for the management of charging stations for electric vehicles

The platform, installed on a personal computer, must be dedicated to management, diagnostics, maintenance and remote assistance of the entire infrastructure consisting of charging stations.

1.1.5.6 Software platform for the management and control of the electrical system of each Smart Road "Module"

The management and control software platform, installed on a dedicated server, will have to carry out the data monitoring and control of each Smart Road module (Green Island), related to:

- Electricity production system;
- Storage System;
- Charging stations;
- Electricity distribution system.

The system must be able to provide information about the status of the electrical and electronic components constituting the aforementioned systems.

The management and control software platform must have the appropriate testing certifications required by the National, European and International regulations. Furthermore, the platform will have to integrate with the RMT Corporate System

1.1.5.7 Software platform for the management and control of video surveillance

The software platform must be able to guarantee the management and control of the two types of cameras planned for the Smart Road:

- *Multi Function Smart Camera*
- *Cameras with smart functionality*

The software platform must allow the management of a number of at least 500 Multi Function Smart Cameras and/or 500 cameras with smart functionality for each Smart Road segment (for a maximum total of 1000 cameras). The software platform must allow, through base software the management of an unlimited number of servers, video recording functionality directly on NAS Storage, signature and encryption of recorded/archived videos, Videowall management, alarm management, availability of SDK for integration with external systems, failover functionality in case of failure on main servers, local/remote video channels management, video analysis based on the service of object tracking, remote management of cameras from remote client, functionality of storage of images received by the camera, access to internal and external database, video search with respect to a time lapse. The software platform must be installed on dedicated management server.

1.1.5.7.1 Software that can be installed on the management platform and on Multi Function Smart Camera

The video surveillance system management software platform, in addition to the basic functions, must be able to be implemented with software designed to manage cameras with smart functionality. This "in addendum" software must also be installed on the Multi Function Smart Cameras.

The "in addendum" software must be able to guarantee the following functions:

- Detect the stationary vehicle in conditions of fluid traffic;
- Detect the stationary vehicle in congested traffic conditions;
- Detect the stationary vehicle due to an accident;
- Detect the congested traffic situation with determination of the queue length (detected by at least two cameras);
- Detect slow vehicles: the system generates an alarm when the speed of a vehicle drops below a certain threshold;
- Detect the presence of pedestrians;
- Detect the moving vehicle in the opposite direction of travel;
- Detect the presence of smoke or reduced visibility;

- Detect the presence of debris on the roadway;
- Detect lane change;
- Intelligent traffic detectors that transmit the following data in real time: speed average [km/h]; traffic volume (number of vehicles per hour) [vehicles /h]; traffic density [Vehicles/km]; lane occupation [%]; vehicle length [m] and classification; Detection on all lanes (including emergency and possible side passages);
- Detection in all environmental conditions (darkness, fog, rain, snow, smoke, cold, heat, etc.);
- Configurability of image encoding/compression mode.
- Automatic detection of the plates of vehicles in transit for all types of EU plates, with possibility of updating, Italian special plates (Police Forces, State Forestry Authority, test plates, temporary plates, etc.);
- Conformity of optical plates reading systems, to UNI 10772 - Class A regulation; Plate detection with accuracy greater than or equal to 95% of the transits;
- Automatic detection of orange ADR hazardous goods panels with decoding of the Kemler and UN Codes;
- The accuracy of the plate reading system relative to the ADR, independently of the number and type of equipment used must be at least 95% of the total transponded ADR vehicles; Search with respect to the license plate number
- Management of the characters of the plates detected partially (sending partial information with associated images for subsequent management on the operator side); Configuration and management of license plate lists (black list);
- Generation for each vehicle that carries dangerous goods or included in blacklist of: infrared/monochrome image, color backdrop image.

1.1.6 Concept Multifunctional station

The Multifunctional Station is designed to be modular and flexible, hosting along its own trunk modules grouped in the following chart according to families: environmental monitoring, security and connectivity.

The function of multi-purpose stations is to host the necessary equipment for the provision of the families of services required by the Smart Road (Environment, Security, Connectivity, Information etc.).

The mandatory services are user and vehicle connectivity and video surveillance with advanced functions, delivered through AP (access points) and cameras, while optional services will be rendered possible through the installation of different equipment (room sensors, information panel, drones, etc.)

The composition of modules for mandatory services and modules for optional services guarantees flexibility and variation in the composition of the multi-purpose station.

FLEXIBILITY

		MANDATORY	OPTIONAL
DRONE SERVICES	3. DRONE		■
ENVIRONMENT	1. GONIOANEMOMETER		■
	2 TACOANEMOMETER		■
	7 ENVIRONMENT SENSORS		■
	8 PLUVIOMETER		■
	9 THERMOIGROMETER		■
SAFETY	6. CAMERA 1	■	
	6. CAMERA 2	■	
CONNECTIVITY	4. ACCESS POINT 1	■	
	5. ACCESS POINT 2	■	
INFORMATION	DATA PANEL		■
LED LIGHTS			■

Figure 20 - Composition of the modules of the multi-purpose station

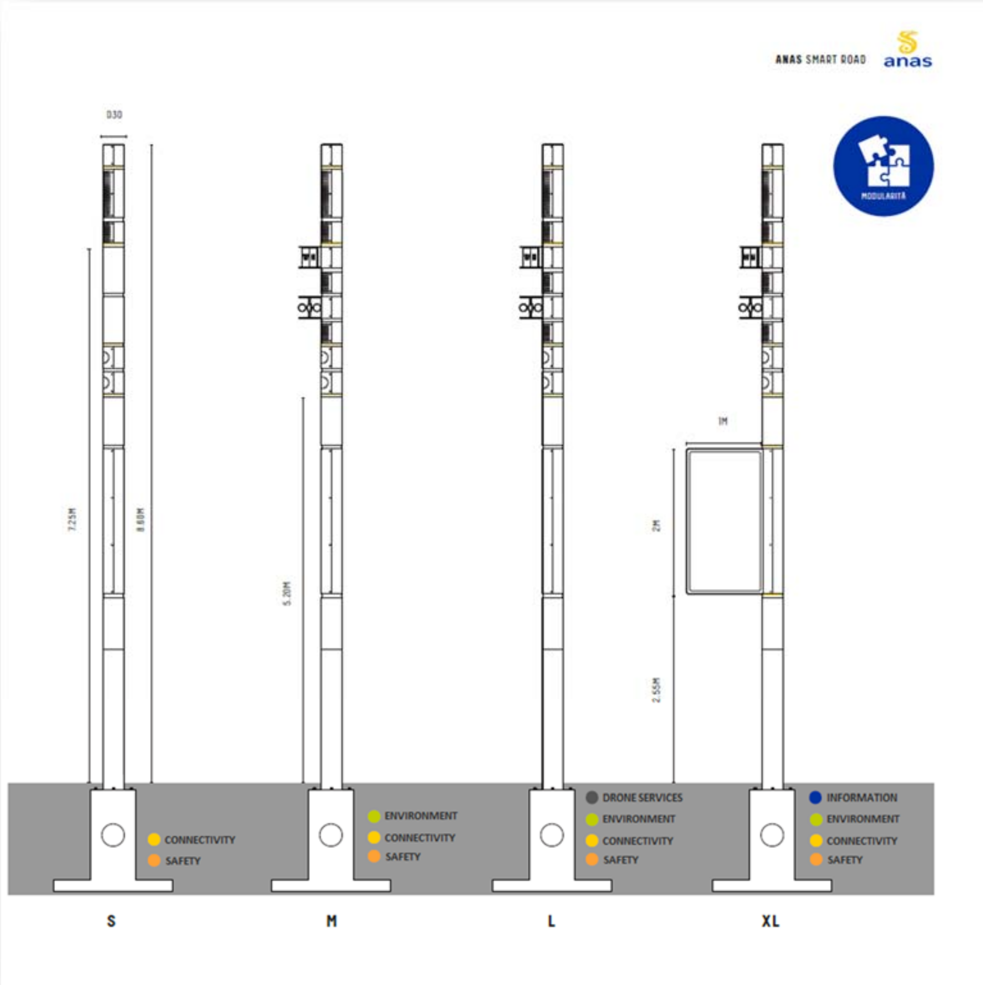


Figure 21 - Types of multi-purpose stations

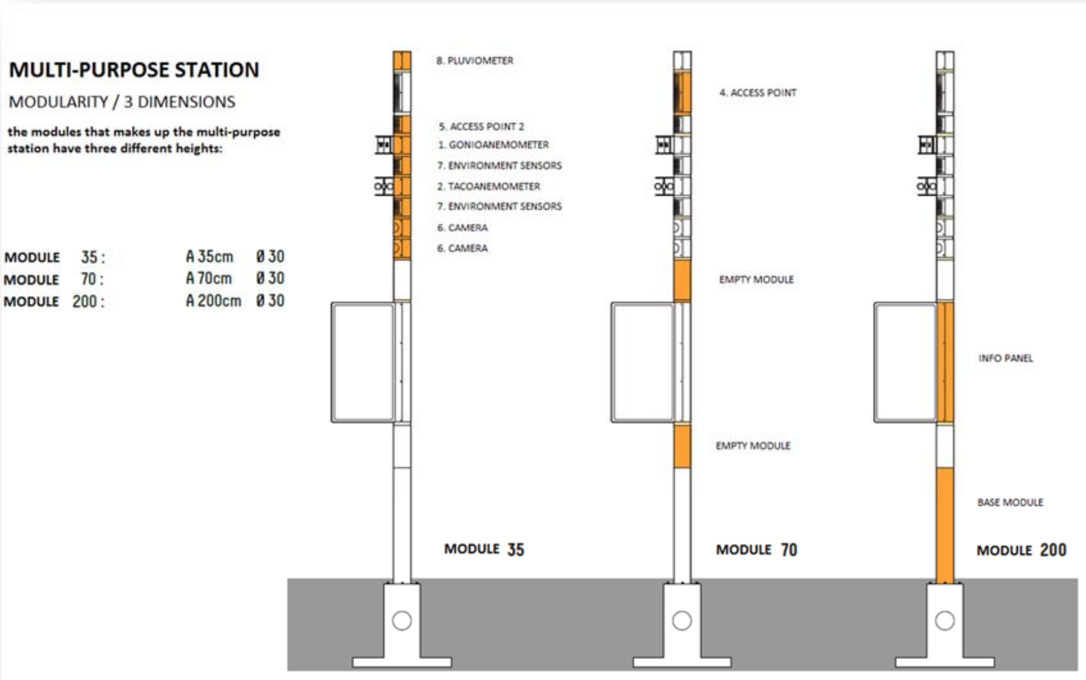


Figure 22 - Dimensions of the modules of the multi-purpose station

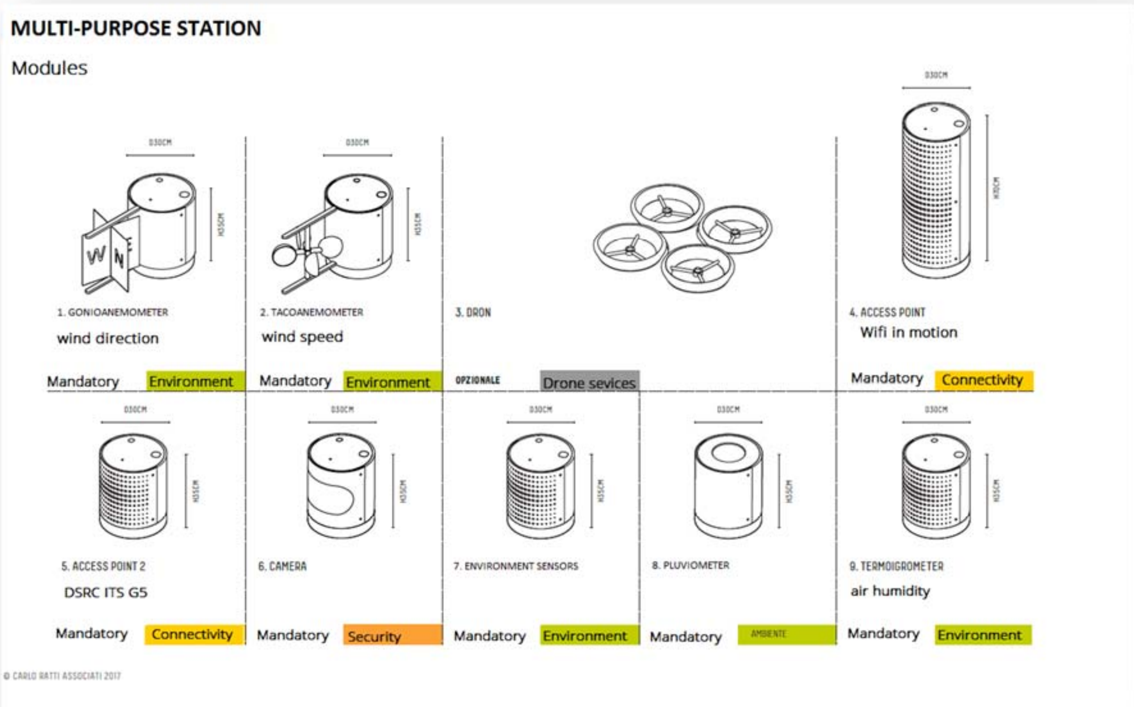


Figure 23 - Multifunctional station, an example of modular elements

The multi-purpose station is composed of:

- a prefabricated concrete plinth with a housing well for distribution components and anchor bolts for anchoring the basic module of the multifunctional station;
- a basic module h 200 with integrated fixing plate;
- a shaft that allows the univocal positioning of the modular elements and the passage of the power and connection cables, connected to the modules through special slots;
- the modular elements stacked along the structural stem and connected together to guarantee the required rigidity;
- the led elements placed to separate the "families" of modules installed on the multifunctional station.

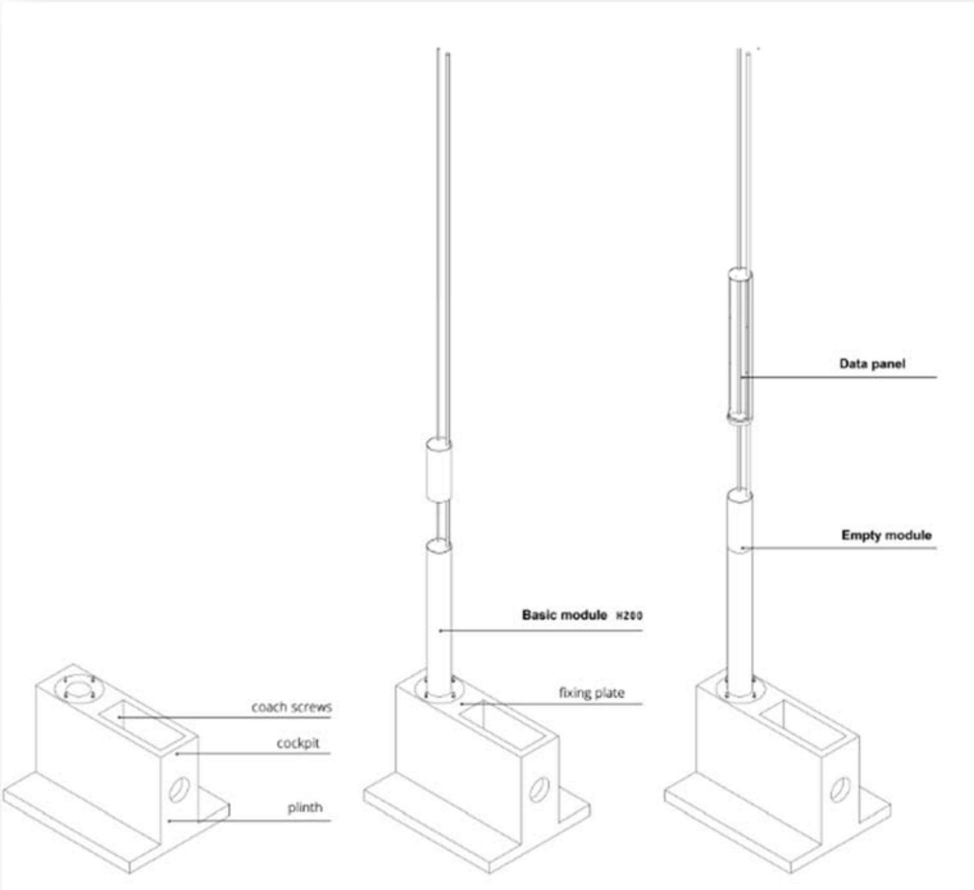


Figure 24 - Constitutive elements of the multifunctional station

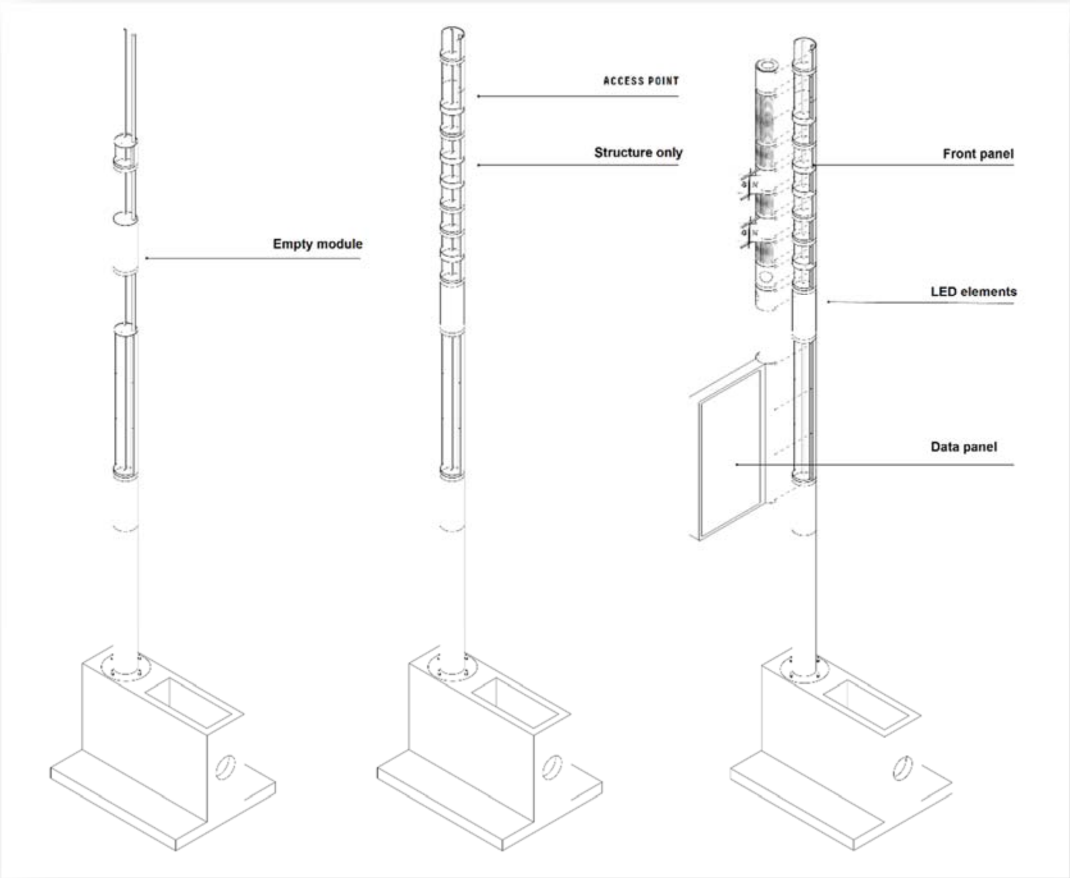
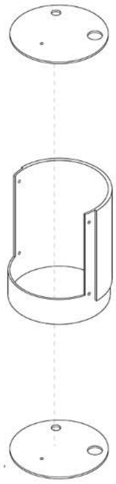


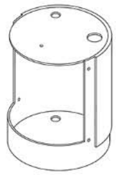
Figure 25 - Constitutive elements of the multifunctional station

MODULAR ELEMENT COMPOSITION



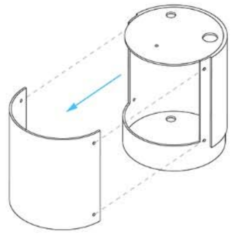
BASIC MODULE

The basic module consists of a cylindrical element and two plates to close the cylinder



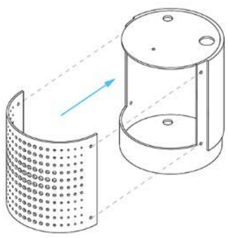
COMPONENTS HOUSING

The module allows the required components to be housed, guaranteeing room for future integrations and/or updates.



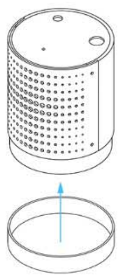
REMOVABLE FRONTAL PANEL

Each module has a removable front panel for inspection of installed components.



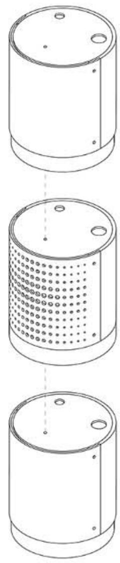
PANNELLO FRONTALE RIMOVIBILE

The panel can be changed and varied as required even after the installation of the multi-functional workstation.



LED LIGHT

A streep led marks the passage between the "families" (drones, environment, safety, connectivity, information) to which the individual modules belong.



MODULES FIXING

In addition to being stacked to form the pole, the modules are attached to each other.

The housing of the modules allows flexibility in the type of components installed.

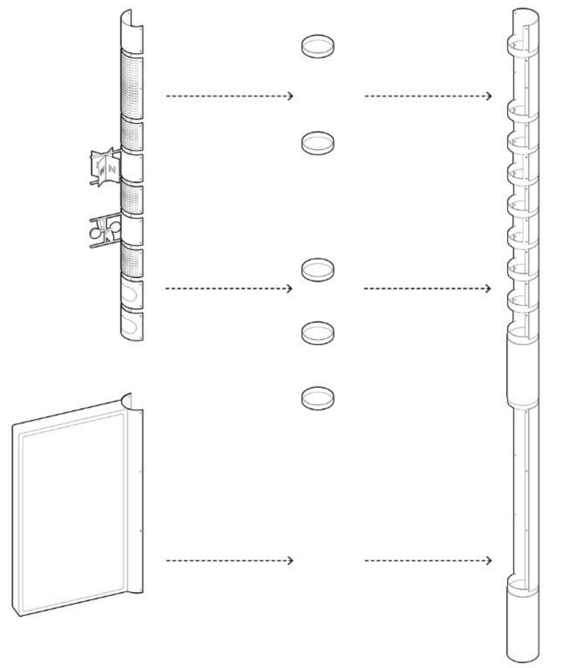
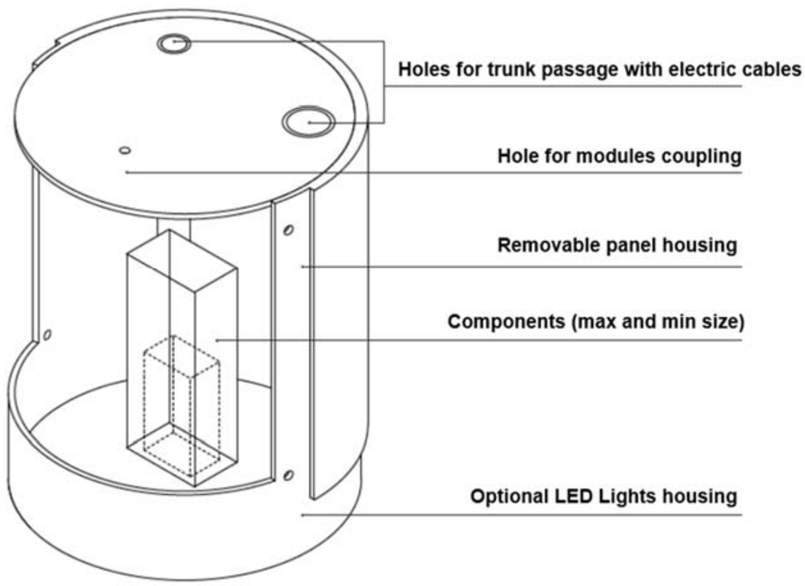


Figure 26 - Schematic representation of a module for a multifunctional station



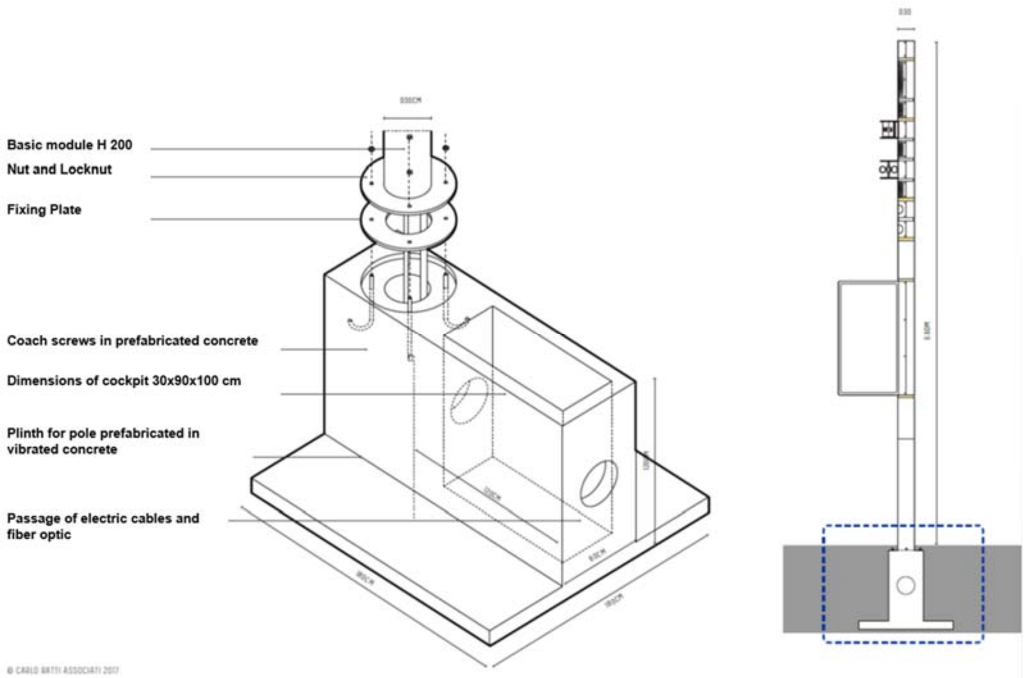


Figure 27 - Plinth and basic module detail

The information panel shows the data monitored by the sensors in real time, for example the level of air pollution, providing detailed and timely information to road users.

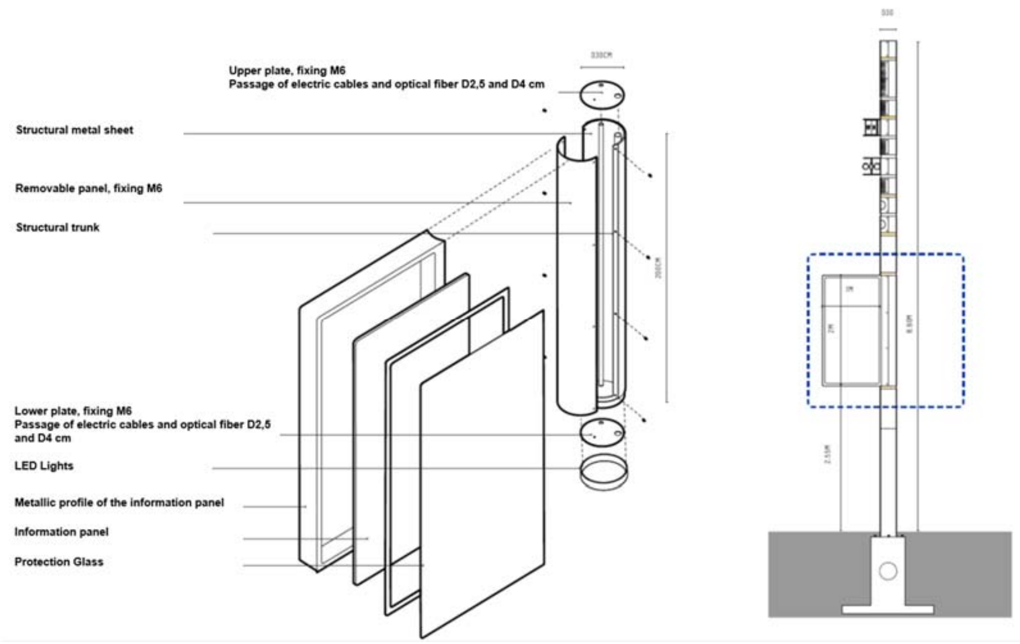


Figure 28 - Information module detail

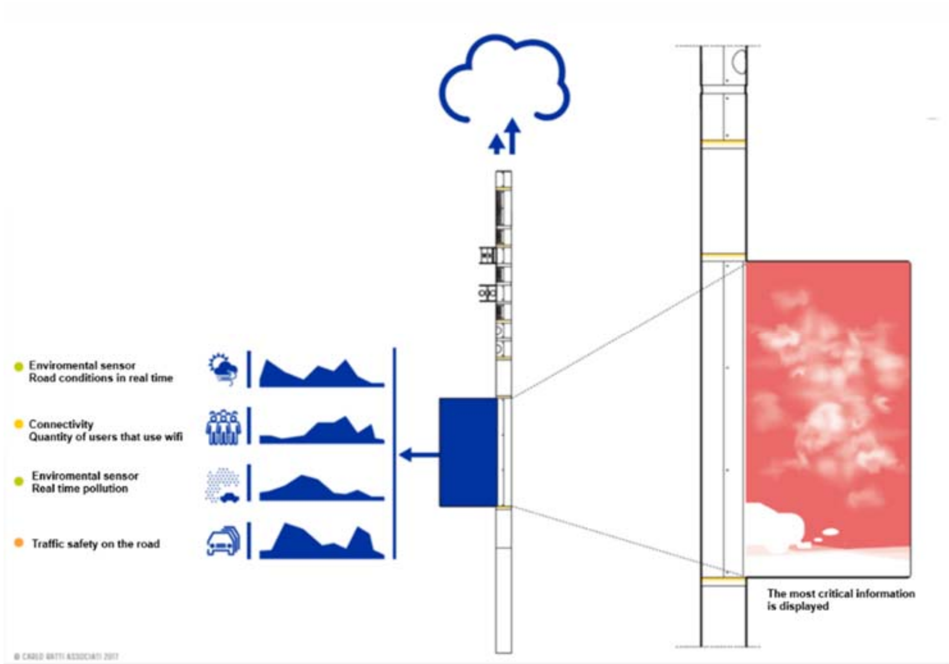


Figure 29 - Transparent data

The type of information shown may vary not only according to the conditions around the multi-purpose station but also based on the position of the multi-purpose station along the route (beginning of the smart road section, intermediate position, end of the smart road section).

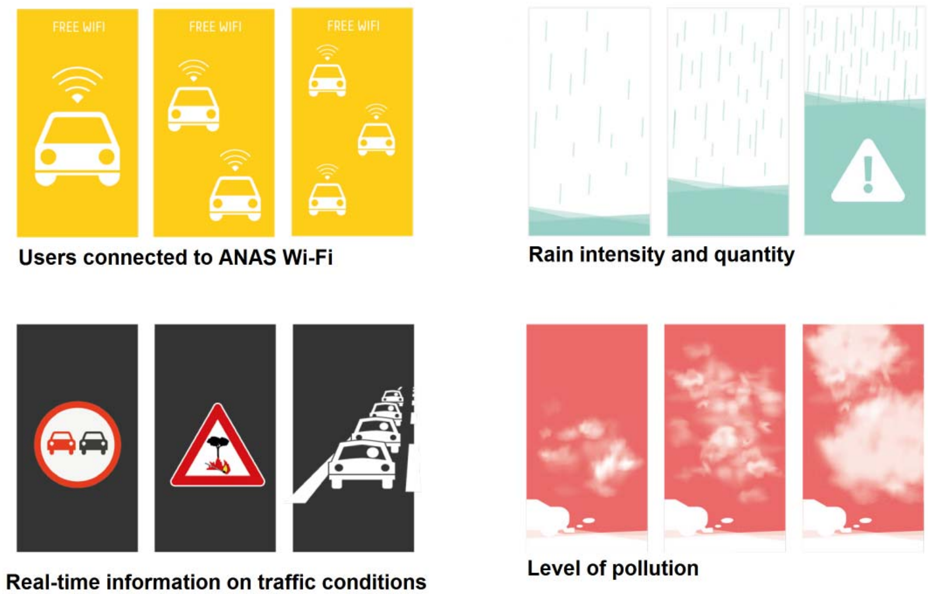


Figure 30 - Example of messaging

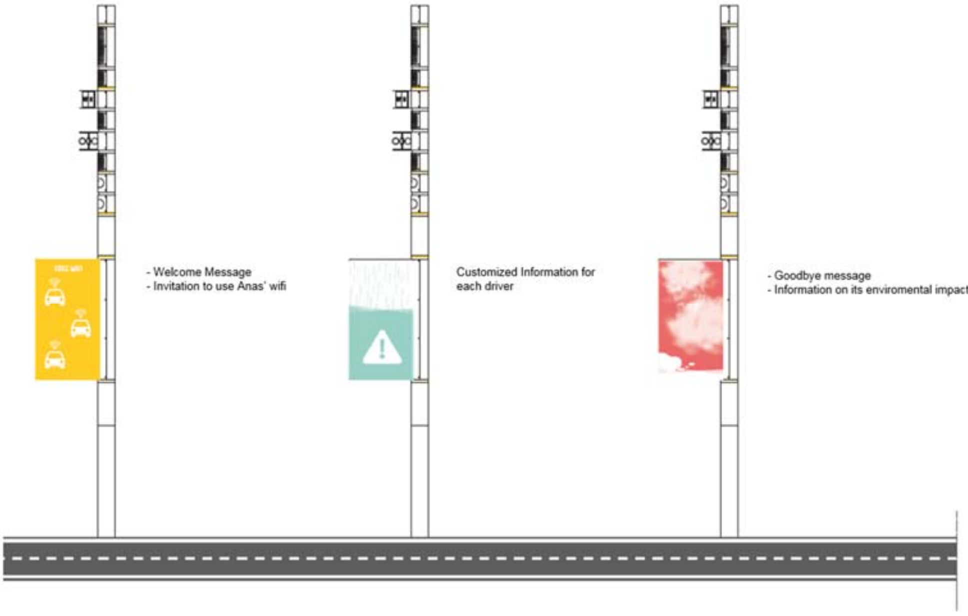


Figure 31 - Example of multifunctional station messaging

Figure 32 - Rendering of a multifunctional station

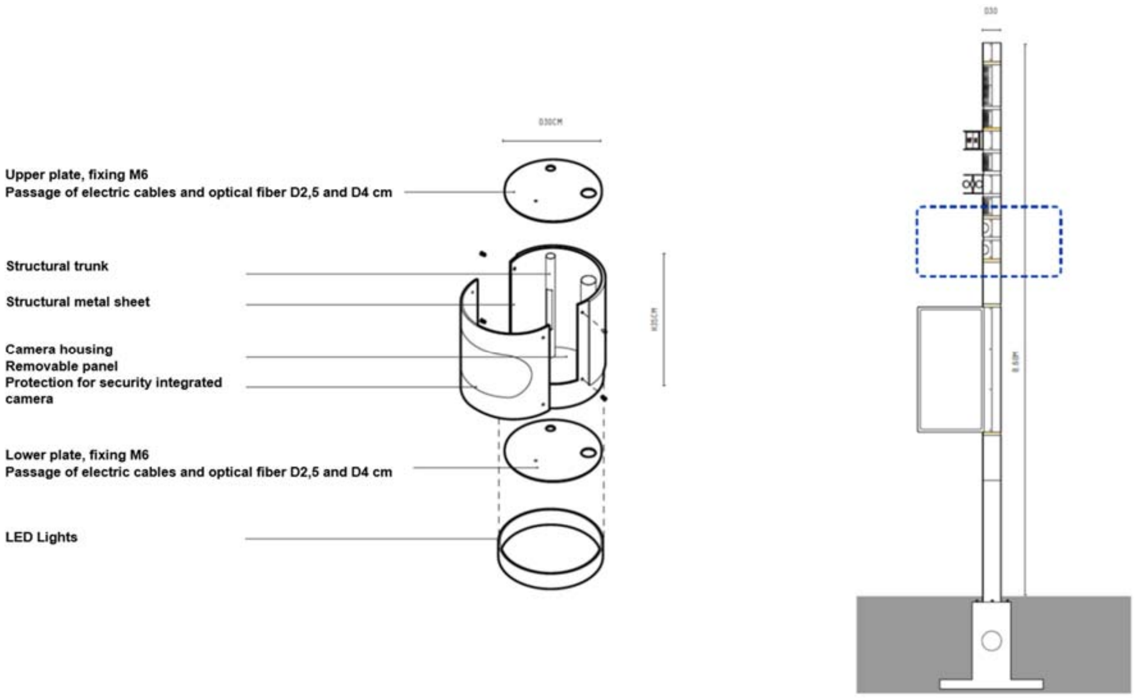


Figure 33 - Camera module detail

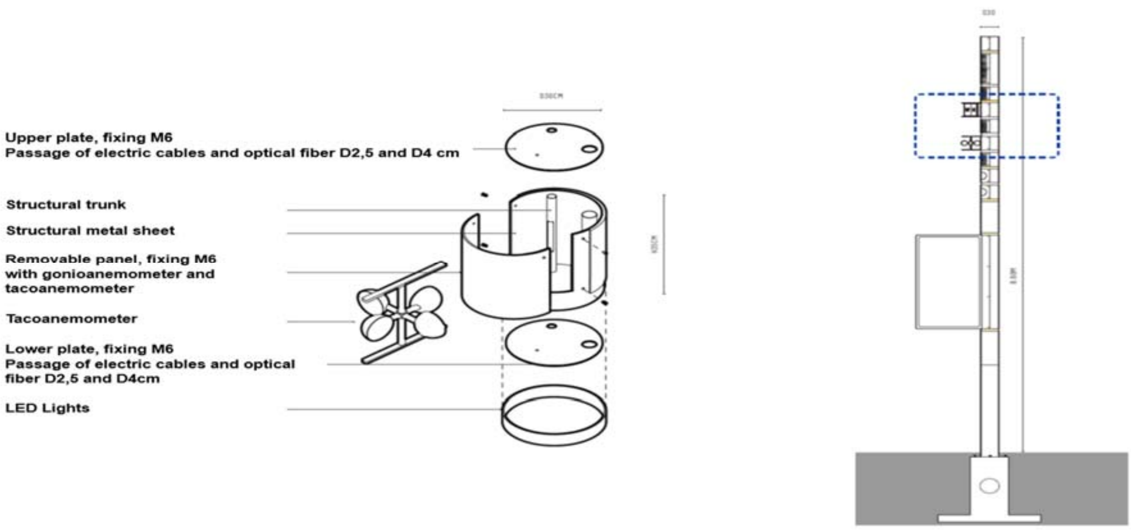


Figure 34 - Tacoanemometer module detail

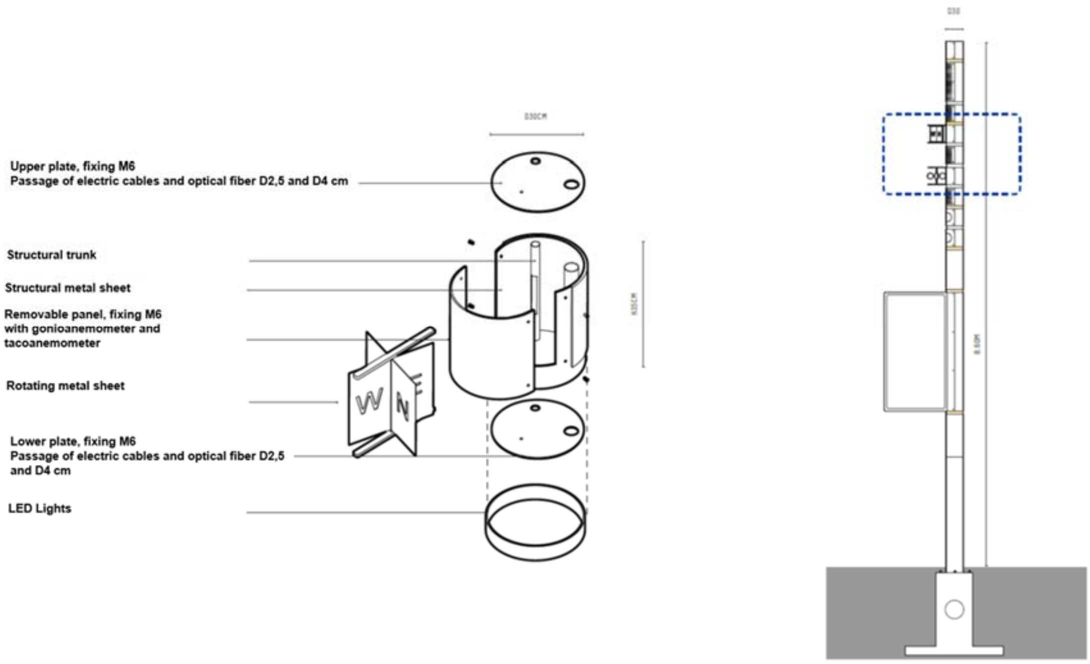


Figure 35 - Tacoanemometer module detail

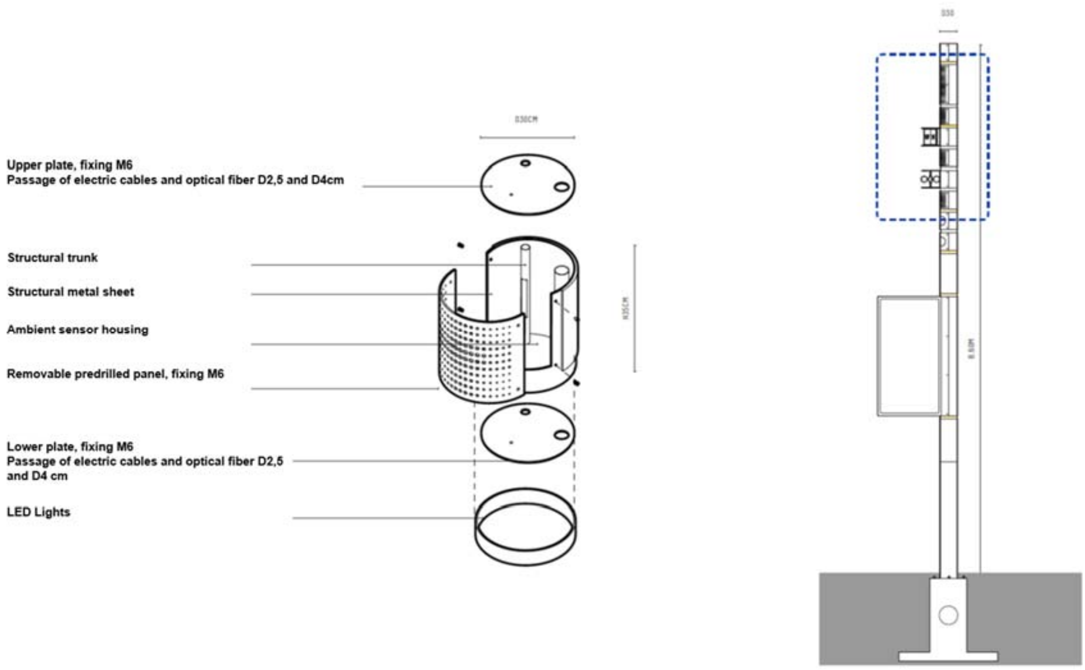


Figure 36 - Environmental sensor module and access point detail

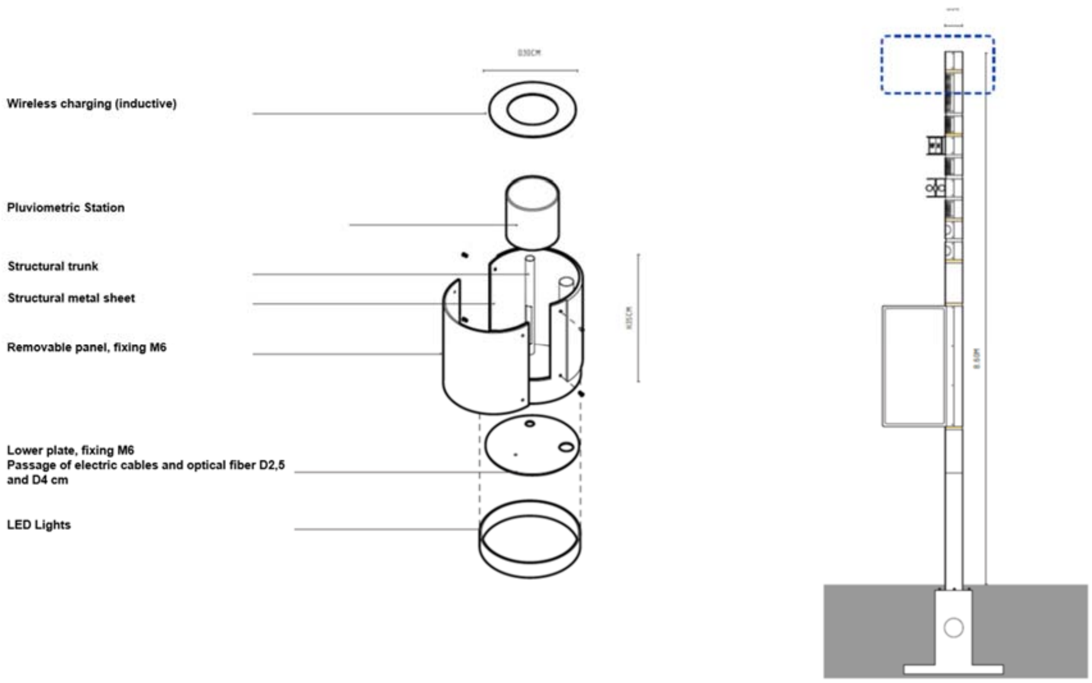


Figure 37 - Top module detail

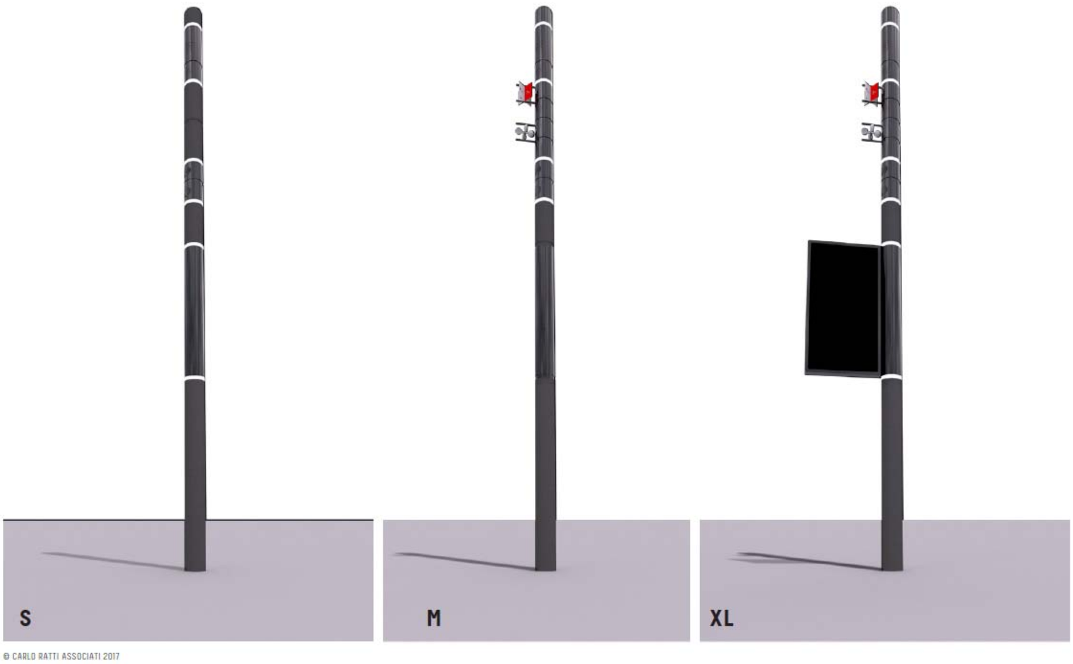


Figure 38 - Rendering of a multifunctional station

Figure 39 - Night view of multifunctional station

1.2 ROAD ANAS NETWORK INTERNET OF THINGS (RANIOT)

The Road Anas Network Internet of Things (RANIoT) is the "IoT" system that Anas wants to integrate into the Smart Road project. With this system, the virtual world of information and communication technologies is closely related to the real world of things, with the purpose of monitoring, checking and transferring information and then carrying out consequent actions.

Within the Smart Road, IoT systems will be used to perform both Structural Health Monitoring (SHM) activities to acquire and transmit information related to the state of the road infrastructure with its major works of art, and monitoring activities of the operating conditions related to the traffic and the transport of goods, as well as environmental conditions.

In particular, quantities related to the following "objects" will be monitored:

- Raod plan;
- Road barriers (Guard Rail, New Jersey and Mobile Barriers);
- Bridges / Viaducts;
- Galleries;
- Unstable slopes;
- Environment;
- Rest areas;
- Construction sites;
- Traffic.

1.2.1 Architecture of the IoT system for monitoring

The infrastructure of the monitoring system is generally made up of the following components:

- IoT sensors;
- Gateways and/or concentrators;
- System controller.

IoT sensors are intelligent devices, generally called "clients", which detect quantities measured and transmit/receive data and information to/from the gateway and/or concentrator.

The gateway is a network device that has the purpose of conveying data packets coming from the field, detected by IoT sensors of different types, and transmit them outside the local network.

The concentrator or HUB is a network device that has the purpose of conveying data packets from the field, detected by IoT sensors of the same type, and transmit them outside the local network.

The system controller is a device that has the ability to collect, store and manage the data coming from each Gateway. Finally, this device must be integrated with the Road Management Tool (RMT) system of Anas, through the STIG system.

The connections between IoT sensors and Gateway and/or concentrator, as shown in the figure, can be of different type and have a different network topology: Star or Mesh.

- *The Star network topology* is typical of LP-WAN networks (with LoRaWan technology) in which all IoT sensors (Clients) are connected to a central node (Gateway). In star topology, direct communication between two sensors is generally not permitted.
- *The Mesh or fully meshed network topology*, typical of protocol-based networks of communication with IEEE 802.15.4 standard, provides that each node sensor (Client), in addition to being connected directly to the Gateway, can also communicate with other nodes.

The connection between IoT sensors and gateways and/or concentrators is provided for data transmission deriving from the field, even with wired systems both through a serial standard communication (CAN-bus, RS-485, RS-232, etc.) for multicast-type fieldbuses and through Powerline systems that exploit data transmission technologies through electric cables. Based on local conditions and to the type of monitoring to be performed, the open EtherCAT standard (Ethernet Control Automation Technology), released as part of the IEC 61158 standard, which represents a high-performance communication protocol for Ethernet deterministic connections, and is born as an extension of the IEEE 802.3 Ethernet standard to data transfer with a predictable timing and exact synchronization can be used.

1.2.2 Types of networks for IoT systems

The networks for IoT systems are realized through the distributed installation of sensors located in correspondence of the "objects" to be monitored.

The use of an IoT monitoring system has the following advantages:

- High reliability of information;
- Low power consumption by IoT sensors;
- Monitoring of infrastructures that are difficult to access; Reduction of costs for cable ducts, excavations and cabling;
- Transmission of information in real time on the status of the infrastructure under monitoring and eventual events and occurrences.
- Security through an adequate level of protection of data transmitted by the devices IoT;

The connection to the Internet IoT sensors allows the exchange, storage, sharing and processing of enormous information flows.

The following summarizes the main requirements of the sensors used in the IoT monitoring system.

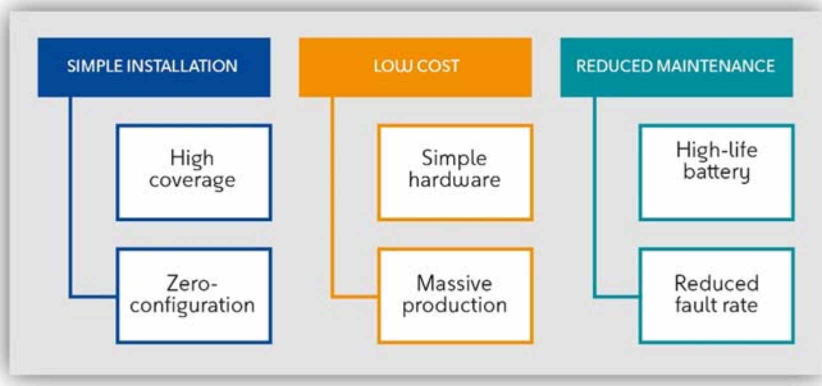


Figure 40 - Sensor requirements in the IoT monitoring system

For the monitoring of longitudinal development infrastructures such as roads, use is expected of sensors with high technological content and low cost, both for the realization of networks distributed in itinere and for local monitoring. These are therefore devices capable of measuring quantities of various kinds (electronic, optical, biological, physical, chemical and mechanical) occupying reduced spaces.

IoT sensors, from the point of view of the power supply, can be powered from the mains electricity or be equipped with a battery. In cases where it is necessary to carry out a monitoring in "continuous" and have a very frequent reading of the measurements detected by the sensor, it must be powered by the mains electricity; instead, in cases where it is sufficient to send/transmit less frequent information, it will be possible prefer sensors equipped with a battery. Therefore, the type of power supply of the IoT sensors is linked to the type of monitoring, as well as the number of daily queries to which the sensor itself is submitted.

From the point of view of connectivity the sensors used can be wired or wireless and will have to be compatible with specific communication technologies (constantly evolving), to be able to send data short or long distance.

In recent years, the panorama of wireless technologies has become increasingly vast and so we had the need to split the wireless communications branch into different groups based on their extension.

As shown in the figure, a classification of wireless networks can be made based on the extension of the coverage area of the transmitted signal.

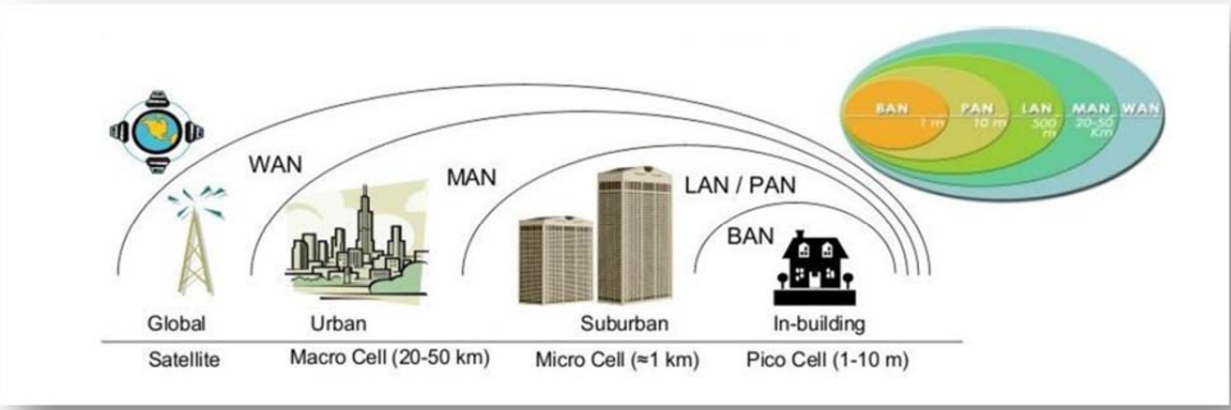


Figure 41 - Classification of wireless networks based on the coverage area

We will then have the following classification of wireless networks:

- WBAN: Wireless Body Area Network, used to connect "wearable" devices,
- WPAN: Wireless Personal Area Network, for connecting devices nearby for the dynamic sharing of information such as laptops, PDAs or tablets and the its maximum communication range is about 10 meters.
- WLAN: Wireless Local Area Network, allows communication between devices far from each other also a few hundred meters and are therefore suitable for interconnections in closed rooms or between adjacent buildings.
- WPAN: Wireless Personal Area Network, for connecting devices nearby for the dynamic sharing of information such as laptops, PDAs or tablets and the its maximum communication range is about 10 meters.
- WMAN: Wireless Metropolitan Area Network, has instead a range of about 10 km, thus providing broadband access to even rather large residential areas.
- WWAN: Wireless Wide Area Network, are macro networks at a much more extensive level that use protocols that allow a range of action even beyond 10 km.

WBAN, WPAN, WLAN belong to the short/medium-range category (Short/Medium Range), while the WMAN and the WWAN belong to the long range category (Long Range).

According to their extension and to the data transmission speed, "Data Rate", there are different communication protocols, as shown in the following figure.

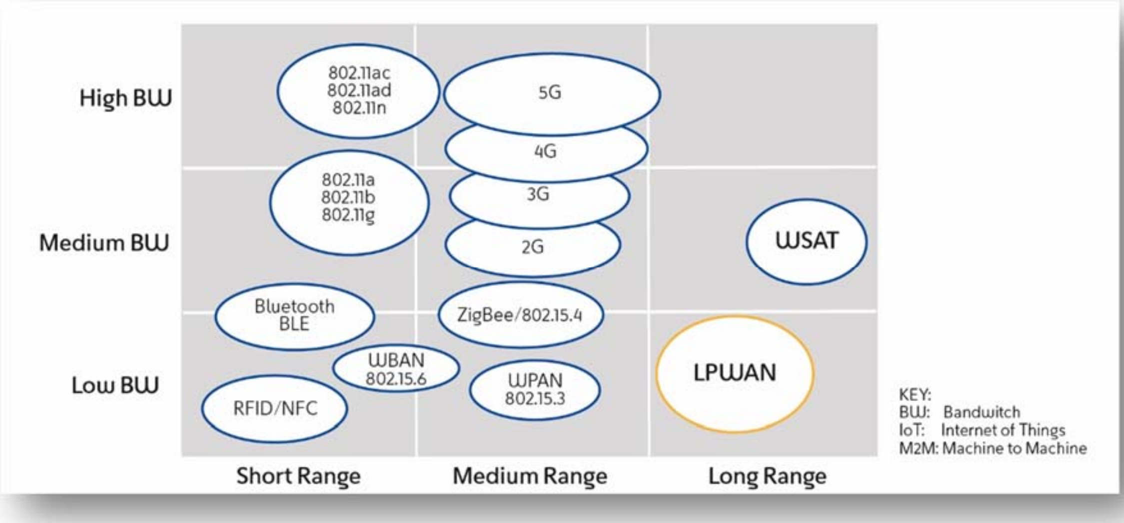


Figure 42 - Coverage capacity according to bandwidth

As described above, the networks are divided into two categories, in relation to the coverage area:

- Short/medium-range networks, with node-node and node-gateway communication capabilities, limited to a few tens of meters, called **"Short Range Networks"** (SRN): part of this category are **LR-WPAN** (**Low Rate Wireless Personal Area Network**) **networks**;
- Long-range networks, with node-gateway communication capabilities extended to some kilometer, called **"Long Range Networks"** (LRN): part of this category are **LP-WAN networks** (**Low Power Wide Area Network**).

The LR-WPAN (Low Rate Wireless Personal Area Network) networks are wireless networks that allow short-distance communications with Bit Rate up to 250 Kbit/s.

LP-WAN (Low Power Wide Area Network) networks are wireless networks that allow long-distance communications with Bit Rate up to 50 Kbit/s.

SRN networks provide higher bandwidth than LRN networks but both types of networks are characterized by low power consumption (Low Power Profile).

The following table shows some examples of the main communication technologies used in the IoT monitoring system, indicating for each the technical characteristics, and distinguishing those that allow short/medium range coverage from those that allow cover longer distances.

Table 4 - Communication protocols for ioT networks

PROTOCOL OF COMMUNICATION	Short Range Network - LR-WPAN			Long Range Network - LP-WAN		
	Bluetooth Low Energy	WiFi	ZigBee	LoRaWAN	SigFox	Weigthless
Range (km/m)	80 m	50 m	100 m/Mesh	2 - 5 km Urban 15 km Suburban 45 km Rural	10 km Urban 50 km Rural	5 km
Frequency band	2.4 GHz	2.4 GHz	868 MHz / 2.4 GHz	Various, Sub-GHz	868 MHz	Sub-GHz
Bidirectional	Yes	Yes	Yes	Yes	No	Yes
Data Rate	1 mbit - 3 mbit	11 mbit - 54 mbit	250 kbps	0.3 - 50 kbps	100 bps	30 kbps - 100 kbps
Amount of Knots	Dozens	Thousand	Thousand	Millions	Millions	Illimitated
Energy Consumption	High	High	Low	Low	Low	Low
Type of insfrastructure	Node-node, Star, Tree	Star, Tree	Node-node, Star, Tree	Star	Star	Star
Standard	Bluetooth 4.0	IEEE 802.11	IEEE 802.15.4	LoRaWAN	No	Weigthless

In the Smart Road project, wireless technology is preferred, to ensure monitoring even of those "objects" that are difficult to access or reach.

Depending on the type of monitoring carried out in the Road Anas Network - Internet of Things (RANIoT), specific for the Smart Road project, LR-WPAN sensor networks can be used, which are based on communication protocols with IEEE 802.15.4 standard, or LP-WAN networks based on protocols of LoRaWAN type communication. Implementation and integration of additional local networks is not excluded, that use other wireless communication technologies, such as Wi-Fi (IEEE 802.11b / g / n) or the future 5G.

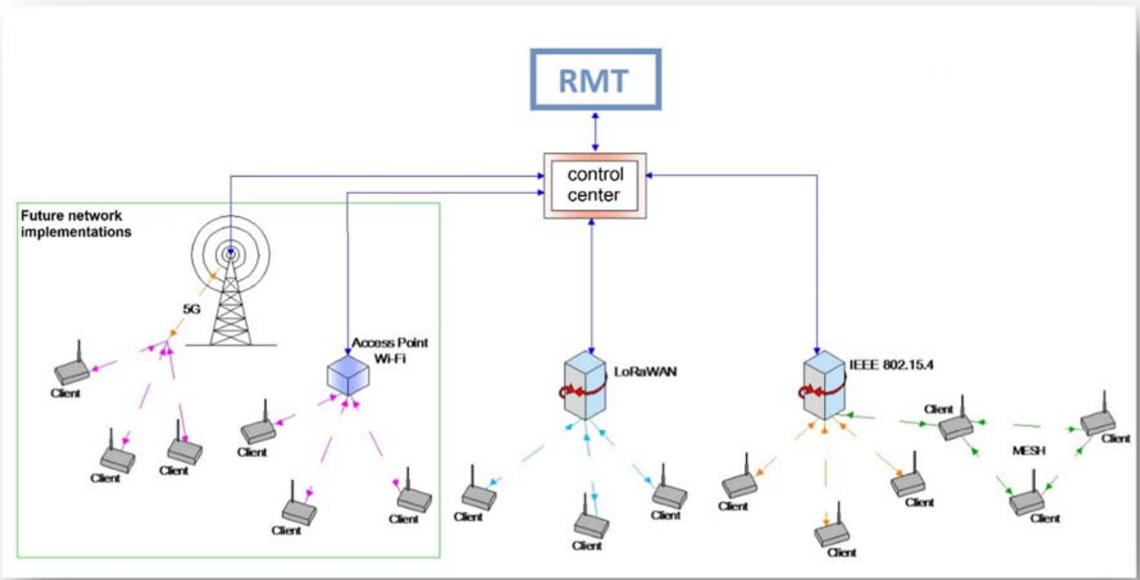


Figure 43 - Typological of Sensor Connectivity (Client) in RANIoT

1.2.2.1 Short Range Network - Low Rate Wireless Personal Area Network (LR-WPAN)

Short Range Networks are networks in which sensors can communicate with each other or with the reference gateway and in which the signal can cover limited distances, about some tens of meters. These types of networks are based on a communication protocol according to the IEEE 802.15.4 standard, characterized by low/medium bit-rate, low power consumption, low costs, use of free frequencies free and high number of sensor nodes.

The IEEE 802.15.4 protocol allows to minimize the time of activity of the radio transmitter so as to reduce energy consumption. Basically this type of protocol communicates with a high number of active nodes of the network (sensors) in static and dynamic conditions, with the ability to remain in a state of inactivity (latency) for a long time without having to talk to the network, implying low consumption in terms of energy.

The topologies of SRN networks are multiple (mesh or star) and the individual devices have a range of coverage between 10-75 m; the greater distances are covered by multihop techniques, jumping from node to node.

In this specific case the SRN networks are divided into:

- C1WSN networks
- C2WSN networks

C1WSN networks allow data transmission through the so-called "multihop" technique (multiple hops) according to which each sensor behaves like a node with the ability to make automatically bounce the information to the nearest node, until it reaches a router positioned near a control center where the received data is processed. If a node is inactive, because for example the batteries are discharged, the network is able to reconfigure and find in any case, a way to let the remaining nodes communicate with each other and thus get information to destination. This type of network guarantees a lower expenditure of energy and greater reliability.

C2WSN networks, on the other hand, use a so-called "single-hop" transmission technique, in which the sensors do not transmit data to the neighboring nodes, but to a node called "wireless router" responsible for sending data from a group of sensors, without any information processing, towards a router near the control center. This type of network is inexpensive in terms of power.

1.2.2.2 Long Range Network - Low Power Wide Area Network (LP-WAN)

The networks that are part of the Long Range Network typology are mainly LPWAN networks (Low Power Wide Area Network), ie long-range transmission and low-power networks, characterized by a reduced data rate and long distance transmission.

This type of network is suitable for carrying out IoT monitoring activities where it is not necessary that the sensors are frequently interrogated, requiring an exchange of a few tens/hundreds of bits and a high long life of the batteries on the sensor edge.

The following figure shows a comparison between LPWAN networks, IEEE 802.15.4 networks and 3G, 4G, 5G networks, in terms of breadth of coverage, energy consumption, bandwidth, latency of transmission and other characteristics and requirements.

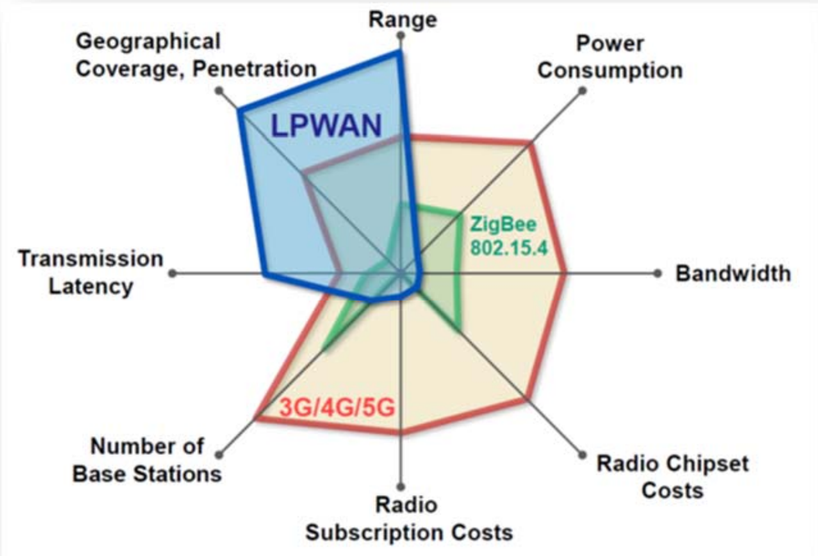


Figure 44 - Comparison between LPWAN and other wireless technologies

LPWAN networks are based on LoRaWAN (Long Range Wide Area Network) communication protocols, a low-power protocol that uses a secure and with large coverage wireless spectrum. LoRaWAN technology is able to connect sensors over long distances, offering at the same time an optimal battery life, requiring minimal infrastructure. This allows to offer advantages such as mobility, security, bi-directionality and improved location/positioning, in addition to lower costs. Sensors with LoRaWAN transmission protocol are able to communicate over distances longer than 40 km in favorable environments, 15 km in semi-rural environments and more than 2 km in urban environments densely populated at a data rate from 300 bits to 100 kbit. This makes them suitable for sending small amounts of data. The sensors also require very little energy and most of them can work for a few years with only one high performance battery.

The topology of a LoRaWAN network provides a star configuration, in which each node (Sensor IoT) is connected to the Gateway. The gateways connect in turn to a Network Server through one connection based on the IP standard, while the final nodes (IoT sensors) use a single-hop wireless communication to one or more gateways. Communication to IoT sensors is in general bidirectional, but it can also support multicast to manage the update or massive distribution of messages in order to reduce communication times.

Depending on the applications, LoRaWAN final devices can be divided into three different functionality classes:

- Class A - devices with lower consumption, with specific timing for the communications. Communications are bidirectional, but received messages can be read only at the end of an outgoing transmission.
- Class B - devices that allow bidirectional communication like those of class A, but which in addition include a random reception window;
- Class C - devices with a slightly higher consumption and which include a window of constantly open reception except during the transmission period.

1.2.3 Monitoring Systems in RANIoT

The set of objects and the relative quantities to be monitored, identifying for each of them the most suitable IoT network type and the corresponding communication protocol, is summarized in the following table, systems not shown here are not excluded:

Table 5 - RANIoT Monitoring

Monitoring "structures"	Variables to be measured	Sensors	Frequency of measurement	Emergency management	Type of IoT network	Communication protocol
Road plan	• Variable surface temperature • Dry • Humid • Wet • Snow • Ice • Residual salt • Temperature • Critical humidity	• TEMPERATURE SENSOR • ASPHALT STATE SENSOR • MICROPHONE ASSOCIATED WITH ACCELEROMETER (for the detection of vibrations and the noise spectrum)	Twice a day, continue in case of reaching the attention threshold	Automatic alarm in case the criticality threshold is reached	LP-WAN/ WIRED	LoRaWAN/CAN-bus/RS-485/RS-232/EtherCAT
Road Barriers (Guard Rail, New Jersey and mobile barriers)	• Vibrations • Vehicle distance • Generalized movements	• ACCELEROMETER • ULTRASONIC PROXIMITY SENSOR • MICROPHONE ASSOCIATED WITH ACCELEROMETER (for the detection of vibrations and the noise spectrum)	Twice a day, continue in case of reaching the attention threshold	Automatic alarm in case the criticality threshold is reached	LP-WAN/ WIRED	LoRaWAN/CAN-bus/RS-485/RS-232/EtherCAT
Bridges/viaducts: decks	• Vibrations • Inclination generalized movements • Local deformation states • Pressure	• ACCELEROMETER • INCLINOMETER • CRACK GAUGE • PRESSURE CELL • STRAIN GAUGE	Twice a day, continue in case of reaching the attention threshold	Automatic alarm in case the criticality threshold is reached	LR-PWAN / LP-WAN/ WIRED	IEEE 802.15.4 / LoRaWAN/CAN-bus/RS-485/RS-232/EtherCAT
Bridges/ viaducts: piles and shoulders	• Generalized movements • Local deformation states	• ACCELEROMETER • INCLINOMETER	Twice a day, continue in case of reaching the attention threshold	Automatic alarm in case the criticality threshold is reached	LR-PWAN / LP-WAN/ WIRED	IEEE 802.15.4 / LoRaWAN/CAN-bus/RS-485/RS-232/EtherCAT
Galleries	• Relative displacement between two points • Local deformation states • Pressure • Generalized movements	• ELECTRIC CRACK GAUGE • INCLINOMETER • STRAIN GAUGE • PRESSURE CELL • TERRESTRIAL INTERFEROMETER	Twice a day, continue in case of reaching the attention threshold	Automatic alarm in case the criticality threshold is reached	LR-PWAN / LP-WAN/ WIRED	IEEE 802.15.4 / LoRaWAN//CAN-bus/RS-485/RS-232/EtherCAT
Unstable slopes	• Abnormal movements • Vertical failures • Groundwater level	• INCLINOMETER • MAGNETIC ASSESTIMETER • ELECTRICAL PIEZOMETER	Twice a day, continue in case of reaching the attention threshold	Automatic alarm in case the criticality threshold is reached	LR-PWAN / LP-WAN/WIRED	IEEE 802.15.4 / LoRaWAN//CAN-bus/RS-485/RS-232/EtherCAT
Environment	• Noise levels, • CO, CO_2, NO, NO_2 • Particulate temperature, humidity and air pressure • Brightness	• SENSOR FOR NOISE CONTROL • SENSOR FOR MEASURING AIR QUALITY • WEATHER STATION • BRIGHTNESS SENSOR	Twice a day, continue in case of reaching the attention threshold	Automatic alarm in case the criticality threshold is reached	LR-PWAN / LP-WAN/WIRED	IEEE 802.15.4 / LoRaWAN

Monitoring "structures"	Variables to be measured	Sensors	Frequency of measurement	Emergency management	Type of IoT network	Communication protocol
Rest areas	Vehicle presence	• SMART PACKING SENSOR	Twice a day, continue in case of reaching the attention threshold	Automatic alarm in case the criticality threshold is reached	LR-PWAN / LP-WAN/WIRED	IEEE 802.15.4 / LoRaWAN
Construction sites	Geolocation of the beginning, end and width of construction site	• SMART TRACER ROAD WORK	Twice a day, continue in case of reaching the attention threshold	Automatic alarm in case the criticality threshold is reached	LR-PWAN / LP-WAN /WLAN/ WIRED	IEEE 802.15.4 / IEEE 802.11/LoRaWAN
Traffic	• Traffic data • Dangerous events • Critical situations on the road • Reading and recognition of plates	• MULTI-FUNCTION SMART CAMERA	Twice a day, continue in case of reaching the attention threshold	Automatic alarm in case the criticality threshold is reached	RETE WIRED IP/MPLS	
Support walls	Generalized movements	• INCLINOMETER	Twice a day, continue in case of reaching the attention threshold	Automatic alarm in case the criticality threshold is reached	LR-PWAN / LP-WAN /WLAN/ WIRED	IEEE 802.15.4 / LoRaWAN//CAN-bus/RS-485/RS-232/EtherCAT
Foundations in the riverbed	• Scaling with combined measurement of local deformation states • Generalized movements • vibrations	• INCLINOMETER	Twice a day, continue in case of reaching the attention threshold	Automatic alarm in case the criticality threshold is reached	LR-PWAN / LP-WAN /WLAN/ WIRED	IEEE 802.15.4 / LoRaWAN//CAN-bus/RS-485/RS-232/EtherCAT

1.2.4 Infrastructure Monitoring System

During the life of an infrastructure, it is necessary to check that it maintains margins of safety with respect to the minimum regulatory requirements, because actions of an anthropic and/or environmental nature, progressively reduce the resistance of structures, such as fatigue phenomena.

Through a real time check and monitoring of the state of the infrastructures and of the structures, it will be possible to obtain an optimization of preventive and/or corrective maintenance interventions and at the same time it will be possible to have a clear picture in case of disasters, useful for the intervention management.

The main IoT sensors, used in the context of infrastructure monitoring, together with their own features, are listed below.

The **electric crack gauge** is a widely used sensor for continuous monitoring of bridges, viaducts, as well as fractures in rock masses. The device consists of a displacement sensor of potentientomentric type able to detect changes in position between two points on either side of one crack or a joint. The sensor must be interfaceable with any wireless datalogger for data transfer.

The strain gauge is a sensor that allows continuous measurement of deformations and displacements of road infrastructures such as bridges, viaducts and tunnels. The device must be connected to an electric transducer that transforms every mechanical movement into an electric signal variation with standard output 4 ÷ 20mA, in voltage or digital RS485. The device must be interfaceable with any wireless datalogger.

The ULP triaxial wireless accelerometer (Ultra Low Power) is a measuring instrument capable of detect and/or measure acceleration, by calculating the force measured with respect to the mass of the object (strength per unit of mass). The sensor is suitable for continuous monitoring of road infrastructures such as bridges, viaducts or even for the monitoring of road barriers. The device is equipped with radio transmission with omnidirectional antennas with maximum wireless range of about 200m.

The mono, biaxial or triaxial wireless inclinometer is a tool that measures the angle that the joining observer-point observed forms with the horizontal. It consists of a needle hinged which can move on a vertical plane, positioning itself according to the vertical by effect of gravity. The sensor is suitable for continuous monitoring of road infrastructures such as bridges and viaducts. The device is equipped with radio transmission with omnidirectional antennas with range maximum wireless of about 200m.

The magnetic assestimeter is a tool that measures the extent of the settlements and settling of the ground, more generally, changes in the distance between two or more points along a common vertical axis. The device is equipped with an axial column with a series of measuring points (magnetic rings) whose position, detected by means of a reading probe, allows to know the lowerings relative to each section between two rings and the total lowering with respect to a point of reference. The device must be connected to a transducer that outputs an electric signal with standard output 4 ÷ 20mA, in voltage or digital RS485 and must be interfaced with any wireless datalogger.

The PT100 temperature sensor is a sensor that measures the temperature of the road surface. The sensor must be able to supply an output signal 0 ÷ 2Vdc, 4 ÷ 20mA, or digital RS485 and must be interfaceable with any wireless datalogger.

The asphalt sensor is a sensor that measures the main physical-chemical characteristics of the road surface. It allows to know the status of the road and then start cleaning or prevention actions against ice formation or accumulation of snow/hail. The transducer must be able to acquire various types of information thus allowing to have in addition to temperature, also the state of the road surface distinguishing between dry, humid, wet, ice, snow, residual salt, also allowing a critical humidity assessment.

The pressure cell is a sensor for detecting local pressures within a mass of ground and for controlling pressures acting on the contact between a support work and a pushing ground. The device must be able to measure the overloads induced by works of foundation and pressures to contact between support works and the terrain. The device must be connected to an electric transducer that transforms every variation of pressure into a variation of electric signal with 4 ÷ 20mA standard output, in voltage or digital RS485. The device must be interfaceable with any wireless data logger.

The tensile load cell is a sensor for the continuous measurement of the tension of the wire ropes which constitute the rockfall networks. The device must be connected to a transducer that provides output of an electrical signal with standard output 4 ÷ 20mA, in voltage or digital RS485 and must be interfaceable with any wireless data logger.

The electric piezometer equipped with a relative pressure transducer, allows to determine the piezometric height measuring the hydrostatic pressure acting on the immersed sensor and then determining the water level. The device must be connected to a transducer that outputs an output electric signal with 4 ÷ 20mA standard output, in voltage or digital RS485 and must be interfaced with any wireless datalogger.

The terrestrial interferometer is a radar technology sensor that allows detection from a location remote the field of displacements of the land through the production of geo-referenced and multitemporal images, which allow to follow in detail the spatial and temporal evolution of the deformation framework. The device must be interfaceable with any wireless data logger.

The liquid level sensor is able to measure the level of liquids. The sensor must be made up from a container and a floating object.

The ultrasonic proximity sensor, for signaling the exceeding of the minimum distance of safety from the road barrier.

For the monitoring of the infrastructure must be provided a specific software that implements an algorithm dedicated to the processing of data collected by the sensors listed above and automatic identification of structure anomalies (significant deformations and cracks, presence of damage due to deterioration of materials and/or accidental actions), both in terms of the location of the damage and of the estimate of its size.

The processing and analysis of the measurements must be conducted by technicians with specific expertise in the field of civil engineering. A technician in charge of structural monitoring must issue a report on the state of the structure and on the possible necessity and urgency of repair interventions. In any case, the system performs a first automatic check by means of the definition of alarm thresholds, which must be defined by the technicians who designed the monitoring, depending on the structural model, the number of sensors, the safety thresholds, etc.

The exceeding of the alarm thresholds must be analyzed by a technician who must issue a report on possible causes and proactively foresee possible interventions that can include:

- Further surveys on the structure;
- Intensification of monitoring frequency;
- Proposals for intervention.

There must also be an automatic alarm system, provided with the necessary redundancies and safeguards to reduce the possibility of false alarms to warn infrastructure managers and the Security Authorities in case the system should detect significant anomalies in the safety of the monitored structure.

The analysis coming from the structural monitoring allows the manager to develop plans for maintenance associated with risk levels and urgent intervention needs, optimizing the resources available for the maintenance of the structures.

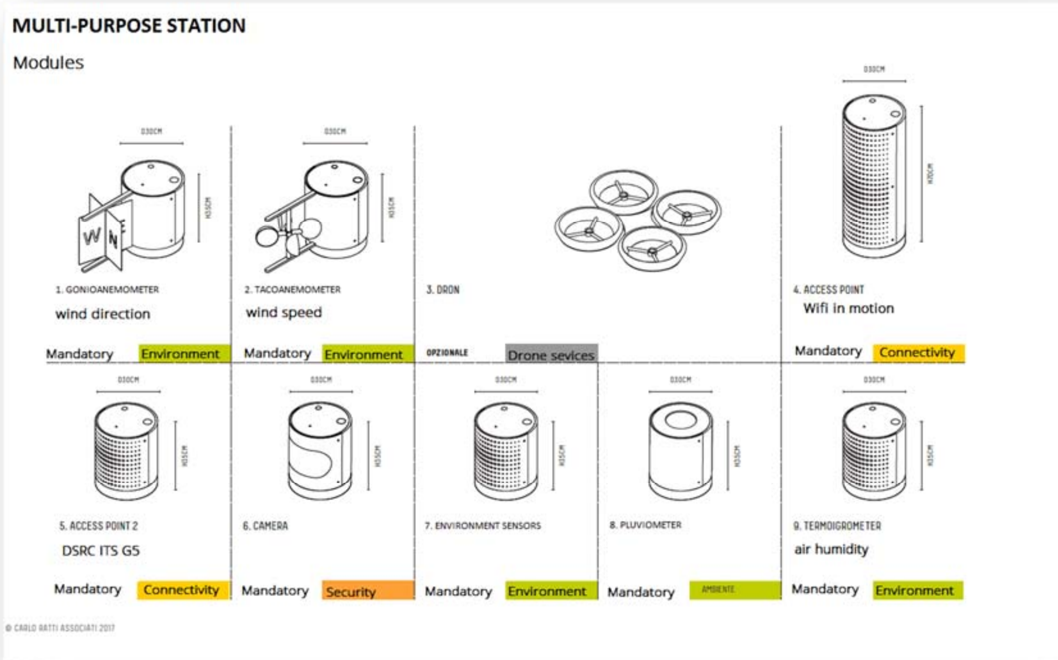


Figure 45 - Example of monitoring sensors modules

1.2.4.1 Monitoring of the viable surface

The monitoring of the viable surface is aimed at the measurement and control of the main physico-chemical characteristics of the road surface and allows to know the state of the surface in real time, with the aim of initiating maintenance and prevention actions, for example against the formation of ice or the accumulation of snow/hail.

Along the road infrastructure, the following sensors will be installed in a distributed manner:

- **Temperature sensor;**
- **Asphalt state sensor.**

The first will provide information on the temperature of the road surface, in order to signal the possible ice formation. The state of the road surface (dry / wet / snowy / icy), instead, can be controlled by an asphalt state sensor.

1.2.4.2 Monitoring of safety barriers

The Smart Road project foresees the possibility of implementing a sensor system positioned on the road barriers, fixed and mobile, able to detect the deformation and the break or the damage to the barrier and the approach of vehicles to the barrier itself. These devices will be able to send an alarm signal to operators and to the Operating Room of Anas if an incidental event occurs.

For this purpose, the development of the following functional features within the barriers has been envisaged:

- Real-time communication of any damage or breakage of the road barrier following the impact of a motorized vehicle, with georeferencing of the event (roadway, direction and kilometric);

- Signaling of dangerous approach of motorized vehicles to the road barrier through an alarm signal communicated to the user.

The main sensors used to monitor security barriers are the following:

- **Shock accelerometer**, for the measurement of acceleration and vibration deriving from collisions to barriers;
- **Ultrasonic proximity sensor**, for signaling that the minimum safety distance from the barrier is exceeded.

Acceleration sensors for traffic safety will be placed directly on the anchoring plates of barriers. The impact detection system performs an acceleration measurement converting the three voltage outputs provided by the triaxial accelerometer into digital. The microcontroller processes the acceleration module and compares it with a threshold value, which if exceeded, activates the alert status, a data processing system that allows the location of the impact between two adjacent sensors must also be provided.

The distance between the vehicle and the barrier, on the other hand, is obtained by measuring the time necessary for the ultrasound wave to be reflected on the vehicle and to return to the sensor placed on the barrier. If this distance is less than a threshold value, variable according to the road category, the alarm system is activated and the hands-free communication sent to the mobile device of the road user. A future application will be a communication system between approach sensors and the system-equipped car

DSRC, which will cause an automatic removal of the vehicle from the road barrier, avoiding so the escape from the roadway and any accidents.

1.2.4.3 Monitoring of bridges and viaducts

The structural monitoring carried out during the operational phase is an essential activity for durability and safeguarding of infrastructures such as bridges and viaducts, which must perform their function for tens of years.

In the case of older, rather outdated structures, monitoring is used to assess the structural conditions and the integrity of the structure itself. Furthermore, it allows to keep an eye on any degradation phenomena that can develop as a result of catastrophic events or during the life of the structure. Their understanding and evaluation can be a valid help in the correct definition of maintenance and restoration interventions.

Monitoring may involve the structural elements that make up the bridge or viaduct or the subsoil affected by the foundations of the structure. The most monitored items are:

- The beams that make up the bridge deck;
- The piles and shoulders of the bridge;
- Foundations.

The IoT sensors used are:

- **Cracks or strain gages**, for the measurement of the deformations of the beams of the decks and of the pulvinos, movements of the joints or fatigue phenomena of the structure;
- **Triaxial accelerometers**, to measure the vibrations of the structure subject to vehicles traffic;
- **Biaxial or triaxial inclinometers** to monitor battery inclinations and rotations;
- **Assestimeters**, for the monitoring of subsidence or differential displacements of the foundations;
- **Temperature sensors** for measuring the temperature of the asphalt;

- **Pressure cells**, for measuring pressures acting on contact between a work of support and a pushing ground;
- **Inclinometers** for the control of the sliding movements of the land;
- **Piezometers**, for monitoring the groundwater.

1.2.4.4 Monitoring in the tunnel

Safety and management of existing tunnels require continuous monitoring above all of the critical sections or of some already deteriorated areas, with the purpose to know correctly the behavior over time of this particular structure.

Diagnostic tools allow identification and location of potential anomalies, damages present in the tunnel structure and are able to generate alarms in the in case of pre-set thresholds.

The sensors to be used for the structural monitoring of the tunnel lining are the following:

- **Accelerometers**, for the measurement of vibrations and subsidence of the final coating of the gallery;
- **Temperature sensor**, to monitor the temperature of the tunnel lining;
- **Strain gauges and/or crack gauges**, for monitoring horizontal and vertical movements and convergence;
- **Pressure cells**, for calculating the stresses and local pressures acting on contact between a work and the pushing ground.

In recent tunnels, sensors and technological systems are already present, as expected from safety regulations in the tunnel, which in turn are connected to PLC and to the SCADA system of gallery. This sensor measures and monitors the operating status of the systems present, the traffic conditions and tunnel traffic conditions, temperature inside the tunnel, air speed, as well as the conditions of visibility and air pollution.

Currently Anas is equipped with a Road Management Tool (RMT) central system, integrated with the Telecontrol System (STIG), which in turn will be fully integrated into the "Smart Road" system.

1.2.4.5 Monitoring of unstable slopes

To monitor the stability of a slope correctly, it is necessary to have as much data as possible to make a continuous observation over time of the potential failure phenomenon.

The main parameters to be monitored are shown in the following list:

- Surface displacements;
- Deformative state of the ground along a vertical;
- Depth and shape of the surface of the landslide movement;
- Space-time collocation of any movements in progress;
- Hydrogeological aspects of the site;
- Hydraulic regime and its possible variations.

The most suitable sensors for monitoring the parameters listed above are:

- **Terrestrial interferometer**;
- **Inclinometers**;
- **Piezometers**.

1.2.5 Traffic and Freight Monitoring System

The Smart Road provides a set of systems for real-time monitoring of traffic conditions and freight transport, such as:

The Multi-function Smart Camera performs the activity of "intelligent" video surveillance, detecting the dangerous events on the road, traffic data, plate reading function, the presence of fog, the distance of visibility.

The Weigh in Motion System allows constant monitoring of the weight of each vehicle which travels on the road by means of weighing sensors installed in the road surface. The control system allows the remote and automatic access control and management activity to the junctions along the highway, through the installation of automatic vehicle barriers.

The Truck Parking system in heavy truck parking areas allows reservations for parking stalls through a dedicated service, ensuring a continuous monitoring of goods, for a stop in full security.

The Smart Tracer Road Work is a device that allows to report and geolocalize the presence of a road construction site and that has GPS, Wi-Fi and GSM modem, battery and LED for the reporting of the start and end point of the construction site..

1.2.5.1 Multi-function Smart Camera

The Multi-function Smart Camera system will be inserted into the Smart Road infrastructure via the installation of devices that will carry out the activity of "intelligent" video surveillance, noting the dangerous events, critical road situations, traffic data, reading and recognition of plates, etc.

The Multi-function Smart Camera will be managed and controlled by a specialized software that will allow to have the following features:

- Detect the stationary vehicle in conditions of fluid traffic;
- Detect the stationary vehicle in congested traffic conditions;
- Detect the stationary vehicle due to an accident;
- Detect the congested traffic situation with determination of the length of the queue; Detect slow vehicles and generate an alarm when the speed of a vehicle drops below a certain threshold;
- Detect the presence of pedestrians;
- Detect the moving vehicle in the opposite direction of travel;
- Detect the presence of smoke, fog or reduced visibility;
- Detect the presence of debris on the roadway.
- Detect lane change;
- Detect real-time traffic conditions, such as:
    - Average speed [km / h];
    - Traffic volume [number of vehicles / h];
    - Traffic density [number of vehicles / km].
    - Lane occupation [%];
    - Vehicle length [m];
    - Vehicle classification;

- Read and recognize the number plates of vehicles in transit for all the following types: European plates, possibility to update in new configurations in the future and new nations, special Italian plates (eg Police Forces, test plates, temporary plates, etc.);
- Automatically detect the orange ADR hazardous goods warning panels with decoding of the Kemler and UN Codes;
- Measure also in conditions of:
  - Rain, even intense;
  - Night or poor visibility;
  - Fog;
  - Snow;
  - Smoke.

The Multi-function Smart Camera system must be activated or deactivated, both locally and remotely, through staff or with appropriate permissions.

1.2.5.2 Check for entry and exit junctions

The junctions control system allows an access monitoring and management activity to be carried out remotely and automatically at junctions along the highway, through the installation of automatic vehicle barriers. The gate system must be able to:

a. Manage the transit of vehicles in the entry and exit lanes;

b. Carry out the registration of vehicles to be transmitted to the control center.

In particular, the functions connected to the gate system are:

- Detection of vehicular classes;
- Video surveillance / traffic monitoring;
- Plate reading;
- Data collection and storage;
- Access control;
- Directions for alternative route in case of non-viability of the road section.

The motorway access control system is a solution that allows to monitor, enable and document digital access to the road infrastructure for security purposes. The system is generally composed of:

- Automatic barrier complete with aluminum rod on which red continuous light LEDs will be installed when the rod is in a horizontal position and green when it is in vertical position;
- Outdoor context camera for video surveillance installed on a pole of appropriate height, equipped with P-IRIS lens control for optimal opening of the diaphragm, in addition to IR illuminators on board, adjustable both for angle and for intensity, which will allow area coverage in a range of 74 m^2 (for angle of opening equal to about 44 °) and 3.413 m^2 (for an opening angle of approximately 140 °); such cameras will be installed at each junction, both inbound and outbound, in order to:

  a. Supervise the requested area;

  b. Monitor any critical issues (accidents, work in progress);

  c. Monitor the operation of the plant equipment present;

  d. Detect any incorrect direction taken.
- RADAR sensor for traffic detection, located at the center of the lane;

- Multi function Smart Camera, able to read the number plates of each vehicle in transit and identify rescue vehicles or Anas vehicles (in case of emergency and closure of the gap for security reasons, it will allow entry on the section only to vehicles authorized for the management and resolution of the intervention)

Moreover, in every junction there is the vertical light signage, consisting of:

- A Variable Message Panel, to inform users about the state of the gate, positioned, at a distance that allows the user to be redirected safely towards an alternative route;
- Mono-Facial Light Boxes, designed to signal the closure of the gate to the user;
- Special semaphore lantern with a fixed circular red light, used exclusively in correspondence of level crossings with barriers. During the period of lighting of the red lights, vehicles must not cross the signal so that they can observe its indications; when the lights go out, vehicles can proceed in their own march.

The system is connected to the control center; in particular, in each passage, a shelter wardrobe is installed that houses the power equipment and data transmission and control equipment.

The control center is based on advanced technologies, connected in a local network with gates, this is able to manage the local system and allow the collection of data recorded in the gates, manage the transit archive and display the acquired data. The remote location allows the operator to view the gate and manage its operation.

The local station, instead, allows the opening/closing of the gate via radio control, proximity reader /keyboard and remote detector. The access system must be interfaced with the system RMT ANAS.

1.2.5.3 Weigh in Motion System (WIM) - Dynamic Weighing

The Weigh In Motion (WIM) system for measuring the weight of running vehicles was introduced within the Smart Road technological infrastructure for the monitoring of infrastructure loads, or selection and subsequent legal measurement of overloaded vehicles. The solution is able to detect the weight of each individual vehicle in transit at any travel speed.

For the highway code, the infraction for a weight beyond the permitted limits can be sanctioned only if the weight is measured on an approved static weighing station. Therefore, dynamic weighing cannot, in the current state of legislation, constitute a sanctioning test. The system of dynamic weighing, will, then, be used only with the aim of identifying the vehicle that has committed the infraction and transmit the corresponding images to the operating room.

The WIM system covers one or more lanes of the roadway and uses inductive loops and sensors with high precision working through piezoelectric technology. These sensors can be installed in any type of road paving (asphalt, cement) and are minimally invasive.

The dynamic weighing system is associated with a vehicle recovery system, which by means of one smart camera, mounted on a side pole, positioned immediately downstream of the weighing sensors, acquires the image of the vehicle that appears to be "overloaded". The camera must be in color, as the color of the medium represents an information essential to its identification, together with the shape, the plate and any writing on the vehicle. At night, the scene must be illuminated by a spotlight mounted on a side pole in line with the sensor system.

For vehicles that exceed the allowed weight limit, some transit images are acquired that allow the identification of the vehicle. Finally, the images are sent to a central system (Smart Road network node) that stores this information in a database in the Operating Room.

In particular, the system will be able to:

- Manage the sensors mounted on two or more lanes: driving lane and fast driving lanes and / or overtaking;
- Carry out a measurement of the weight of vehicles passing between two lanes (between driving and overtaking, or between driving and emergency);

- Determine the weight per axis, for groups of axes and the distance of the axes;
- Determine the length of the vehicle;
- Determine the speed of the vehicle;
- Classify vehicles in transit;
- Record the date and time of the transit;
- Acquire image of the vehicle if overweight.

A system based on a pair of WIM piezoelectric sensors must nominally guarantee one accuracy of 5%, determining the weight as the arithmetic mean of the weights detected by each individual sensor.

The plant consists of:

- WIM piezoelectric sensors installed in the roadway. The length of the sensors is in agreement to the width of the lane to be covered;
- A dynamic weighing unit, Datalogger with Web interface and protocols of communication. Configuring of the Datalogger based on the number of lanes to monitor;
- Inductive loops installed in the roadway, at the piezoelectric sensors;
- Power supply, switches and cables;
- A vehicle shooting unit: multifunction smart camera reading license plates;
- A central monitoring and data storage unit;
- Temperature sensors, to correct the measurement according to the asphalt temperature;
- Bi-component resin for sealing piezoelectric sensor cuts.

The WIM sensors used are piezoelectric weight sensors, characterized by a flattened profile to reduce the noise transmitted by the road when an axis approaches the sensor or a vehicle passes on an adjacent lane. The sensors installed cover the entire width of the lanes.

WIM piezoelectric sensors can be of two types:

- Piezo-ceramic sensors, with weight correction based on the difference between the measured temperature and that to which the system calibration has been performed.
- Natural quartz sensors, which ensure the accuracy of maximum response as well as in the time also to the variation of the temperature.

The dynamic weighing unit processes the signals from the sensors installed in the asphalt: two piezoelectric WIM sensors and one loop on each lane, and temperature sensors for the compensation of the derives from the signals coming from the piezoelectric sensors.

The unit consists of a processing system that, processing the signals coming from the sensors, obtains information on transits. For each vehicle in transit the lane is determined, the category of membership, number of axes, speed and weight, as well as the weight of each axis on each individual sensor. The unit works as a data logger, so the transit data remains stored on one flash memory for a user-configurable period.

The unit communicates via TCP/IP channel with a program with a graphical user interface, through which it is possible to configure the equipment, examine the transit data, carry out the temperature curve control. The unit communicates with the smart camera using a serial channel. The trigger for image acquisition is provided to the camera by the four signals ON/OFF, one for each loop. When the vehicle leaves the system, it sends on a serial channel a message containing information about the transit.

The equipment also handles anomalous cases, such as transits straddling the first and second lanes, or transits that engage the turn in the emergency lane (if provided). These transits are identified by particular flags in the message and contain all the information detected (in the case of transit with engagement turns into an emergency lane) or reconstructed from those detected by the two systems (in case of transits between the lane and the overtaking lane).

The vehicle recovery unit consists of a smart camera with high resolution color head 1280X980 able to acquire one or more images of each vehicle transited on the system, where the vehicle number plate is visible along with other details useful for identifying the vehicle.

The camera is mounted in a watertight container with standard IP66 protection, equipped with fan and heater controlled by separate thermostats.

The image acquisitions are synchronized by the ON / OFF signals sent by the weighing unit.

If the vehicle is overweight with respect to its category, images are acquired with full resolution of the vehicle, and are sent to the central monitoring unit and associated with the data acquired from the weighing unit using the TCP / IP protocol. If the weight of the vehicle is regular, only the data acquired by the dynamic weighing machine are collected and the images related to it are deleted directly from the shooting unit.

The unit is positioned in such a way as to pick up vehicles that transit in all lanes (driving and overtaking); if the service takes place at night, the camera commands the lighting of the side light, placed in correspondence with the weight sensors.

Finally, a wardrobe is placed at the base of the side pole on which the multi function smart camera is mounted containing in its inside:

- Terminal;
- Power supply unit complete with network filters;
- Dynamic weighing unit;
- A switch;
- A contactor to control the lighting of the external spotlight.

1.2.5.4 Intelligent Truck Parking system

The Smart Road project provides the improvement of safety and comfort of the hauliers and their goods through ITS applications. Along the artery road parking and rest areas dedicated to heavy vehicles and commercial vehicles for the transport of goods called *Intelligent Truck Parking* (ITP), implemented with surveillance, information and booking services may be created.

For this purpose, as part of the IoT sensors, in the parking areas for each stall **smart parking** sensors will be installed, which are able to determine the status of a parking (free / busy) and then detect the arrival and departure of a heavy vehicle from the parking area.

1.2.5.5 Smart Tracer Road Work

The Smart Tracer Road Work is an intelligent device that can be installed on vertical signs of beginning and end of the construction site, used to outline work areas, routes, accesses or operations of extraordinary / ordinary maintenance. The device is equipped with a GPS position sensor, triaxial accelerometer, able to detect shocks / overturns / displacements and manual on / off switch.

The device must be set up for data communication via wireless systems (3G / 4G / LoRaWAN / IEEE 802.11 / IEEE 802.15.4) with ability to remotely communicate its position at least every hour and at every move. The Smart Tracer Road Work must be equipped with a rechargeable battery with a duration of at least 10 days and a casing with a degree of protection minimum IP65.

The device must be able to interface with the Anas RMT Corporate System or systems of management and control of ownership of the Contracting Authority, for data processing in real time coming from the field (construction site start point, construction site end point and overall length of construction site).

1.2.6 Environmental monitoring system

The road meteorological information system ("Road Weather Information System" - RWIS) is aimed at estimating in real time variables potentially capable of raising the level of risk of road traffic. In particular, the main environmental parameters will be measured connected to the road infrastructure, in order to have forecasting information alert and warn the user through alert messaging as well as mobilizing the teams in a short time and increase safety levels.

The RWIS is dedicated to the control of the following environmental parameters:

- Wind direction and speed;
- Air temperature;
- Air humidity;
- Atmospheric pressure;
- Noise pollution;
- Concentration of atmospheric pollutants (CO, CO_2, NO_2, PM-10); Brightness;
- Intensity and type of precipitation;
- Water level of watercourses.

An environmental monitoring station may consist of a single sensor or the combination of the following equipment.

The anemometer is a sensor that measures wind speed and direction. Through the measurement of the rotations performed by a cup anemometer (supported by three arms), whose rotation is caused by the movement of the air, the wind speed is measured. Particular bearings and the presence of a special lubricant must guarantee the optimal functioning of the anemometer in both favorable and extreme climatic conditions. The wind direction is instead detected by a wind vane anemometer.

The "precipitation" sensor (or Meteo Station) consists of the disdrometer and other sensors (like the temperature, pressure, humidity sensor, etc.) and performs the detection of the weather conditions. This set of sensors must be able to detect the following information:

- Type and level of snow and / or rainfall precipitation and estimate of visual distance;
- Water level or ice thickness on the surface of the road surface and relative salinity / chemical concentration and freezing point;
- Indication of precipitation in progress (beginning / end of last precipitation);
- Precipitation intensity and accumulation value;
- Precipitation classification;
- Measurement of solar radiation;
- Thickness and visibility classification;
- Humidity and air temperature;
- Atmospheric pressure.

The global radiation sensor (pyranometer) is a direct solar radiation device spread throughout the electromagnetic spectrum, calculating the difference in temperature detected by high precision thermoelectric cells (thermocouples). The sensor must have aluminum housing and a glass half-dome to protect the measuring area from both cooling caused by the wind and from the influences of external agents, must also be equipped with a leveling plate for optimal positioning. The device will have to be prepared for connection to the analog input of the multi-functional control unit, specially designed for the measurement of low voltage signals.

The "noise" sensor is a device that measures noise levels in real time. The sensor is equipped with an omnidirectional microphone and an acquisition module, processing (calculation of spectra, audio recordings, signal processing, recognition of events, etc.) and a programmable data transmission module.

The "atmosphere" sensor measures the main environmental parameters such as: carbone monoxide and dioxide, nitrogen monoxide and dioxide, fine particles. The high precision measurement sensors for pollutants and powders are equipped with an acquisition, processing module and a programmable data transmission module.

The brightness sensor measures indoor / outdoor brightness through transformation of light intensity in a digital output signal in lux. This device allows to perform lighting control and ensure intelligent and efficient energy consumption.

The liquid level sensor that measures the level of watercourses at the crossings, such as bridges and viaducts.

Control unit for the connection of the sensors. Weather data and all environmental information, detected by the various sensors mentioned above, must be stored in a database that will make them available for their consultation and processing. Reporting concerning the states of operation will be made available and integrated with the control center system that will use them to alert the staff responsible for restoring correct operation. The sensors will be installed on a pole, while inside a cabinet a local datalogger that will have the task of recording the data collected by the control unit in real time and send them to the integrated center system via the Smart Road network node will be placed. In case of deficiency or no connection, the data will be stored on the local memory and made available to transmission when the connection is restored.

1.2.7 Monitoring and intervention system with drones

The implementation of drones on the Smart Road allows to monitor road traffic in strategic points for traffic and allows the planning and efficient management of traffic flows along the road.

Critical information obtained through drones is aimed not only at managing the road traffic, but provide a valuable contribution in monitoring the area in which an eventual accident occurs, allowing the management of the intervention actions of the rescue vehicles and transport of emergency kits.

Images captured by drones are sent in real-time, via a secure Wi-Fi connection, to the control room, which initiates the coordination of the emergency. The drone is remotely controlled by an operator or carries out a pre-established path in an automatic way.

The transmission of images guarantees, in any case, the privacy of sensitive user data.

The drones allow continuous monitoring of the infrastructure through photogrammetries and surveys of different nature that display areas of construction and state/operation of the civil and technological works in places that are difficult to inspect, also allowing an effective management of road personnel and adequate maintenance.

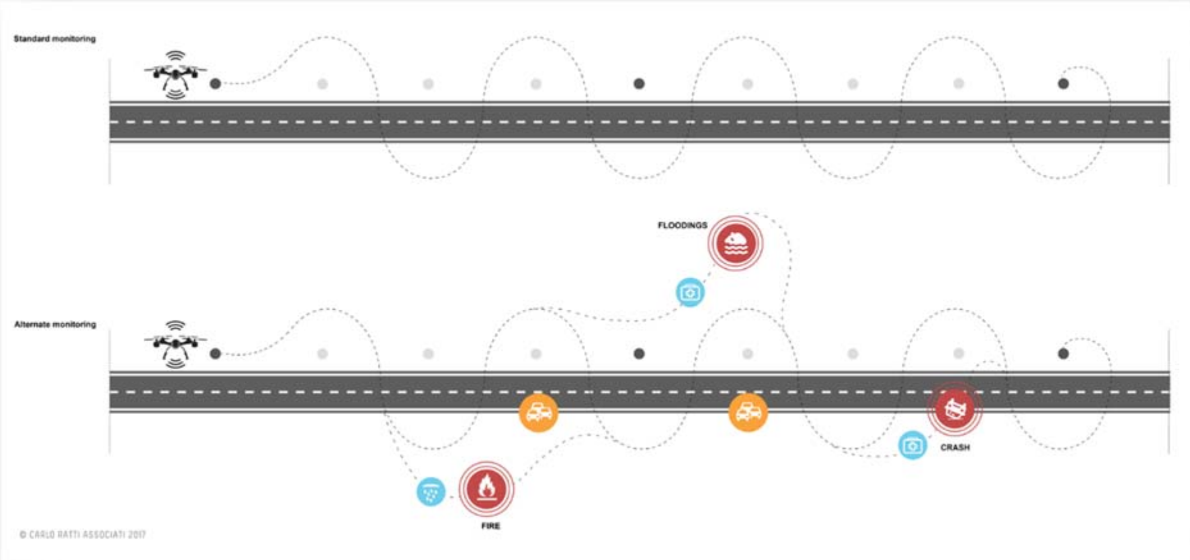


Figure 46 - Monitoring scheme using drones

The system provides useful information for tracking vehicles of interest such as in the case of exceptional transport or transport of dangerous goods in order to be able to monitor the vehicle along the stretch of interest.

The drones can also detect illicit behavior of users as vandalism and theft constituting a valid support to surveillance cameras.

In the near future the areas planned for electric recharging of drones can also be used for equipment intended for the delivery of small size goods.

The areas of landing and charging of drones are "smart", automatically governed and able to communicate, at short range, with the drones that are nearby, indicating them station status (free / busy) and its location via GPS. The station also plays the drone deposit function.

Most of the advanced drones are equipped with an automatic landing system capable of hooking the position of the landing platform using GPS. Operation is relatively simple as a flying drone detects that the battery is running out, searches for the nearest charging station, the latter informs the drone of its position and the possibility of recharge (in case it is free); once the green light is

obtained the drone, by knowing the GPS coordinates of the station, approaches and takes the vertical landing on the assigned area.

Once landed, a subsystem recharges the battery through a mechanical arm that uses different charging standards, USB, plug-in system or via an induction system. Once the recharge has been completed, the drone can be used or hosted in the dedicated box that closes down to guarantee complete protection.

The drones must interface with the RMT system for the functions of location, video surveillance and complete diagnostics of the apparatus.

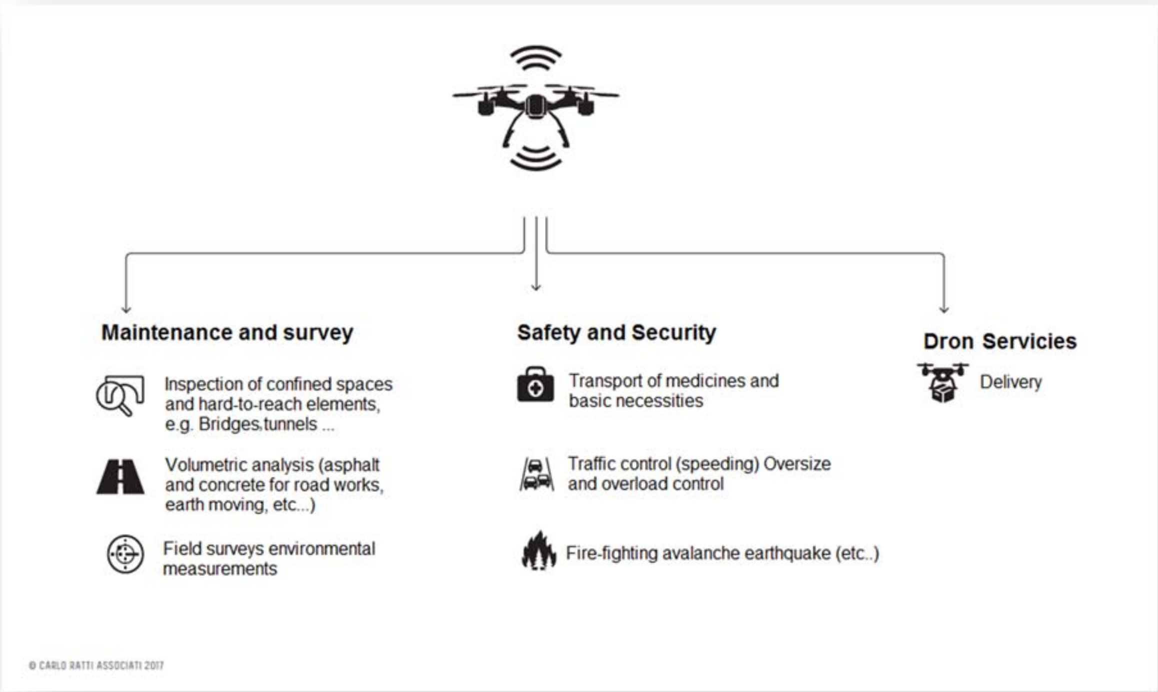


Figure 47 - Summary diagram of the DRONE functions and services

1.2.8 Identification with RFID TAG

The TAG is a "passive" element, as it is not able to initiate communication and exploits, to respond, the energy of the signal sent by a modern device.

A TAG contains at least one univocal and read-only identifier (UID, or Tid, ie the TAG identifier) often limited to a few characters and an additional memory that, according to the choices, can contain from a few tens to several thousand characters. The same memory can be read and written via a standard communication protocol (NDEF messages) with which formatted data can be saved (such as text strings, address book contacts, web URLs) etc.) and that can be interpreted correctly by every RFID reader.

Taking advantage of the aforementioned functionality, all infrastructural works, electrical, electronic and electromechanical appliances, as well as complex composite equipment and technical premises belonging to the Smart Road, will be equipped with passive TAGs accessible from the outside and containing web URL addresses where all the documentation is stored (as-built documents of the structures, the technical sheets of the technological components, the wiring diagrams) and all the information necessary for Anas specialized operators.

1.2.9 Permanent fiber optic monitoring system for road infrastructures

In the smart road, a fiber optic monitoring system may be provided, where necessary for the evaluation of the safety of the main road infrastructures through the control of the three basic parameters:

- Resistance to stresses, understood as the difference or relationship between the resistant entity and the stimulating entity, that is, between the system of forces able to cause the collapse of the work and those applied;
- Normal operating conditions (functionality) with regard to deformations or excessive vibrations;
- Durability assessed as the possibility of the structure to maintain constant over time the two previous parameters.

The purpose of the safety checks of a structural complex or of a portion of structure is to ensure that the work is able to withstand with adequate safety to the actions to which it may be submitted, respecting the conditions necessary for its normal operation, and ensuring its preservation over time.

The permanent control of the tenso-deformative state of the road infrastructures in operation will take place through the monitoring that consists of the following phases:

1. Measurement of temperatures and levels of deformation, inclination and accelerations linked to static and dynamic stresses of exercise (e.g. earthquake and / or particular situations);
2. Transmission of the measured structural data to the reading and processing units;
3. Evaluation of the presence of any hardware anomalies on the sensors by analysis of the measured data or through signals / indicators of anomalies sent directly from the sensor to the control center;
4. Interpretation of numerical data in terms of synthetic and graphical parameters that describe the tensile-deformative state of the structure and its relative state of efficiency.

The data coming from the monitoring of the above mentioned parameters will also allow updating of the theoretical models of the structures subject to monitoring in order to reduce and correct the differences between the structure itself and the theoretical model.

The objective of the aforementioned monitoring systems is to measure the significant parameters for the assessment of the state of health of the infrastructures in order to plan and optimize the maintenance interventions, to seize the occurrence of anomalous structural conditions to be put into particular attention, as well as for structures of strategic importance, the possibility to extend their useful life of project, carrying out some targeted maintenance interventions.

The significant parameters monitored, in relation to the different types of infrastructure, are classified as follows:

a. Monitoring of the deformations of the beams of the decks and the pulvinos;
b. Dynamic monitoring of the vibrational components of the structure to obtain information on the acceleration levels to which the entire structure subject to vehicular traffici s subject;
c. Monitoring of inclinations and subsidence (phenomena of subsidence) of the piles;
d. Monitoring of the fatigue phenomena of the structure amplitude stress due to the vehicular traffic; is.
e. Monitoring of structural integrity through the variation of natural frequencies of the structure.

The sensors required for deformation monitoring are all based on fiber optics technology. One of the technologies that can be implemented is that of the Bragg grid, FBG

(Fiber Bragg Grating). A Bragg reticle (FBG) is a set of reflectors constructed from a small fiber optic filament segment, each of which reflects a particular wavelength of the light beam and transmits all the others. In short, the concept of FBG sensors is based on the perturbation of the refractive index of the optical fiber at certain points (FBG sensors) of it: these perturbations allow to reflect a determined wavelength and to continue to transmit the others within the fiber. The light beam passes through the nucleus of the optical fiber filament undisturbed and any deformation (caused by the variation of the surrounding environment temperature, pressure, vibration or stress from the external world) causes a jump and a change in the amplitude of the wavelength reflected.

Fiber-optic technologies can be used with performance equivalent to or greater than that described above.

The fiber-optic monitoring system of a viaduct will have the minimum configuration, described below:

- One or more fiber optic deformation / temperature sensors on each of the beams of the deck for each span;
- One or more triaxial accelerometers on the deck;
- An accelerometer / inclinometer for each pile.

The elements of the monitored decks are grouped by a certain number of modules. Every module is represented by a string consisting of maximum 4/5 sensors of fiber optic deformation / temperature (to avoid optical interference between the signals produced by the sensors on the same string). The fiber optic deformation / temperature sensors of each string are interconnected on a Local Network through single-wire cables of the SMR 28 in type sheath or similar.

Each Local Network is connected to a site monitoring system in a technical room through optical fiber backbone attested in optical drawer on SC-SC compasses. Fiber optics backbones are terminated in junction box at the edge beams of each viaduct on which local networks are arranged. Each local network is wired through watertight containers, boxes of derivation and cable entry tubes. Each string of sensors in the local network is merged into junction box at both ends with a backbone fiber.

The fiber optic section (backbone) attested at the technical room is shown below.

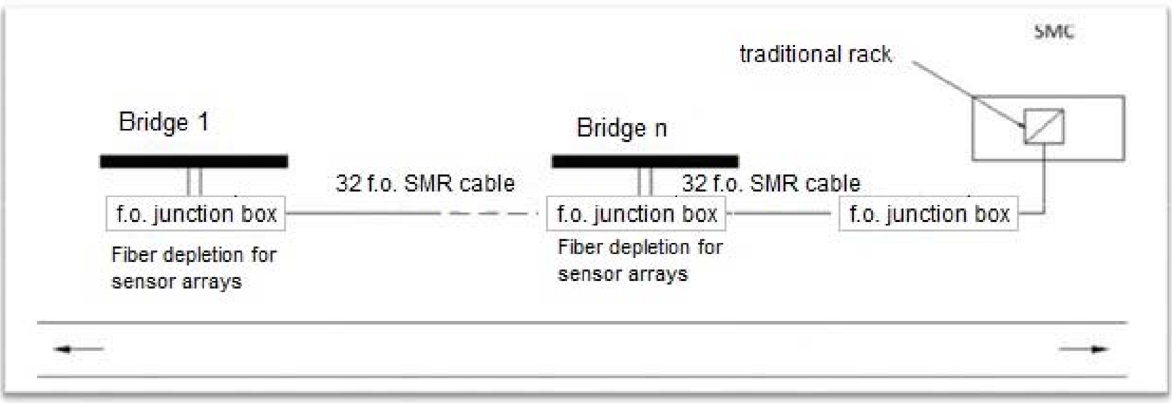


Figure 48 - General scheme for fiber optic monitoring

The system will be able to continuously acquire:

- The vibratory phenomena to which the main structural elements of the infrastructure are subject (decks, piles, etc.);
- The quasi-static thermal deformations (summer/winter cycles and day/night cycles) to which the structure is subject;
- Long-term deformations (settling of the soil, aging of the structural elements, etc.).

The monitoring system will allow to:

- Adapt the design of the monitoring system and the instrumentation used to current regulations;
- Define the synthetic parameters of the deformations that are representative of the structural health of the work monitored;
- Choose the frequency of the measures appropriate to the phenomenon to be measured;
- Define thresholds of the structural parameters to quickly activate alarms for the reporting of any anomalies;
- Return the data in both tabular and graphical form allowing the correlation with any calculation models;
- Web-based software platform that acts as a collector and a computer with a user-friendly graphic interface, which allows ANAS operators, with the access credentials, to interact with the output of the local monitoring system via the web with the most advanced tablets and smartphones;
- The Web platform makes it immediately possible to access data in real time using the TCP/IP protocol;
- Each monitored infrastructure will be selectable on screen using the GIS Web application.

For the monitoring of deck stacks using accelerometers and electrical inclinometers is adopted an architecture based on an autonomous local measurement station (located on different viaducts to avoid problems of attenuation of the electric signal), connected directly to the monitoring system using a suitable fiber optic transmission network.

The architecture of the sensor system therefore presents the following two subsystems:

1. The matrix of optical deformation/temperature sensors located on the different viaducts, is managed directly by the monitoring system through an optoelectronic control unit able to manage matrixes of optical sensors;

2. The matrix of electrical accelerometer/inclinometer sensors, connected via signal cable to a control data logger for automatic data acquisition. Electric signals coming from the sensors are acquired at fixed intervals. Appropriate electro/optical converters will be used for electrical sensors.

A dedicated fiber optic backbone will be used to channel the signals from the systems above mentioned to the local control center.

The remote control center periodically interrogates the peripheral units and by means of a management SW visualizes and stores data related to the entire set of sensors: strain sensors, accelerometers, inclinometers and thermometers. These operations can be conducted locally also at the local control center.

1.3 Management and control system of the dynamic lane

The dynamic use of the emergency lane, like n + 1 lane of transit, represents a short-term solution to congestion due to the increase in traffic on the road network. The use of advanced technologies, such as traffic detection systems, remote surveillance, and panels with variable message, allow to manage the use in safety and in particular traffic conditions of the emergency lane. Through the use of the emergency lane it is possible to get advantages in short times such as:

- Expansion of motorway capacity and reduction of congestion;
- Reduction, with the same traffic, of vehicular density with reduction of conflicts and reduction of accident probabilities;
- Availability of systems (variable message panels, cameras etc.) for other uses already envisaged in the Smart Road project;
- Reduction of traffic peaks.

The system will be implemented in compliance with current regulations. The system will be realized through the installation of vertical emergency signs, video surveillance (CCTV) both along the entire route mentioned above and in correspondence with the areas of interchange and / or connection with the "ordinary" viability, in order to make the emergency lane (dynamic lane) usable in the occurrence of particular intense traffic conditions at certain times of the day.

The software used must be developed on the basis of communication protocols of widespread use in order to be able to provide centralized management of this plant together with other plants of the same type.

The configuration of the system serving the affected road section includes:

- Management platform located in a dedicated room inside a cabin of electricity supply on the Green Island;
- PLC Master always located in the same cabin where the general management algorithms reside and the communication protocols towards any of its Slaves; the Master, moreover, has all the information coming from all the devices in the field;
- PLC Slaves located along the route serving the various users;
- "Remote" terminal blocks, ie without management CPUs, located in the cabinets of each PMV.

All the local equipment of the system will be connected via fieldbus in FIPIO cable to the cabin PLC with coordination functions of them.

The collected data must be processed and placed on the multimode fiber optic data network with Ethernet protocol, which will allow to inform all the programmable controllers of the system (PLC) of the situations present in real time, so that after data processing is possible to control, according to the needs, the single devices present in the field.

Instead, the connection of the equipment to the plants will be accomplished by:

- Digital input and output signals;
- Analog input signals;
- Field connections via serial line for information and commands exchange.

The entire remote control system will be managed by the management and control software platform that allows to manage all the equipment.

The following is a list of the system equipment for system implementation:

- Vertical emergency signage system;
- Video surveillance system (TVCC);
- Telecontrol system (Software platform).

By way of example, diagrams and signs are shown for a typical installation of a fourth motorway dynamic lane.

1.3.1 Vertical emergency sign system

In order to provide complete information to users in the event of opening to traffic of the emergency lane, they will be prepared along the entire route both in internal and external carriageway a series of PMV of different types. The panels, of an alphanumeric type with pictograms and arrow-cross, will be positioned on special support structures with flag and / or on a galvanized steel trestle.

For the opening/closing of the dynamic lane, different combinations of panel stations with variable message summarized as follows will have to be provided:

- PMV type A station;
- PMV type B station;
- PMV type C station;
- PMV type D station;
- PMV type E station.

Type A PMVs (on-site stations) are graphical panels that provide information on the use of the available lanes and speed limits as shown in the following figure:

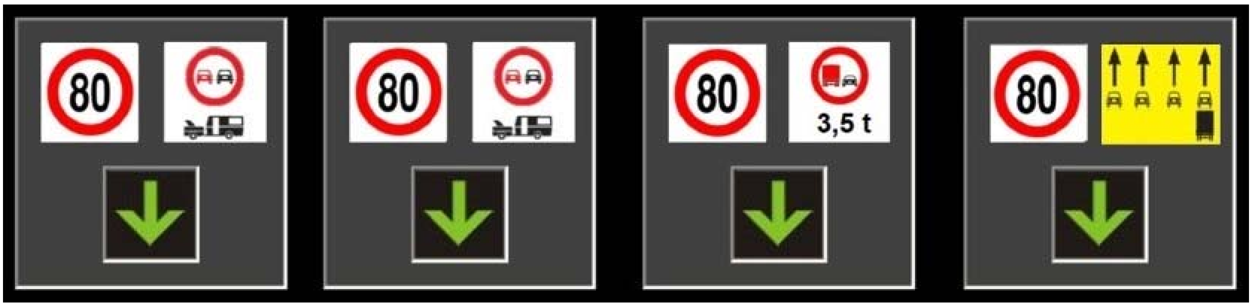


Figure 49 - Example of a type A station

The **type B** station (in itinere stations) consists of graphic panels that provide information for the user's safety and on the variation of the lanes available in the experimental section of the dynamic lane.

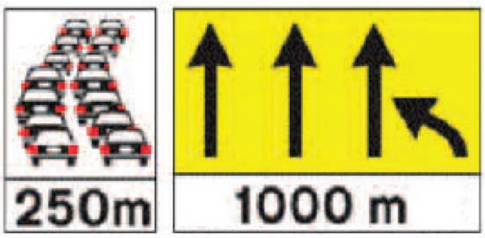


Figure 50 - Example of a type B station

The **type C** station (in itinere stations) provides panels of a graphic type which give specific information on permitted speed limits. They consist of a panel with full color led per pictogram technology, totally programmable. The system provides the possibility of displaying alternatively more pictograms:

Figure 51 - Example of a type C station

The **type D** station (stations at the motorway junctions) consists of three LED technology panels, two of which are full color for pictogram and one is alphanumeric that provide information to users. The alphanumeric panel will be composed of 3 rows of 20 characters each, with the individual character's height of 200 mm.

Figure 52 - Example of a type D station

The **type E** station (in itinere stations) is made up of graphic and alphanumeric panels that provide information to users. They consist of 3 LED technology panels, two of which are fullcolor for pictogram and one alphanumeric. The two full color panels are totally programmable and the alphanumeric panel will be composed of 3 lines of 20 characters each, with the individual's character height of 400 mm. The system provides the possibility of alternating display of several pictograms and more alphanumeric text pages as well as control and brightness adjustment independent for each graphic and alphanumeric element:

Figure 53 - Example of a type E station

Each PMV station will be equipped with a power and control panel consisting of a IP54 cabinet of minimum dimensions 900x1700x600 mm, with appropriate base, inside which the control unit, the modem and all the power devices to power and drive the panels connected to it are inserted. The control unit will control the panels via a serial line and execute its diagnostics. The supply will be complete of all the connections to the panels, the wiring, the fixing accessories, the system programming through specific management software and the connection to the control center and anything else necessary to give the system perfectly working.

1.3.2 Video surveillance system (TVCC)

The monitoring of vehicular traffic on the stretch of road affected by the intervention results fundamental in order to guarantee the safety of users who transit daily.

Furthermore, the installation of a camera system is useful for checking the traffic conditions 24 hours a day and at critical moments (like peak hours).

1.3.3 Software management platform and remote and local control

The road section will be equipped with a special automated and centralized tele control system, designed to check the regular operation of the installed systems as well as their local management collecting status reports, measures from the field and giving the appropriate remote controls. In addition, it will report all the possible anomalies, recording them on a special historical register, and provide assistance in maintenance operations.

In this way, we can satisfy the need to guarantee the highest level of safety for the user and to have the possibility, in real time, to know the parameters related to the management systems, to safety and to the environmental state of the entire road section under examination. This system will therefore be structured in order to guarantee, through programmable logic controller (PLC) suitable for the control of medium-sized machines / systems, structured on different hierarchical levels of operation, the immediate maintenance intervention in case of breakdowns and / or alarms and to provide drivers in transit with information about the environmental state of the moment and therefore to avoid alarm and danger situations. The management system of the section under consideration must allow, locally and remotely, the command, the control and the self-diagnostic of all the systems. The control system must be structured in order to maintain the vital functions of the elementary units of the systems so that an interruption of the system itself does not in any way compromise the basic intervention of the systems of safety.

Furthermore, the traffic control and management system must be able to:

- Manage the operation of the variable messaging sign system by activating the procedure of opening and closing of the dynamic lane as described below;
- Manage the operation of the video surveillance system (CCTV).

The roadway management system must provide for the redundancy of the management hardware of which at least a part must be able to carry out minimum emergency procedures. The management program, in case of breakage of a component or failure to activate of a procedure must be able to commute to a known emergency condition. The program must be structured in order to allow managing safely the system under examination when it is subject to updating and reconfiguration operations. The situations of alarm must be managed through specific algorithms in a differentiated manner, providing for each of them a priority, so that the system can be directed according to the seriousness associated to them, rather than depending on the sequence of recognition of the alarms themselves. In any case, the alarms must be memorized in order to correctly implement the sequences of refresh. The system must always provide for the possibility of manual switching of the controls in order to carry out all the "reset" operations (in any case in safety) by an authorized on site or in remote location operator. Putting into service the supervision and control system must be carried out simultaneously with the activation of all the technological systems in the service of the road section. The expected materials and the software packages have to respond to the main European and international standards. With particular reference to the IEC regulation 1131, concerning the standardization of Programmable Logic Controllers. Communication is carried out through standard industrial protocols in compliance with IEC EN 60870-5- "Transmission Protocols".

The procedure for opening and closing the dynamic lane is described below:

- **Phase 1**- A road police patrol and / or an ANAS surveillance team check the general traffic conditions for opening the dynamic lane. In this phase in all the type A panels the following signage is present:

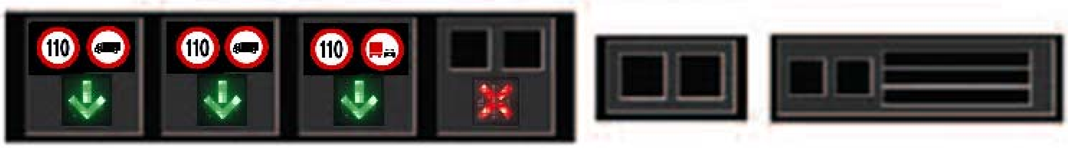


Figure 54 - Phase 1 procedure for opening and closing the dynamic lane

- **Step 2**- A phase of speed harmonization and dynamic lane opening warning is implemented. In this phase all the panels will indicate the established speed limit (ex. 90 km / h):

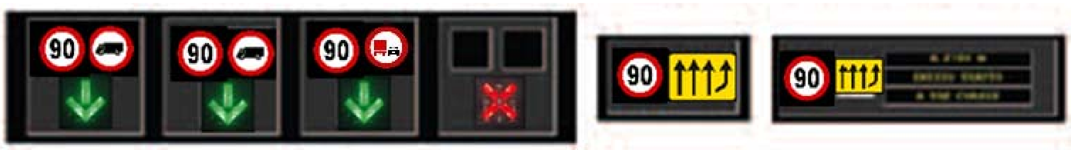


Figure 55 - Phase 2 procedure for opening and closing the dynamic lane

- **Phase 3**- The operator evaluates that the vehicle flow is increasing and proceeds to open the dynamic lane. In this phase the panels will present a configuration like the following:

Figure 56 - Phase 3 procedure for opening and closing the dynamic lane

- **Phase 4**- In this phase it is possible to implement the closure of the dynamic lane:

Figure 57 - Phase 4 opening and closing of the dynamic lane procedure

- **Phase 5** - When the vehicle flow returns flowing on three lanes and decreasing, the panels of type A will show again the following starting configuration:

Figure 58 - Phase 5 opening and closing of the dynamic lane procedure

with speed limit established in the parts of GRA not affected by the dynamic lane (ex.130 km/h) different from the speed limit in the parts of GRA affected by the dynamic lane (ex. 110 km / h).

1.4 Smart Tunnel

1.4.1 System description

The added value for infrastructure safety is given by the type of installed technologies, from sensors and an efficient management system, both in ordinary operation and during the phases of emergency.

The Smart Tunnel system allows:

- Developing and implementing solutions that improve management and safety aspects of the tunnels;
- Developing management systems allowing to prevent and control the situations of danger in the tunnel;
- Monitor constantly and remotely the operating conditions of a specific tunnel;
- Optimize the maintenance of the systems inside the tunnel;
- Having a predictive system of dangerous events.

The high number of sensors already installed and the constant development of the Internet of Things allow implementing a distributed monitoring system using:

- Sustainable wireless redundant sensors distributed along the tunnel
- Traffic sensors: average speed, flow, gridlock.
- Environmental sensors: weather, air speed, pressure, pollution, lighting
- Fire detection sensors: smoke, temperature, dangerous goods

The IOT allows an installation of sensors that can be deployed in large numbers and characterized by the following benefits:

- Low cost
- Small size
- High capability of integration into materials and environments
- Ease of installation
- Use of wireless networks for long distance data transfer thanks to the protocols of communication used (LoRa - up to 15 km in free field and 2 km in urban areas)
- Possibility to operate promptly to deal with anomalies, failures and critical situations.

The Smart Tunnel allows the dynamic management of emergencies; it begins in a preventive manner before that the critical event happens and adaptively after the event to manage the most risky scenarios.

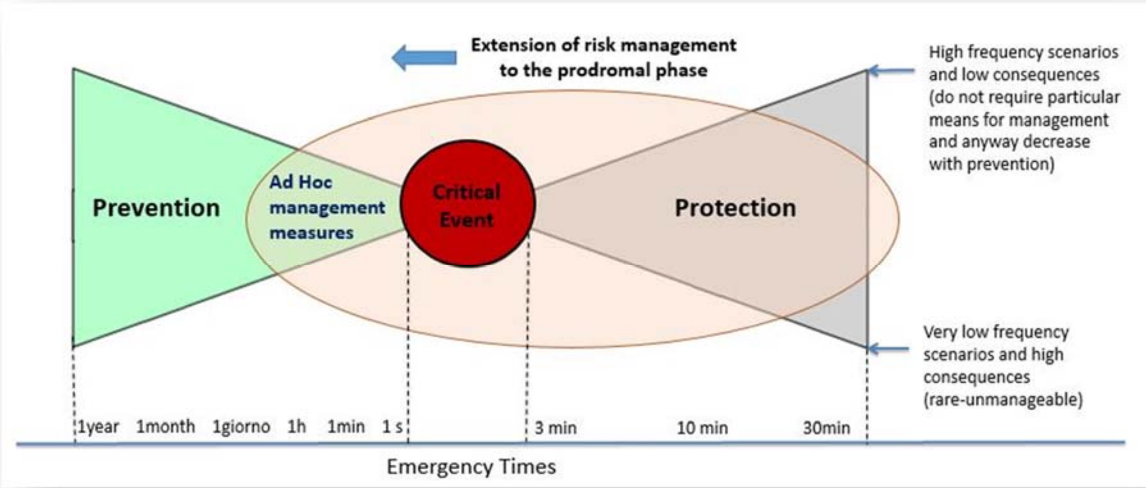


Figure 59 - Representation of the dynamic risk analysis

1.4.2 Management and control software platform

The Smart Tunnel system is based on a software platform, which communicates with the system of supervision and control of the tunnel. The platform calculates the security level of the tunnel on a standardised scale from 1 to 10 after having analyzed a series of parameters.

The input data of the platform are divided into two broad categories:

1. Dangerous events considered as:
   - Generic accident;
   - Fire;
   - Dangerous goods accident.
2. Calculation variables such as:
   - Traffic flow
   - Systems efficiency;
   - Design speed
   - Percentage of heavy vehicles;
   - Geometric features of the tunnel;
   - Gridlock
   - Variation of weather conditions (wind-rain-fog);
   - Efficiency variation of the systems;
   - Variation of average travel speed;
   - Average safety distance (before the tunnel);
   - External luminance;
   - Temperature and humidity of the air outside and inside the tunnel;
   - Concentration of combustion-view products;

The software platform processes the input data above described according to the following diagram, and for each tunnel, a risk value is defined, variable on a scale from 1 to 10, that refers to the present condition of the infrastructure.

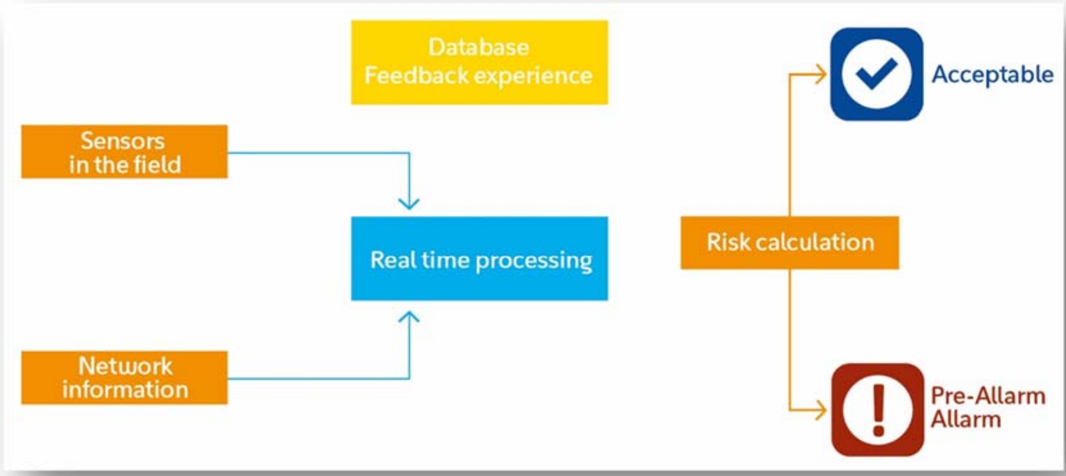


Figure 60 - Representation of a possible model for a Smart Tunnel

For the calculation of the risk value, we can use the following risk model:

$$R = P(n)\, k\, f^3 VP(M + I + D)\varepsilon_p \varepsilon_{pr} N {\sigma_V}^2 \frac{V}{3600\, V_P}$$

$P(n)$	probability function of critical event
k	is a dimensional constant
f	is the flow of traffic
VP	is the percentage of heavy vehicles
M	is the function factor of the weather conditions
I	is the lighting factor to be defined according to the hours of the year
D	is the maintenance factor to be defined according to the degradation conditions of the systems
V	is the average speed of vehicles
V_P	is the design speed
ε_p	effectiveness function of the protection systems
ε_{pr}	effectiveness function of prevention systems
N	magnitude of the event expressed in potential victims according to the type of event
σV	is the standard deviation from the average vehicle speed

The software platform, once known the traffic distribution have to calculate the instantaneous risk on a base continuously lower than 60 seconds, as well as the cumulative risk on the day or on a year.

When the behavior of the operating tunnel distances itself from the virtual one while the ideal one increases the risk index and consequently the security level decreases.

The Software platform when the risk level exceeds the tolerable threshold (ALARP PRINCIPLE) have to send an alert to the responsible departmental room according to the following scale:

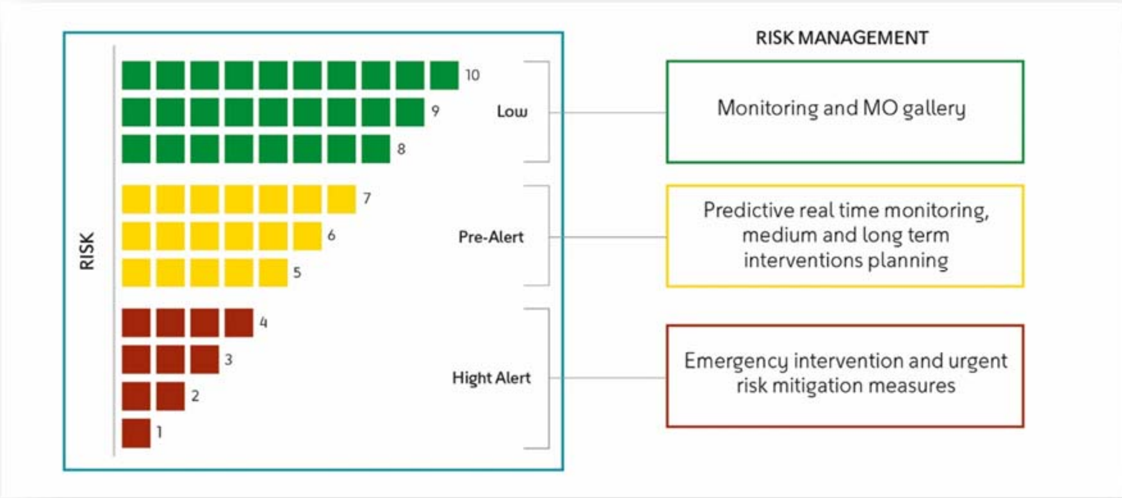


Figure 61 - Example of risk management

The software platform have to be installed on a dedicated server and have to communicate with the Local Control Centre (LCC) of the smart road segment of the tunnel with the Road System Management Tool (RMT). The data of the risk value calculated by the platform will have to be recorded with a continuously frequency lower than 60 seconds will have to be saved on an appropriate storage, historicized and made available for at least ten years.

1.5 ENERGY SYSTEM: Performance and technical specifications

1.5.1 General architecture

The architecture of the energy system provides electricity generation points from renewable source, connectivity to the network of the national distributor, the transformation system, the distribution system of electricity and a generator for power in emergency conditions, as generally reported in the following diagram:

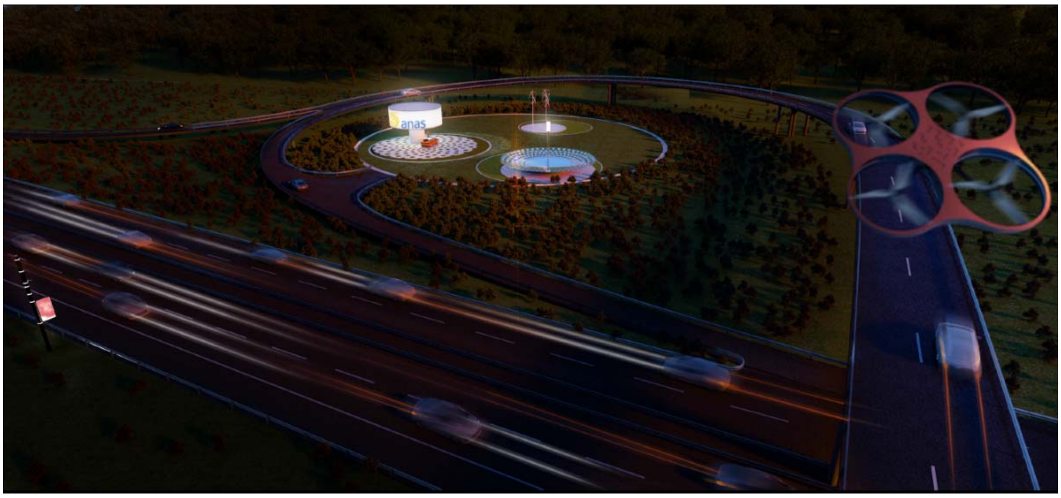


Figure 62 - Representation of a Green Island

Figure 63 - View of a Green Island

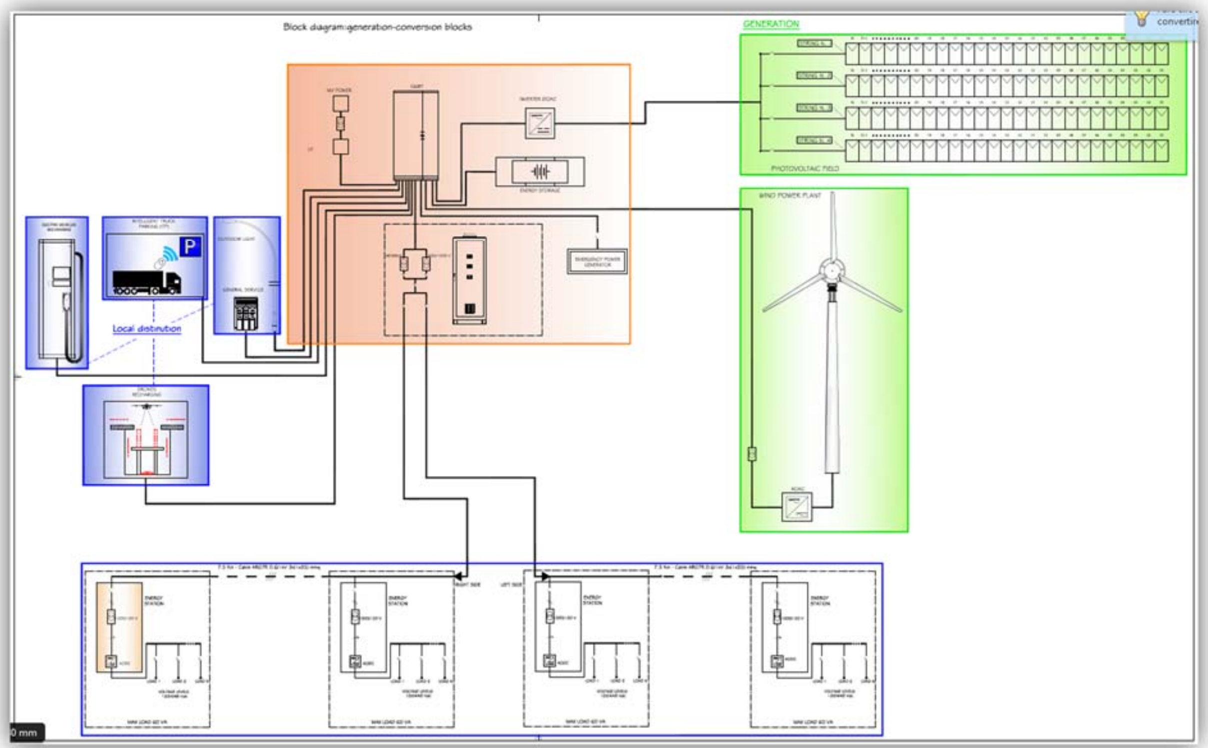


Figure 64 - Energy System Layout

The qualifying aspect is the so-called "Green Island", a multifunctional area for:

- generate energy from renewable sources;
- storing the energy produced;
- connect to the MV or LV electrical network of the national distributor;
- hosting electrical commands and controls;
- hosting the Smart Intelligences distributed by the Smart Road;
- hosting the electric charging columns;
- hosting the recharge and landing / take-off areas for drones.

The green box, in the diagram in Figure 64, represents the generation predominantly implemented with a photovoltaic system and possibly with a small-scale wind turbine. There will be an accumulation system able to guarantee continuity of supply during the hours of non-production or higher energy need.

The technological powerhouse, represented by the orange box in Figure 64, is a room that houses the equipment for transformation, conversion, regulation or marshalling of electrical energy.

The blue boxes, on the other hand, represent the distribution of electricity, subdivided into distribution room for the loads present inside the Green Island and distribution on going for the loads distributed along the road or motorway section of the considered module.

The local distribution of energy, necessary for feeding the loads inside the Green Island, occurs with three-phase lines with neutral, at a voltage of 400 Vac.

Along the way, however, the electrical architecture provides a distribution system suitable for feeding all the Smart Road technologies, including the so-called "multifunctional stations". The output voltage from the general three - phase low voltage with neutral panel with 400 Vac, located in the Green Island, is transformed into 1000 Vac three-phase, without neutral, using a step-up transformer, to feed long road sections and guarantee lower management costs. The distribution of energy to multifunctional stations is carried out, thus, through two three-phase backbones without neutral at 1000 Vac, 15 km long, which feed the loads distributed in right and left compared to the "Green Island" position, for a overall road or motorway section of 30 km. In each polyfunctional station there is an energy station that transforms the input voltage of 1000 Vac, in direct current of 12/24/48 Vdc. The maximum power installed in each multi-purpose station is about 60 W.

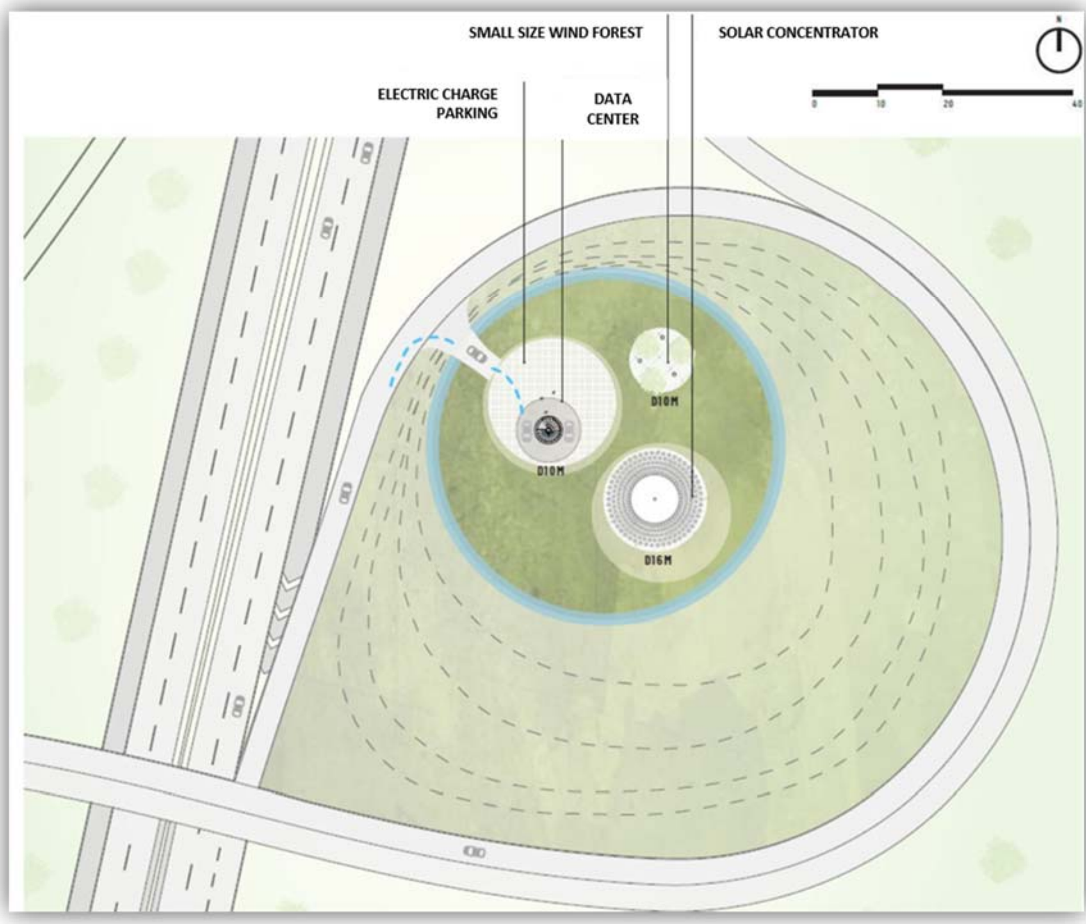


Figure 65 - Representative diagram of a Green Island

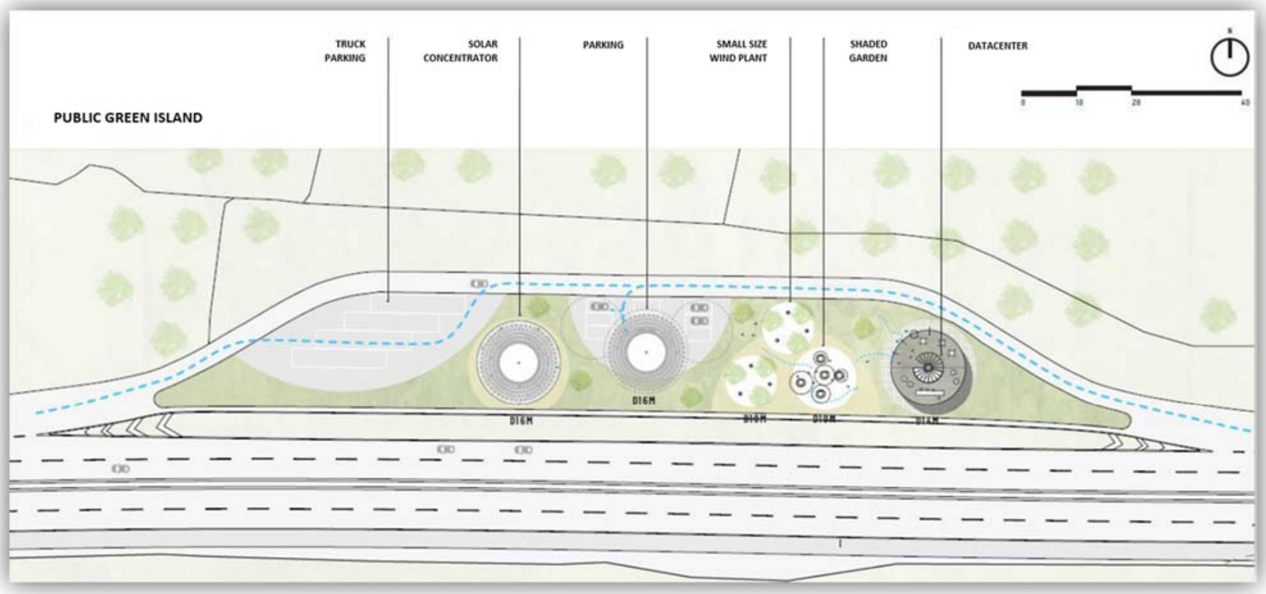


Figure 66 - Representative diagram of a Green Island

The energy system above described refers to a "module", which includes the Green Island and the two 15 km backbones, which feed the multi-purpose stations.

Such modularity gives the Green Island the appearance of "microgrid", low voltage networks having distributed sources, presence of accumulation and load control devices. The Green Island always operate connected to the electricity network, though with the aim of optimizing operating conditions of production resources / energy storage. In case of lack of electricity from the network, there is a generator for emergency power supply, which guarantees a range of at least 24 hours.

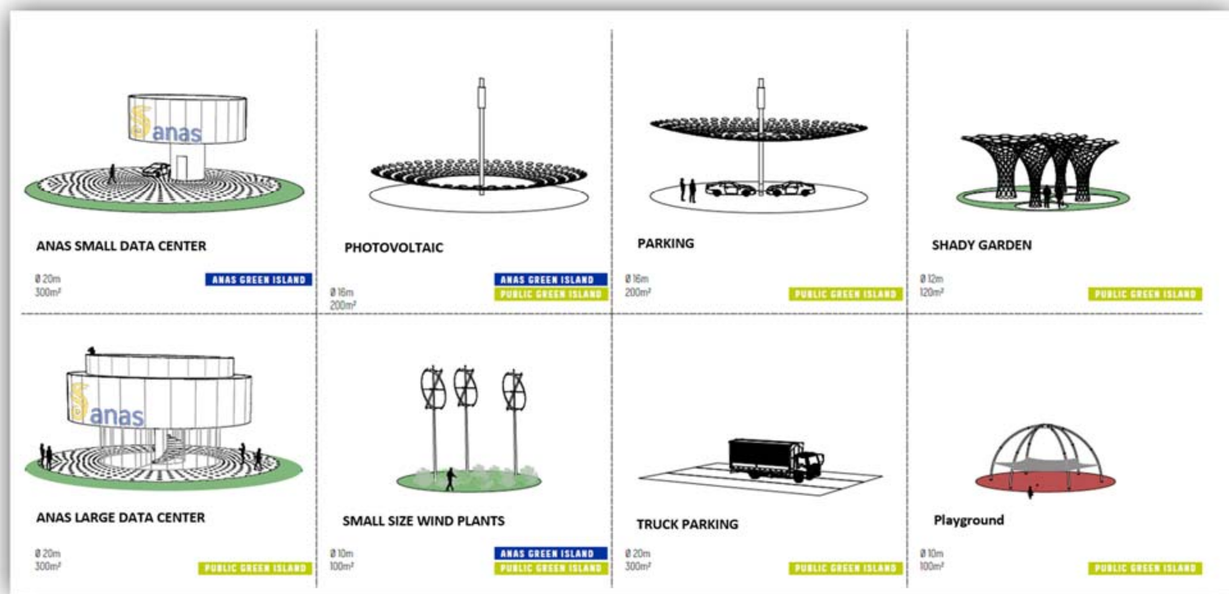


Figure 67 - Green Island modules representations

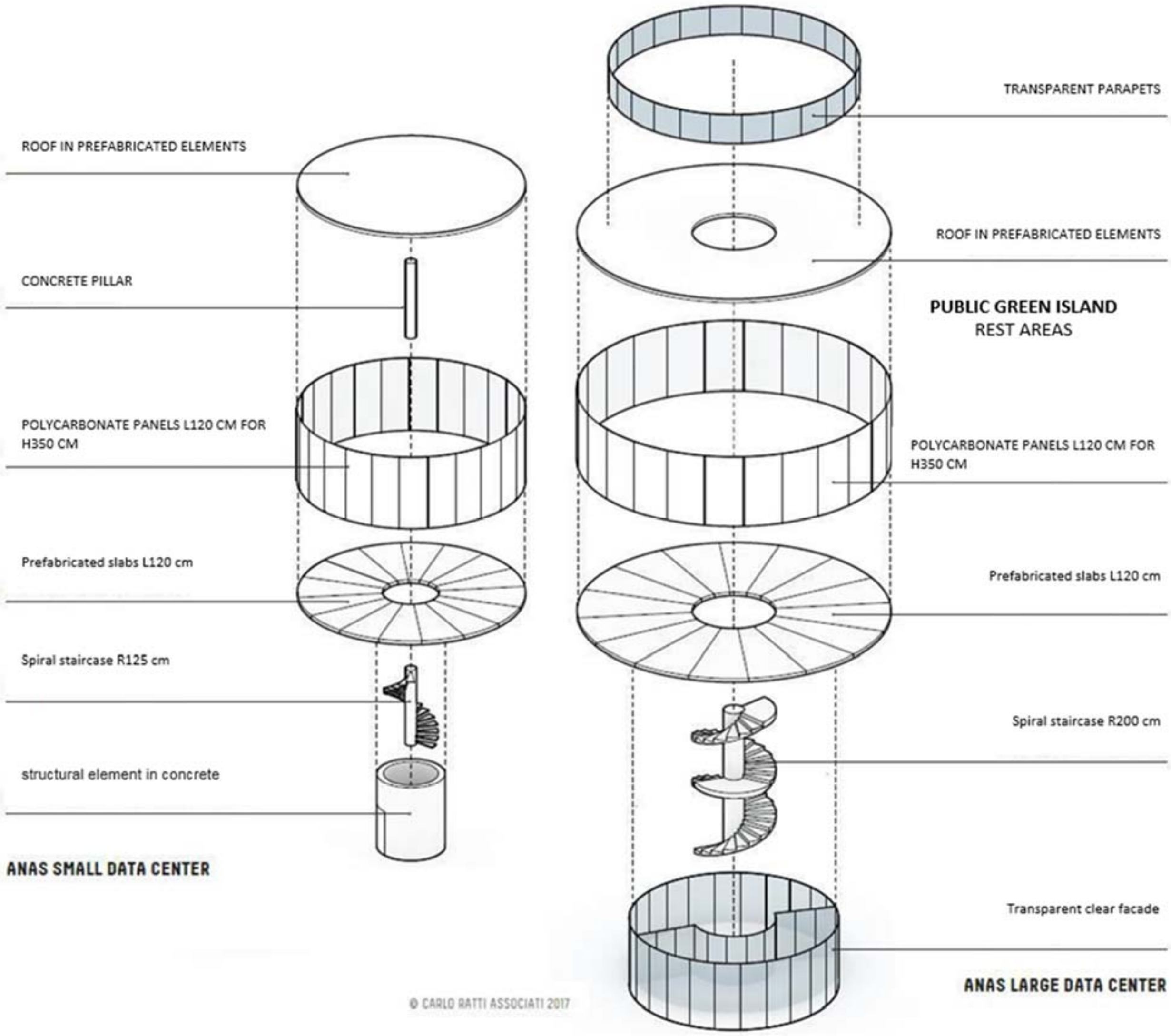


Figure 68 - Module concept diagram of the data centre of the Green Islands

1.5.2 Power generation

The power generation in each Green Island is achieved through sustainable source systems photovoltaic and small size wind power, which allow a high guaranteed savings from self-consumption of the energy produced, which reduces the occasions of withdrawal from the electricity grid.

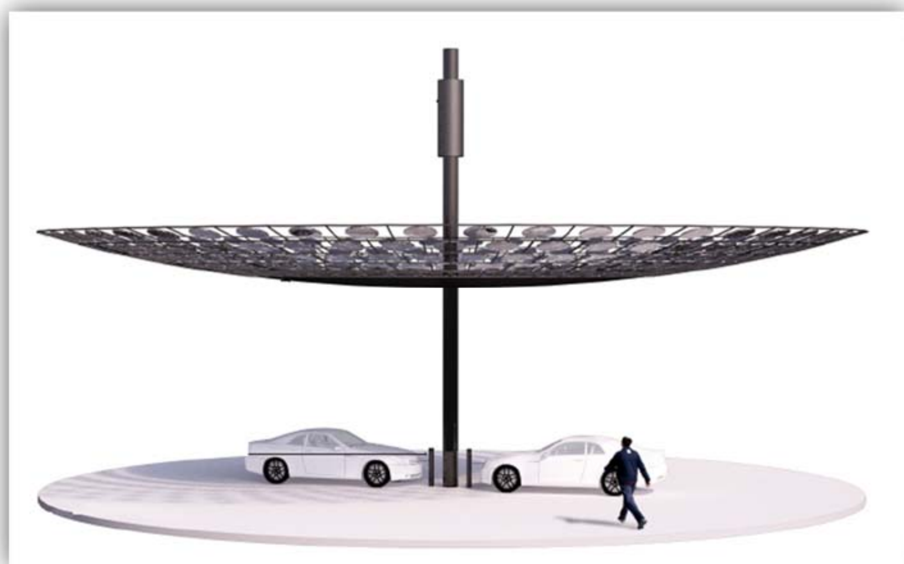


Figure 69 - Example of renewable energy generation in the Green Island

Figure 70 - Example of renewable energy generation in the Green Island

For the installation of renewable source systems, in each Green Island, the authorization procedures and the environmental assessment procedures will be identified based on the Legislative Decree 152/2006 and subsequent amendments, in addition to the measures adopted by the individual regions.

The assessments of landscape-environmental nature will be shown in the executive design, as well as the activities subject to fire prevention control.

1.5.2.1 Renewable energy systems: photovoltaic and small size wind power systems

Photovoltaic system

The photovoltaic system in the Green Island will consist of special structures, on the ground or on shelters, and will have a power that will be calculated according to the energy demand of the Green Island, as well as the dimensional features of the useful surfaces, the structural constraints and the possible presence of obstacles in close proximity.

The system connected both to the network and to a storage system, will have to include:

- Maximize the efficiency of the plant and its manufacturability: choice of the best declivity of the modules and their position compared to the south;
- Easing the maintenance through the subdivision and optimum arrangement of the modules;
- The use of the barycentric criteria for the distribution of the lines and the positioning of the electrical panel;
- The high degree of selectivity of the protections;
- The minimization of the sources of shadowing.

The components of the photovoltaic system will be:

- Photovoltaic modules and related support structures;
- Static DC / AC converter;
- Measurement and control system;
- Wiring cables;
- Electrical system and panels.

The photovoltaic module can be in monocrystalline silicon consisting of anti-reflective tempered glass of a minimum thickness of 3 mm with low iron content to optimize the absorption of solar light from an anodized aluminium frame giving solidity and strength, resistant to loads and climatic shocks. The panel must have high conversion performance, that is, a high power / energy ratio for the same inclined surface and have a minimum efficiency of 16%, a power class, under irradiation conditions of 800 W / sqm, equivalent to at least 200 WP.

In case of installation of the photovoltaic system on a shelter, the structure have to be carried out with a single laminated structural wood (fir, pine, larch, etc.) roof (GL24h type). The main structure of the shelter (pillars, beams and arched struts) is equipped with prismatic section piers, appropriately fixed with a grounded iron bracket, suitable to support:

- the joists warping in treated laminated wood with adequate section;
- the shutter planed wooden floor on a face placed on the joists;
- photovoltaic modules;
- the completion elements (roof flashings and eaves in annealed copper, etc.).

The dimensions of the roof will vary depending on the installed power. The interaxis between the pillars will be about 5.00 m. The foundation must provide a reinforced concrete abutment in appropriate section cast in place.

In the case of a concentrator photovoltaic system, the structure can be represented as follows:

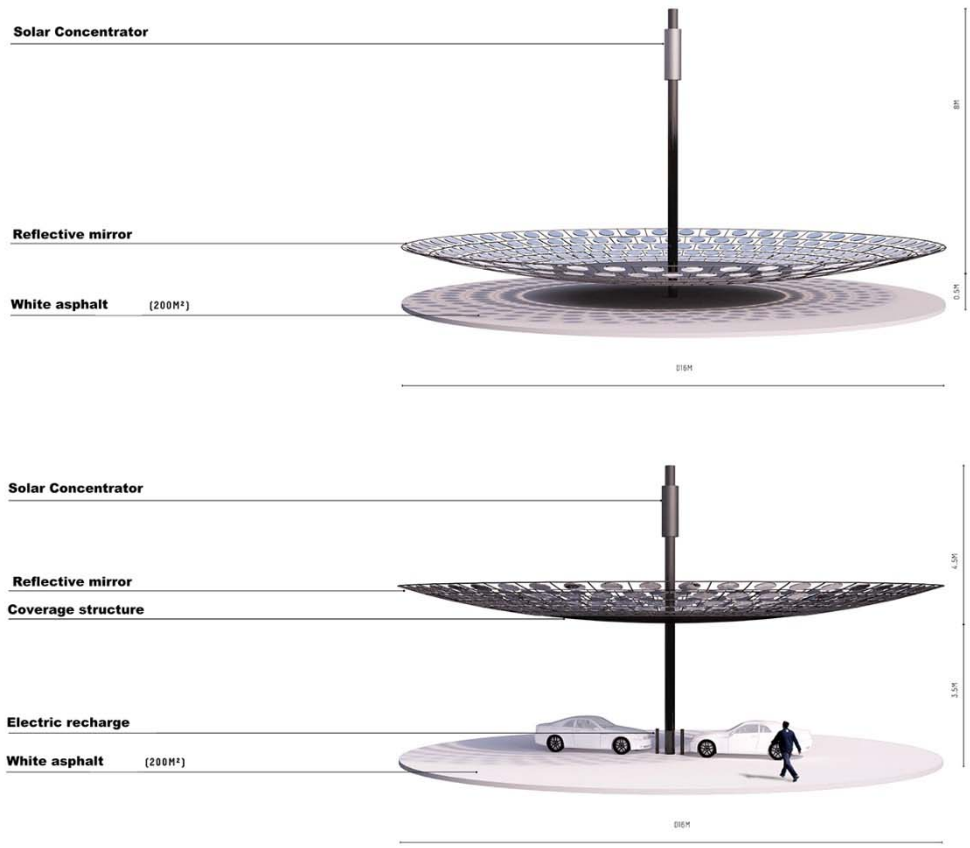


Figure 71 - Solar Concentrator

The power group, consisting of a static DC / AC converter (inverter) must be suitable for transferring the power from the photovoltaic field to the electricity grid, in accordance with the technical and safety regulations requirements. The operating range of the inverter must keep in consideration the nominal voltage and frequency values, in particular: the values of the voltage and of the input power to the DC / AC converter must be compatible with those of the corresponding photovoltaic field, while the output voltage and frequency values must be compatible with those of the network to which the system is connected.

Inside the panels, containing the individual inverters, the first protection provided is realized by the CEI 11-20. Each inverter is protected against overcurrents and short circuits by means of an appropriately sized protection device. The inverter itself is equipped with groups of measurement able to give information about the voltage and the power supplied. The connection panel to the network acts as an interface with the electricity grid.

This panel implements the second protection provided by the CEI 11-20.

The interfacing system between the photovoltaic system and the network consists of a set of protections placed between the inverter and the network, aimed at safeguarding the quality of the electricity service and avoiding dangers to people and damages to equipment.

In addition, a system must be provided for diagnostics and data monitoring, for remote control with integrated IP system and connection in modbus, via the RS485 interface. The Energy control and monitoring System must be able to evaluate the energy production of the photovoltaic system and the electricity produced and measured at the output of the inverters. The system involves the use of a data logger capable of acquiring the data provided by the inverter.

The same device is connected also to the irradiation sensor, to detect solar radiation incident on the surface of the modules, and for the acquisition of the temperature for the calibration. The irradiation sensor will be installed at the photovoltaic system and will be operated by a device, which acquires the data and sends them to the remote control center. The control and monitoring system has to allow, through a computer and a dedicated software, to query in every moment the system in order to check the functionality of the inverters and the installed modules.

All conversion, protection, switching and control equipment such as inverters, switchboards in alternating current, interface panel, monitoring system with irradiation and temperature sensors for data collection with integrated IP system and RS485 connection must be placed inside a specific technical room.

The photovoltaic system will be wired in the place where it will be installed and connected by means of cable lengths cut to size and equipped with wire terminals suitable to heading the termination terminal board of every single module. The cable-laying going from the photovoltaic field to the control device will be carried out in adequately sized PVC pipes.

The selection criteria for the cable are the following:

- Not propagating the fire
- Low emission of toxic gases

The free laying cable have to be chosen with the following features:

- Operating voltage at least up to 450/570 V;
- UV rays resistance;
- High resistance to atmospheric agents and humidity;
- High operating temperature range;
- Not propagating the fire

The choice for the electrical connection of the system components is determined by the particularity of the support structures that will be adopted.

In order to avoid phenomena related to indirect lightning, every production system must be equipped with appropriately sized Surge protector devices. The lightning, in fact, represent an important component of risk, to be assessed both for the direct effects of lightning on the photovoltaic panel, which for overvoltages generated on the system. Requirements necessary for SPDs for the realization of such a system of protection against lightning and overvoltage within the zone protection concept according to IEC EN 62305-4 are established in the IEC 60364 5-534 standard.

A protective shore network must be provided in order to allow the proper functioning of induced overvoltage surge protectors.

Small size wind turbine plant

As an alternative and / or as a complement to the photovoltaic system, in the Green Islands there will be the installation of a small size wind turbine plant. Compared to solar radiation, wind is a resource much more irregular and difficult to predict, especially on a local basis. Also the small size wind plant, as well as the photovoltaic system, have to be installed aiming at favoring the self-consumption of the produced energy.

Hence, the installation must be carefully assessed in terms of feasibility in order to ensure that it performs the expected role during its operation.

The aerogeneration system must consist of the following elements:

- support structure (foundation, tower and pole);
- containment structure (boat shaped framework);
- rotor (generation, regulation, actuation and brake);
- control panel;
- èower control and regulation devices.

The system must be equipped with an appropriate electric box of appropriate size, inside which conversion, protection, switching and control equipment will be installed.

The small size wind plant, which may be horizontal or vertical, must be able to make the most of winds with medium-high intensity (20 Km / h) and must have a minimum starting threshold of about 4-5 m / s.

The generators must be supplied with declarations regarding the nominal power (W), diameter of the rotor, sound emission, rotor speed and construction material, number and height of the blades, position of the rotation axis, total weight, wind speed for starting charging (cut-in), type of alternator, electricity produced in a month at an average wind speed of 5.4 m/s, maximum power corresponding to a wind speed of 12.5 m / s even in the 230Vac version. If the wind reaches dangerous speeds, the mechanism for appropriately limit the speed of rotation of the blades have to take over automatically. The charge controller must be separated from the body of the generator, which must be equipped with individual rectifiers of the 3 phases; and everything must be complete with dissipators for excess current, with LED lights of the power regulation and rotor brake and stop switch.

The control system must be equipped with a dedicated PLC and communication interface for remote diagnostics, integrated IP system or RS485 connection. All materials and components constituting the machine must be deprived of radioactive or chemical impact.

The small size wind turbines must be equipped with devices, called BOS - "Balance of System "which, in the case of systems connected to the network, include:

- Turbine controller;
- Static converter
- Isolation transformer
- Safety devices (generator, interface and general);
- Energy meter.

Here following, there is a single-line diagram of the small size wind power plant connected to the network with asynchronous type generator:

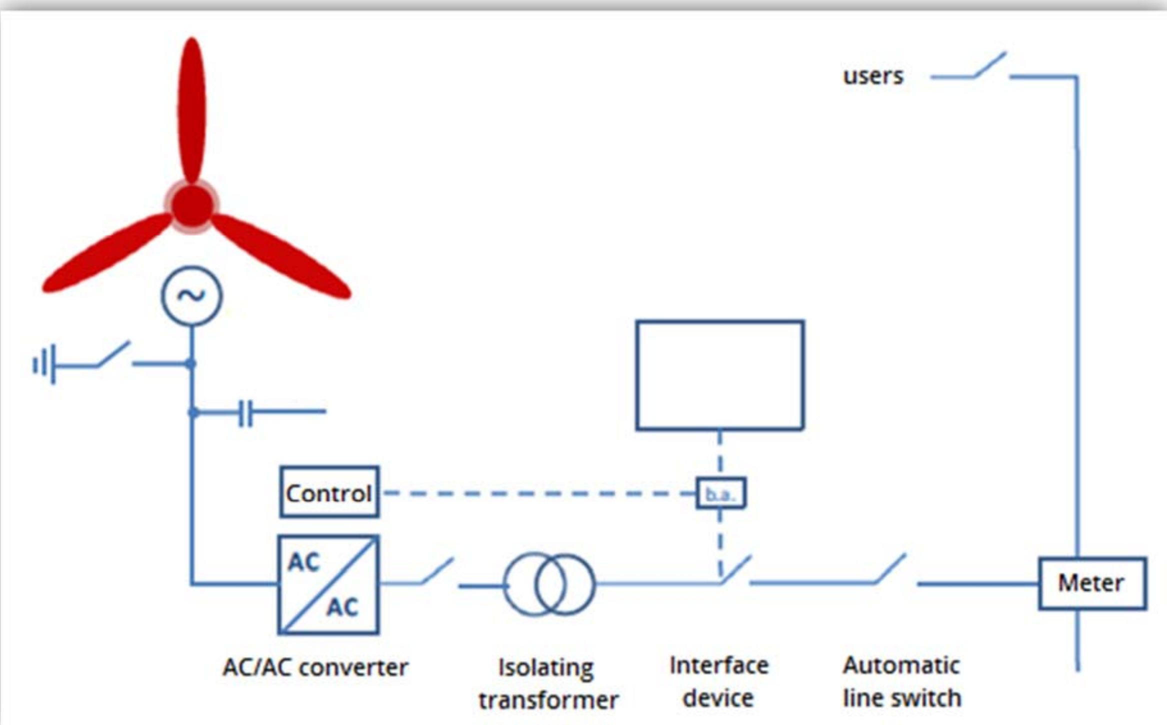


Figure 72 - Single-line diagram of a small size wind power plant connected to the network

The converter and the related control systems are electronic devices controlling the generator and converting the current in an appropriate manner to the characteristics of the network. The safety and connection devices guarantee the quality and safety of the energy going into the network.

1.5.2.2 Connection of renewable production facilities to the network

The scheme for connecting renewable energy production plants to the national, photovoltaic and small size wind system, is defined physically and electrically in a univocal way, according to the conventional scheme reported in CEI 82-25 and must include the following devices:

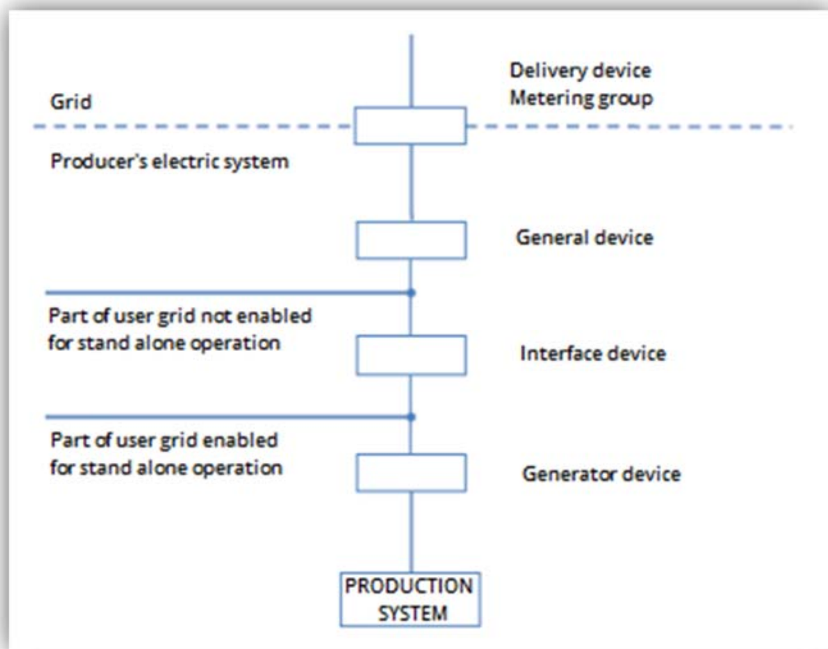


Figure 73 - Connection diagram of the production plant to the Distribution network

- The general device (DG) is a safety device that intervenes in the event of a failure of the plant or of the utilities. It consists in a magneto thermal circuit breaker that intervenes as a disconnecting breaker on all phases and on the neutral. It should be installed immediately downstream at the delivery point of the electricity and its execution must meet the requirements on connection of the CEI 64-8 standard.
- The interface device (ID) separates the production plant from the network or from that of user and consists in a switch operated by an interface protection. The ID must be "intrinsically safe", equipped with an opening coil in the absence of voltage. This coil, supplied in series with the trip contacts of the protections, must cause the opening of the device, both in the case of correct intervention and internal failure of the protections, and both in case of absence of auxiliary power supply. Its execution must meet the requirements on connection of the CEI 64-8 standard.
- The generator device (GD) is a safety device that must be installed downstream at the terminals of each generator group, in order to exclude the single group in open sky conditions. The DG must comply with the cutting requirements of the CEI 64-8 Standard.

The architecture of the electricity generation system from renewable sources, which is shown in the single-line diagram in Figure 73 provides for the connection to the LV distribution network via a general LV switchboard depicted in blue. Each generation plant is equipped with an interface device present in the related switchboard illustrated in orange. In conclusion in green there is the switchboard containing the generator device, which excludes the individual installations in open sky conditions.

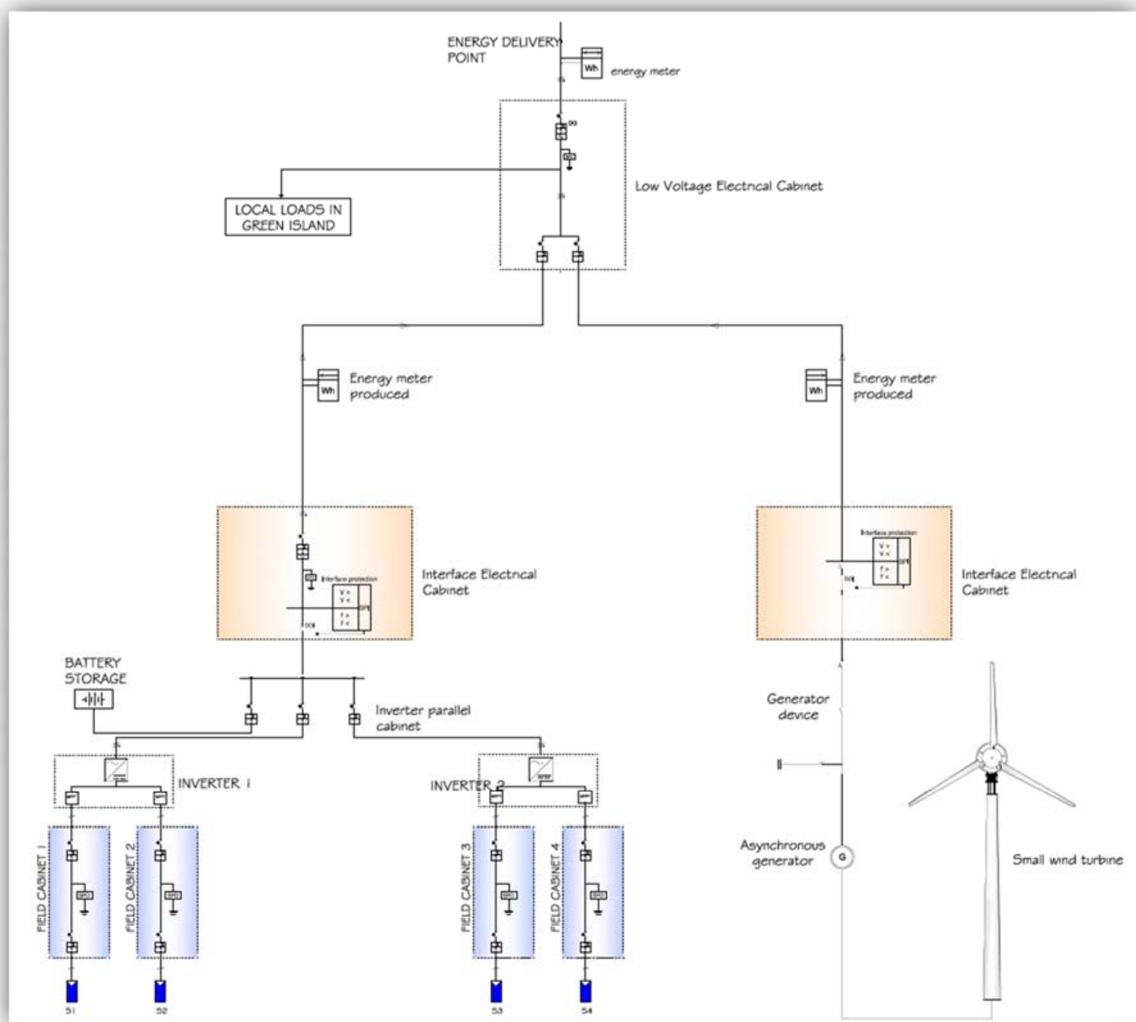


Figure 74 - Single-line diagram connection of generation plants to the network

1.5.3 Technology powerhouse

The technological powerhouse is the technical room that houses the equipment for the transformation of the voltage, supplied by the electric network, regulation and storage of the electricity coming from the renewable generation site.

1.5.3.1 Network Connection

The Green Islands are always connected to the national power grid. Depending on their location along the road / motorway section, the connection of the Green Island to the network can take place through:

- LV supply point;
- Electrical room MV/LV

1.5.3.2 Electrical room equipment

Electrical panels

Among the electrical room equipment, there are the electrical panels, which have to meet the specific regulations in force and conform to the following specifications:

- Use of insulating materials with a high degree of self-extinguishing and complete metal segregation between the individual compartments, to prevent the spread of fires;
- Solid grounding of the whole structure of the switchgear and of the extractable components throughout all the connection or the insertion;
- Minimum protection IP30 after the translation of withdrawable or disconnectable switchs;
- Elevated Insulation of all live parts;
- Mechanical and electromechanical blocks according to the design scheme of the single executive contract;
- Accessibility to equipment and circuits without risk of contact with the components in tension;
- Careful selection of insulation materials used based on low fumes emission characteristics.

The switchboards will consist of side-by-side compartments and will be completely closed and bolted together. The modularity of the compartments and of the different components will have to allow future extensions on the two sides. The various compartments must be completely segregated among themselves and compartmentalized in elementary cells segregated with metal from each other as indicated in the project drawings of the single application contract.

Each compartment must be an independent unit, consisting of a self-supporting structure in steel sheet, thickness 20-30 / 10 mm, composed of standardised elements, provided with modular drillings, put together by means of electric points and special screws that ensure robustness and electrical continuity. On this structure side and rear sheet metal closures, front doors, partition and segregation baffles, the metal supports for the different devices. The minimum thickness of the steel sheet for these elements should not be lower than 20/10 mm, observed before protective treatments. The compartments will have to be divided into the following areas:

- Front zone reserved to the cells of the power devices, for the measuring instruments and / or protections and auxiliary services; this zone is divided by individual cells that are metallically closed on all sides with modular dimensions depending on the equipment to be lodged;

- First back area, containing the derivation bars and the connections in bar of wide range switches;
- Second back area, reserved to the power connections of the switches that are normally made in cable;

The front area that houses the section of the modular conformation equipment will have to be equipped with a double front with transparent laminated glass panelling.

Consumption analyser

Inside the technology powerhouse there will be an electricity consumption analyser, able to directly and indirectly measure through measurement transformers currents and single-phase voltages, frequency, phase displacement and the power factor of the three-phase system. The internal electronics calculate all the other electrical derived parameters, such as powers and energies.

Switches

The general machine circuit breakers must be boxed or open according to threated power of the transformer. The breaking capacity must be adapted to the value of maximum power expected on low voltage distribution. User breakers of the external circuits will be boxed and or modular in mounted version. The circuit breakers supplying the powerhouse circuits must be modular in a mounted version.

The abovementioned breakers must be suitably coordinated with each other in order to guarantee the selectivity, the protection of the circuits and calibrated according to what is indicated in the design schemes of the single application contracts. The breaking capacity of the circuit breakers must be at least equal to the three-phase power surge current calculated on the busbars of the LV panel. In some cases, the breaking capacity of the circuit breaker may be lower than the power surge current abovementioned, if there is a upstream device:

- which has a breaking capacity corresponding to the short circuit current above determined;
- which limits the specific energy passing to a lower value than the one which can be tolerate by the automatic breaker and the protected conductors.

Main busbars and subpanels

The main bars and the subpanels must be in bare copper electrolytic plate (ETP UN1 5649-with rounded corners, appropriately sized and floated to support the thermal and electrodynamic stresses due to power surge currents. Insulation must be completely realized in air; the busbar supports must be carried out using componentized elements molded in self-extinguishing insulating material with high resistance mechanics and non-marking specifications.

The form of segregation must be the one provided for in the project documents of the single executive contracts. For the cooling of the busbars area, the front panel has to be equipped with louvers at the bottom and in the lower part of the closing rear panel. For the hot bleed air there will be dedicated louvers on the roof.

Auxiliary circuits and wiring

The auxiliary equipment must be arranged in cells separated metallically from the circuit breakers cells. It should always be possible to access the auxiliary equipment with the power grid under tension. The internal wiring must be carried out with flexible cables non-propagating the fire (sec. CEI 20-22), with a section no lower than 1.5 mmq for auxiliary circuits and 2.5mmq for power circuits.

All connections must be carried out using compression cable terminal, and each conductor must be numbered with appropriate marks.

The conductors must be housed on dedicated plastic channels and in special spaces inside the compartments. All conductors must refer to numbered modular terminal blocks. Appropriate pantographic plates facing the panel, must indicate each equipment and the related sequence of maneuver. All status indicators and commands of each equipment must be repeated to the terminal block in order to be used for the remote control and the tele control from the Operations Center.

A copper busbar, with a nominal section of 200 mm^2, will have to cover longitudinally the whole power grid; all the main components must be connected to such a bar. All the elements of carpentry will have to be solidly connected to each other through special screws in order to ensure a satisfying electrical contact between the parts. The doors must be equipotentially connected to the structure by means of copper plaited bands having a section of 16 mm^2.The paint job cycle for low voltage switchboards must be completely similar to the one envisaged for medium voltage switchboards. Series of accessories to be supplied:

- Support shelf, several levers and handles;
- Lifting eyebolts;
- Touch-up paint for damaged spots;
- Diagrams and design drawings of the single executive contracts;
- Instructions for installation, operation and maintenance of the panel;
- Equipment identification plates;
- Single-line diagram supplied to the carpentry;
- Accident prevention posters in compliance with Legislative Decree no. 81/08 and the Leg. Dec. 626;
- Type testing;
- Ordinary and extraordinary maintenance manual.

Energy Storage

The energy storage must allow to store the energy produced by renewable sources plants and must be appropriately sized for the self-consumption of the Green Island.

The battery pack must consist of elements connected on in series or in parallel branches and must meet the following regulatory requirements:

- IEC 61427;
- DIN 40736 and DIN 40742;
- DIN 43539T5;
- DIN 40740;
- IEC 60896 part 11-21-22.

The main characteristics for storage systems must be:

- Continuous operation in order to guarantee a constant ability to accumulate or supply electricity in large and small quantities;
- Power supply sufficiently large;
- Long lifetime in cyclic operation;
- Low maintenance in operation.

In order to prevent the overload phenomenon, the battery pack must be equipped with an electronic charge controller (control unit) series / parallel type, whose function is to block the charging process when too high cell voltages are reached. In order to avoid, instead, the excess of discharge of the battery pack, with the related risk of sulphation of the single elements (in the event that a subsequent charging does not occur), the regulator will have to stop the withdrawal of electricity, if the voltage of the element drops below a certain level. The charge regulator moreover, must be able to take into account the temperature variations in order to avoid on one hand lower capacity effects (low temperatures), on the other side greater self-discharge effects due to the speeding up of chemical reactions (high temperatures).

The positive tubular plates and the negative grid plates of the battery pack must be isolated one from the other through microporous separators, or must be obtained from alloys rich in tin and poor calcium; this gives the battery pack a good resistance to the cycles of charge / discharge, low self-discharge, low maintenance and long lifetime. The battery pack must be equipped with an additional glass fiber envelope, whose function is to enclose the positive electrode and prevent internal power surge phenomena. The efficiency of the battery pack must be at least equal to 0.83 and its duration must correspond at least to 10 years. In order to preserve the battery pack it is necessary to check periodically the electrolyte.

Emergency power supply: generator set

In case of lack of electricity from the network or unavailability of the renewable energy source or exhausted storage, a generator is provided for the emergency power supply, which must guarantee a full load autonomy of at least 24 hours. The generator set must be installed in environments built according to the specific fire prevention provisions, with natural ventilation directed outward, or directly outside protected by a special hood. The generator set must be laid on a special base made of concrete. The generator set will have the following general characteristics:

- power factor 0.8;
- frequency 50 Hz;
- voltage 400/231 V Three-phase;
- rotation speed 1,500 rpm

The generator set must be delivered with a lead-acid battery for heavy-duty with 12VDC / 155Ah of power supplied for electric starting and 12VDC circuit. The battery is mounted on a metal platform positioned in the internal profile of the base. The terminals of the battery are connected to the engine by means of flexible cables.

It will have to be three-phase, self-regulated, self-excited, and synchronous, without brushes, 4 poles.

A control unit that automatically launches the Generator Set must be provided, when all the conditions are met, it closes the Generator Set, and then stops the engine by external signal or by pressing the mushroom-head button.

Ground system

The ground system of the electric powerhouse must be carried out with an earth collector characterised by a ring in copper or galvanized steel plate 30x4 mm plate. The ring must be connected to the electro-welded mesh present in the foundation slab at least at the corners of each room. All metal parts and the powerhouse equipment must be connected to the collector of cabin. In particular:

- metal doors and windows;
- carpentry of electrical panels;

- transformer housings;
- neutral point of the transformer (s);
- transformer rails;
- cable trays and metal raceways (if necessary).

The ground connections of moving parts must be made of copper plated bands having a minimum section of 50 mm^2. The collector will then be connected to the external discharge device through at least two ground conductors having an adequate section. The discharge device will possibly consist of a ring along the perimeter of the powerhouse, made of 35 mm^2 bare copper rope (minimum section) or other equivalent material. The discharge device will be integrated with vertical elements (spreaders) and will be connected to the reinforcing rods of the foundation.

1.5.3.3 Anti-theft system and cable monitoring

The utilities served by the supply powerhouse are connected with aluminium cables; these have to be placed as far as possible in a protected location and / or in stainless steel ducts. While observing the laying prescriptions and the passage of the cables provided for, a special attention must be paid to the verification of the cables themselves, understood as "presence of the cable" and "cable degradation".

These two factors are important and fundamental for guaranteeing the safety of the road sections, as it is necessary to know in advance whether the power supply system is available. For this reason, we have to provide and install for each "sensitive" user a system guaranteeing constantly the monitoring of the connection between the utilities provided on the Smart Road.

The purposes are to monitor the systems and communicate any anomalies of the plants, in the following ways:

- Presence of the cable: the state of the cable and therefore its presence in the plant is constantly checked, both during normal operation and during user inactivity.
- These controls are measures dictated by the occurrence of more and more frequent thefts of cables on the plants. The device must be able to verify in real time a possible cable theft for a rapid reaction. In order to give better information to the control room and law enforcement, the system will have to guarantee to identify within 250 meters the cutting point of the cable itself, reporting the data to the control center.
- Cable degradation: the system must be designed to check that the status of cable operation is correct and efficient to ensure the safety of the service. A degradation of the insulation characteristics or a problem on the cable can cause serious disruptions in the energy distribution system. The device must be able to determine the degradation values of the cable and, through an appropriate algorithm, to plan a preventive intervention for repair and / or replacement of the damaged cable.

The operation of the system must also allow a preventive maintenance of the systems that in terms of time and burden is much more advantageous. The objectives of the evolved system, including the optional part, must be the following:

- verify that the cables installed in the system are present and have not been stolen by delinquents;
- periodically perform in automatic mode the measurement of the insulation resistance of the cables with respect to the ground; this function allows to obtain a photographic picture of the state of the cables, allowing intervention in advance of a hypothetical degradation that would create downtimes or system malfunctions;
- measure the electrical parameters of the users, in order to draw a consumption map to plan appropriate actions and / or adequate functionalities to improve energy efficiency;

- Energy sending alarms to the local control center according to a programmable configuration.

Generate technical alarms:

- lack of power supply to the panel;
- intervention of the magneto thermal circuit breakers;
- intervention of the residual current devices (RCDs);
- remotely: reset items and switch on / off circuits.

The device must be implemented in an insulating container with IP 54 protection rating, suitable for being assembled inside the electrical switchboard. A functional display must also be provided for the detection of all electrical parameters and a series of leds necessary for checking the state of the communication with standards opened towards the local control center.

Regarding the protection against theft of equipment located in outdoor areas they will be dissuasive and protective measures such as:

- video surveillance system for Green Island service area monitoring;
- burglar-proof system of the wells on the service area and ongoing by filling them with layer of sand and concrete, after injection of cement mortars within the cable ducts;
- anti-intruder system for powerhouse and technological rooms access control;

Each powerhouse e will also be equipped with a special anti-intruder system, which should be installed inside, and including the following devices:

- central for anti-intruder systems with 8 inputs expandable to 16 inputs with integrated telephone dial and ready for GSM operation;
- telephone interface with GSM / GPRS module for tele-manageable anti-intruder system;
- high tolerance aluminium magnetic contacts mounted on sight;
- outdoor volumetric detectors with two MV channels and two PIR channels with quadruple technology and range up to 15m;
- type 2x0.50 + 4x0.22 shielded alarmed cable.

This system will be integrated with the installation in the powerhouse rooms of two-door metal doors (cm 120 x 215) with HB lock.

The video surveillance functions, the signals deriving from the sensors and the alarms generated by the anti-intruder system will have to be interfaced with the RMT system of the CCR.

1.5.4 Ongoing distribution of electricity

For supplying the ongoing distributed loads in itinere, such as multi-purpose stations, three-phase output electricity from the 400 Vac low-voltage general panel, is converted in 1000 Vac using a step-up transformer, in order to maximize energy efficiency and guarantee lower management costs. The 1000 Vac distribution system will be of IT type and will allow:

- Not automatically interrupting the power supply when a first fault occurs;
- Automatically shutting off the power supply when a second fault occurs, with the first one not secured yet, adopting similar prescriptions to GTG systems, since the ground systems of each power station are independent.

For this reason, a three poles protection without neutral must be installed downstream of the 400/1000 Vac transformer.

400V/1000V transformer

The voltage boost transformer, positioned downstream of the general low voltage panel, must be able to receive an input voltage of 400 Vac and increase it to 1000 Vac for the distribution towards users located on the road. The transformer must be carried out according to the Reference standard EN 61558-2-4, and it must be located in a special containment box.

There will be the installation of two step-up transformers of the same size, one of which with a function of backup.

The distribution of energy to multifunctional stations is carried out, through two 1000 Vac backbones about 15 km long, which feed the loads distributed on the right and left with respect to the position of the "Green Island". The supply voltage is transformed from 1000 Vac into direct current at 12/24/48 Vdc through an energy station. The maximum power installed in each multi-purpose station is equal to 60.

Energy station

The energy station must be positioned at the ongoing multi-purpose stations and must have the ability to withdraw a 1000 Vac input voltage directly from the backbone to and, through an internal rectifier, convert it to 12/24/48 Vdc, in order to feed in direct current the devices present on each multifunctional station, such as:

- Access point for Wi-Fi system in motion 2.4 / 5 GHz;
- Road Side Unit for Wi-Fi V2I system;
- Intelligent CCTV;
- Weather station

Through the battery pack, placed in buffer with respect to the users, the continuity of the supply voltage, instantly compensating for any blackouts and / or operational anomalies are guaranteed. Its features are:

- Voltage: 12V
- Minimum capacity 5 Ah
- Minimum autonomy 30'

The monitoring of the energy station must be carried out with a remote software or locally using the RS232 and / or RS485 or Ethernet communication ports which have to be provided to the station.

A synoptic panel displays on a display and selectable through a keypad all the parameters of the energy station and of the single power supply modules of which it is composed. This unit includes a microprocessor control whose task is to manage the display, the electrical parameters, the alarms, the serial interface RS232 and / or RS485 and of the LAN. In case of excessive discharge of the battery it shall disconnect them avoiding to damage them. The microprocessor manages also the alarms when they are present, providing for their visualisation on the display, the dispatch of alarm messages via the RS232 and / or RS485 or LAN interface and, at the same time, by closing the corresponding alarm contact.

1.5.5 Electricity distribution in the Green Island

From the general low voltage panel of the technological center, the 400 Vac three-phase electric energy is distributed to supply local loads of the Green Island, such as:

- Systems in the technological room.
- Exterior service area lighting;

- Recharge of electric vehicles;
- Recharge of drones;
- Intelligent truck parking.

1.5.5.1 Charging stations for electric vehicles

Inside the Green Island recharge stations of a type "slow recharge" alternating current and "fast charge" in direct current, which will be used for charging the electric vehicles of the Anas park. Each station will be equipped with at least two sockets for charging and therefore, for each of them, two parking stations will be identified to be reserved for the aforementioned electric vehicles: it will therefore be possible to charge simultaneously two vehicles. Supply of the charging stations will take place both from the photovoltaic field and from the electricity grid.

Figure 75 - Local distribution of energy for charging electric vehicles

The power supply will be single-phase and three-phase, with maximum output power up to 22 kW for slow recharging and up to 50 kW for fast charging, which can be even partialized up to 60% of the output. The charging station will have:

- Type 2 charging sockets with shutter (IPXXD for protection against accidental contact of live parts) and mechanical cable retention system while charging.
- Automatic reset device and integrated automatic periodic test for the warranty of the continuity of service even in case of untimely pressure of the differential device and for the automatic periodic verification of the proper operation of the differential device, for the safety of people and things;
- Graphic LCD display for user interface and with RFID card reader for enabling / disabling users;
- MID energy meters for metering the energy supplied;
- OCPP protocol by using web services (SOA) and with an Integrated communication interface RS485;
- Possibility of a network (local and remote) management of the system monitoring products.

1.5.5.2 Drone charging stations

In each Green Island, there will be recharging, stopping areas for drones, which will allow monitoring road traffic in strategic points for traffic and allowing planning, and efficient managing traffic flows along the road.

The area inside the Green Island dedicated to the drone consists of a box system housing the drone and the devices required for remote control, which can also supply its electric charging (as shown in the following Figure).

The landing platform is square and can host the largest models of drones existing on the market, having side of about 2 meters, for their safe landing and for reloading them.

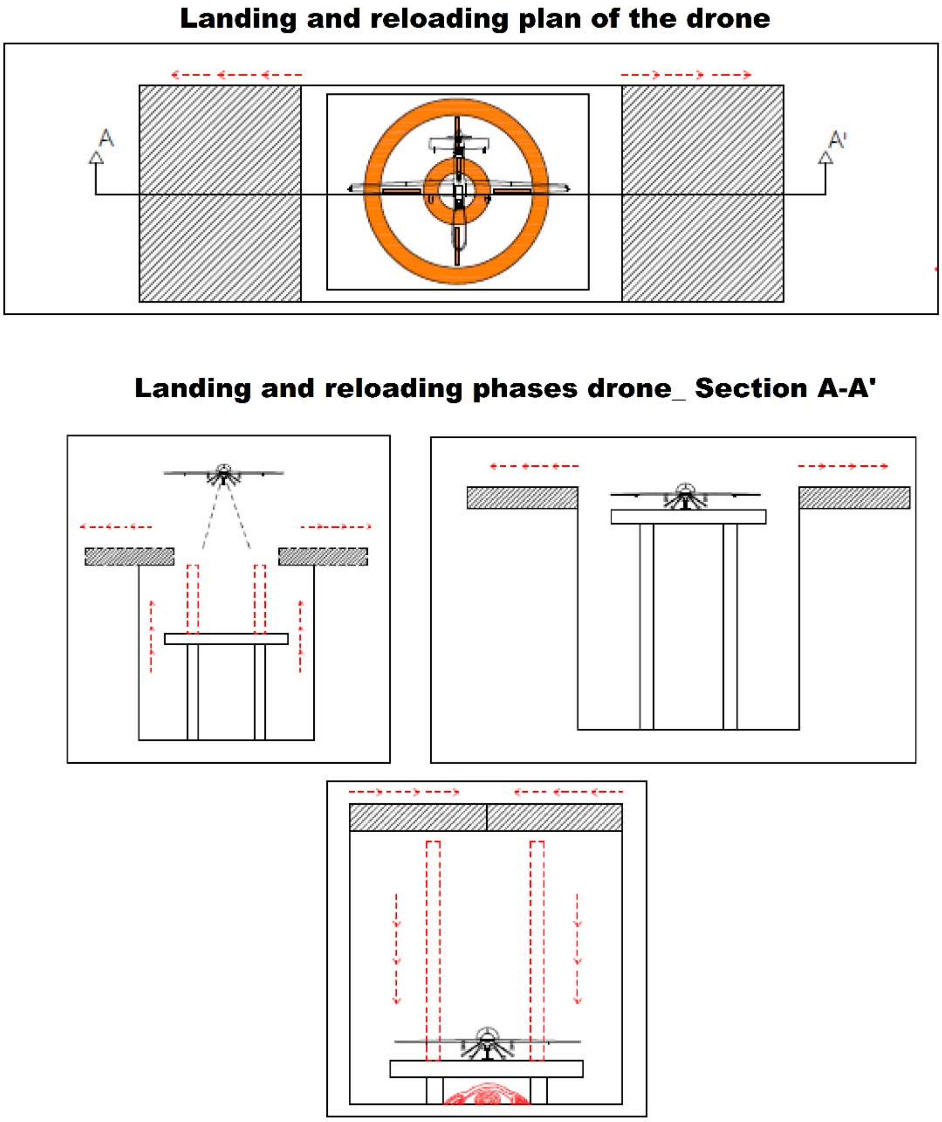


Figure 76 - Accommodation box and drone recharge

Li-Po (or Li-Poly) batteries, lithium ion polymer type battery elements from which the abbreviations in the name are born, provide the power supply of the drones.

Li-Po batteries have a nominal voltage of 3.7 volts per cell and in some cases on small size drones size, a 3.7 Volt Li-Po cell is enough to supply the model and make it fly. The normal Li-Po drones batteries have at least two or more cells connected in series to provide higher voltages and for large dimensions drones, which require a lot of power, the number of cells can be higher than 6.

Once the drone has landed, a subsystem recharges the battery through a mechanical arm that uses different standard of USB charging, plug-in system or through an induction system. When the recharge has been completed, the drone can be used or is hosted in the dedicated box that closes to ensure complete protection of both the drone and the necessary devices for remote control.

The automatic drone charging system is intelligent and dedicated to charging exclusively the batteries Li-Po: the charging system is able to control not only the state of the charge but also its voltage so that during charging each battery cell never exceeds 4.2 Volts, correctly balancing the charge of the cells.

1.5.6 Types of cable laying

1.5.6.1 Ongoing

The ongoing type of laying of the cables is supposed to be below ground. The electric cables can be laid in piping. A special monitor tape will signal the piping containing the cables. The sheath must protect the cable from laying stress and the mixture that compose it must be anhygroscopic, it must be able to defend the cores against the contact with water. The piping containing the cables must be interrupted by wells of suitable size to allow a simple threading of the cables, as better defined in the graphics.

In this case, cables with aluminum conductor type ARG16 (O) R16-0.6 / 1 kV must be used. In compliance with the bending radii established by the manufacturer and, as far as possible, the pipes of a duct, which belong to the same well, must be aligned with each other. The towing force required during the threading (Standard CEI 11-17) must be applied on the conductors and not on the insulators of the cable and must not exceed 60 N / mm2 referred to the overall section of copper conductors (50 N / mm2 for aluminum conductors). Rolls can be used to facilitate pull-in operations for towing that allow to reduce the necessary effort while avoiding damage to the cables themselves.

If an energy cable is laid near other cables, metal pipes, tanks fuel tanks must meet special requirements and be installed respecting Minimum distances. In particular, in the intersections with underground cables for telecommunications, the space between must not be lower than 0.3 m and the signal cable must be protected for a length of at least 1m through a cable run, a tube or a metal box having a thickness of at least 1 mm. If it is not possible to respect this minimum distance, it is necessary to protect the energy cable with the same criteria.

When the minimum distances cannot be respected, the telecommunication cable must be protected with a metal tube or cassette and, if the distance is lower than 0.15 m, an additional protection must also be provided for the power cable. In the intersections with metal pipes, the energy cables must be placed at a minimum distance of 0.5 m, which can be reduced to 0.3 m if the cable or metal pipe are contained in a non-metallic casing.

The protection can be obtained through slightly reinforced concrete or through a non-metallic separator item such as a slab of concrete or other rigid material. In the presence of connections directly on underground cables, the metal pipes must be at least one meter far from the crossing point or the abovementioned supplementary protections must be adopted. In the parallelisms, the energy cables and the metal pipes must be separated by a distance from each other lower than 0.30m.

In the presence of tanks containing flammable liquids or gases, safety distances not less than 1 meter from the outer surface of the tank must be adopted. The same requirements, indicated for the metal pipes, also apply to underground gas pipelines: both at intersections and in parallelisms the space between must not be lower than 0.5 m.

Safety distances with energy cables that are laid in pipe or conduit in the presence of pipes for the transfer of flammable fluids are set by the Ministerial Decree of 24/11/1984 "Safety fire protection regulations for transport, distribution, accumulation and use of natural gas with density not exceeding 0.8 "and must from time to time be agreed with the gas distribution stations.

1.5.6.2 In tunnel

All cables in the tunnel with regard to fire behavior must be CE marked according to EN 50575 of flame-retardant type, halogen free and low emission of opaque fumes, toxic and corrosive gases, according to the CEI 20-45 Standards, CEI EN 50363-0, IEC 60228, IEC 60332-1-2, IEC 60754, IEC 61034, CEI 20-37 / 4-0, IEC 60331-2, IEC 60331-1, CEI UNEL 35016 Cca - s3, d1, a3, CEI 20-29. In this case, cables with an aluminum conductor of the type ARTG10 (O) M1 0.6 / 1 kV and ARG16 (O) M16 0.6 / 1kV must be used.

The cables laying in the tunnel will be in visible cable ducts (cable trays, pipes, protective channels, etc.) and must be implemented with stainless steel with an AISI (Internal Intelligence and Security Agency) characteristic of at least 304, or materials with equivalent services. The cable trays systems can be with or without cover. For cable laying, we have to take into condsideration the reference standard concerning cable trays: that is CEI EN 61537. A particular attention must be taken during the installation phase to support and fastening systems of the pipelines for the purpose of functional maintenance even during ordinary operations.

1.5.6.3 Bridges and Structures

In case of laying on suspended structures (bridges, viaducts, overpasses, etc.) which do not offer the possibility to carry out excavations, the cables must be laid on a cable run or metal pipe. The cable runs or pipes must be appropriately fixed to the support structure through galvanised iron brackets placed at a distance lower than 150 cm. In correspondence of expansion joints of the structures, you will have to provide for the installation of suitable expansion systems (telescope compensator).

In this case, cables with aluminum conductor type ARG16 (O) R16-0.6 / 1 kV must be used.

1.6 Smart services

The ANAS Smart Road will allow a proactive use of integrated technology inside the infrastructure, increasing its resistance and optimal management, as it can vary performance characteristics based on precise inputs. Furthermore, it will allow fruition by the road users of value-added services that will lead to an extended customer experience whose benefits will be tangible: first of all the increase in security, given above all by the higher levels of automation, connectivity and continuous monitoring of road infrastructures, moreover the possibility of providing users with real time information about dangerous events via mobile device and, in the future, through the Car Head Units (devices that are already installed in the cars of the main car manufacturers).

1.6.1 User information

The services that can be activated vary from those aimed at the operational management of traffic, enabled by the performance analysis, of scenarios and forecasts of the vehicle flow that only a digital road is able to offer efficiently, up to including the management of emergencies and of criticality in real time.

Some examples of information / services that can be provided to users are:

- **Security-related information**: the infrastructure will be able to communicate with vehicles (mainly through mobile devices and later, with the expansion of technology, through the devices installed directly on the vehicle) signaling, through visual and sound alerts, for example the presence of generic dangers along the road (accidents, stray animals, vehicles which are stationary on the roadway, objects, rock falls, sudden traffic jams after a curve with poor visibility, etc.), the distance on the emergency lane and / or the excessive approach to side barriers. The infrastructure will also be able to understand situations potentially dangerous by signaling, for example, sudden braking in preceding vehicles thus avoiding chain accidents, sending an alert in case of exceeding the speed limits or without the observance of the safety distances, indicating the dangerous points along the track (such as dangerous curves, ice formation, junctions and intersections, etc.) and possible skidding of both the preceding vehicles, and of the vehicle subject to skidding (to avoid drivers falling asleep). The infrastructure will also be able of tracking the rescue vehicles so as to inform users in real time about their arrival times and distance;

- Traffic information: all conditions such as delays, gridlock, presence accidents, construction sites and in general all information that may cause a traffic event will be provided in real time to users. Such information will be provided integrating conventional communication systems (variable message panels, radio bulletins, etc.) with the new I2V communication systems. Thanks to the Smart Road, it will be also possible to provide users with alerts related to road intersections, roundabouts, junctions, etc. that inform the user about the next state of the intersection and the arrival of cars from other directions;
- Meteorological information: information related to the presence of fog that obstructs the visibility, ice, critical weather conditions, etc. Exceptional meteorological events could also make circulation with chains / winter tires, or cause any temporary traffic prohibitions and / or alternative roads;
- Information on alternative routes: in case of traffic events or adverse weather conditions, information will be immediately provided about the deviation of traffic flows on alternative itineraries with a view to suggesting the optimal route. The Smart Road system will also be able to calculate interventions on average speeds (speed control) and suggest trajectories and lanes (lane control) in order to avoid the persistence or the formation of new gridlocks;
- Management of emergency situations through "SOS on board": it will be possible, in case of difficulty, to send distress call directly to law enforcement, to the ANAS Operations Room or request assistance for vehicle breakdowns;
- Information concerning the services provided by the rest areas along the route: refreshment points along the route, services offered in service areas (Wi-Fi, possible shops, special assistance, etc.); fuel prices, electric charging points (with possibility to book the recharge and billing of consumption directly via mobile device), the presence of vehicle repair shops, etc. will be indicated. Thanks to the technology platform, making use of crowdsourcing, it will also be possible to update data through the community: users will have the opportunity to report any change in the services offered, in fuel prices, etc.
- Information about points of touristic interest along the route: tourist routes, indications of places of interest, etc. The distances and journey times, will be indicated in order to offer a customer experience as complete as possible;
- Information reserved to heavy vehicles: in order to maximize security, a particular attention will also be given to the circulation of heavy vehicles, looking as much as possible to avoid dangerous situations both for the vehicle itself and for other vehicles. For this purpose, it will be possible for example, to monitor the time spent driving and send an alert to the driver in case of its excess (a feature which can be extended to other users of the road), alert in case of travel on not dedicated lane, alert in case of excess of the size or weight allowed for a specific type of heavy vehicles, etc. Furthermore, it will be possible to provide value-added services such as: reservation service for ITP (Intelligent Truck Parking), SmarTruck service (a service designed for transporters allows to program trips, get to know position, regularity of travel and estimated time of arrival of the vehicles, as well as interacting with the logistics centers and giving in advance them the transport documentation), goods loading / unloading services in defined areas reserving them, truck platooning, reporting of time slots for circulation and signalling in case of loss of cargo or transport goods. Finally, thanks to the Dangerous Goods service, all the users in the vicinity will be informed about the transport of dangerous goods by a heavy vehicle or more simply the presence of towing or trailer vehicles (boats, caravans, etc.).

The above services should be considered as examples of the potentiality of the Smart Road and the vastness of information that can be communicated through a common mobile device: it is understood that some of them are of immediate implementation, for others it will be necessary to wait for a greater diffusion and maturity of technologies.

Figure 77 - Example of user messaging

Figure 78 - Example of user messaging

1.6.2 User information

In an effort to find a balance between Big Data and Privacy, ANAS considers it essential to apply the principle of privacy by design: a transparent approach that allows users to understand the reason why the data concerning them are collected and how they will be used as well as a high degree of user control over the same data (unconditional possibility of opposition to transfer and processing of the data).

Figure 79 - Type of possible data collected by users

Data that could be collected by users in order to create a repository that allows data processing for statistical purposes are:

- Speed;
- Acceleration/Deceleration;
- Geolocation (through the position provided by the GPS);
- Orientation (through the magnetic sensor);

- Inclination (using the gyroscope);
- Telephone operator and type of cellular network (3G, 4G);
- Language / Country of origin;
- Make and model of the mobile device;
- Operating system version;
- Telephone number and IP address;
- Proximity sensor;

The uses that can be made of such Big Data (as the volume of the Big Data, the variety of sources from which they come and the speed with which they will be processed can be considered), will be destined to the use in the processing of traffic estimates and the provision of services previously analysed.

However, the collection and storage of sensitive data and the ability to analyse individual and collective behaviours by processing billions of information in real time is undoubtedly a potential threat to confidentiality. Therefore, as indicated by the European Data Protection Supervisor for the Protection of Personal Data regarding their management, ANAS will acquire them, process and use them in compliance with the provisions of the current legislation on privacy without the possibility to transfer them to third parties, thus ensuring non-disclosability. Statistical data, about traffic and events necessary for the management of traffic and infomobility, will also be made available on the channels of interoperability already existing with the CCISS (Road Safety Information Coordination Centre). The possibility of transferring to third parties only the aggregate data that can be used, anonymously, for statistical purposes (traffic data, mileage, times, events, etc.) will be assessed.

Currently, the possibility of granting advertising space (exclusively related to value-added services for the Smart Road user, such as information and offers on service areas along the route) and access to specific services dedicated to third-party companies (for example services dedicated to logistics operators) are under preliminary evaluation but there are no plans to activate them in the first planning phase which is focused on ensuring greater road transport safety and on the improvement / enrichment of the infomobility service to road users.

These measures represent a real strategy that will maximize the advantages of the digital road while ensuring the protection of user privacy.

1.6.3 Intelligent Truck Parking - Rest areas for heavy vehicles

The Smart Road project provides for the improvement of the safety of road hauliers and their goods through ITS (Intelligent Transportation Systems) applications: along the road parking and long-term parking areas dedicated to heavy vehicles and commercial vehicles for the transport of goods called Intelligent Truck Parking (ITP), will be implemented with surveillance, information and reservation services.

For this purpose, as regards to the IoT sensors, in the rest areas for each stall a smart parking sensor will be installed, able to determine the state of a parking (free / busy) and consequently to detect the arrival and departure of a heavy vehicle from the parking area.

The security issue, understood as security, in the road haulage sector is mainly connected to theft of cargoes and the attacks against drivers, which occur, mainly in rest and service areas. Another important theme is related to the requirement of mandatory respect of the rest provided by law for hauliers, who currently, at night, improperly stop in inappropriate areas (lanes of acceleration / deceleration of service areas, rest areas) with obvious road safety risks.

The areas dedicated to heavy vehicles will also be used to manage particular emergencies such as accidents and particularly adverse weather conditions.

Primary objectives that the Intelligent Truck Parking (ITP) service offers are:

- Definition of a standard in line with the European one for the safety of rest areas reserved to heavy vehicles;
- Creation of "model" parking areas, including automated stalls with the possibility to book them and the accessory services available (such as surveillance, medical attention, power supply of refrigerated vehicles, repair shops, etc.)
- Development of a reservation system, parking guide and information related to all the types of staging areas for heavy vehicles under Anas management, through a free access gateway with information about all ITP areas along the road arteries. The gateway will allow consulting the following information: ITP area location, size and services of the area, availability of stalls; possibility to book the stalls online, access to the area and to the stall booked for a certain time slot through online booking; generation of a QR Code, necessary to access the protected stall.

It is particularly important the last point that will allow, by entering a location, the number of a motorway or an itinerary, to display an interactive map on the screen presenting the list of all the ANAS ITP parking areas. You can filter search results based on several criteria for knowing, for example, whether the rest area includes surveillance services, medical assistance, power supply of refrigerated vehicles, repair shops, etc.

The stalls indicated as "bookable" are marked on an interactive map with the letter "R", and can be immediately booked via Internet, with any device or from a computer on board of the vehicle: the possibility to reserve a place in the ITP parking from the user allows him to avoid long researches to check the availability of rest areas and to optimize travel and parking expenses.

The procedure that the driver or planner will have to follow for the booking is the following: after having logged in, the user can choose a free rest area along the journey segment or in a specific location, then enter the date and time of arrival and departure provided, and finally confirm: the system will send an e-mail and an SMS message confirming the reservation with all relevant data (name, location of ITP area, stall reservation number, name of the contact on-site). The registered user will have the possibility to reserve a place, depending on availability, several days in advance or just before arrival.

2 The regulatory context

The regulatory scenario of intelligent transport includes a large and fragmentary regulation, the main guidelines for the Smart Road are shown below.

Regulations and European Directives

DIRECTIVE 2010/40 / EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 July 2010 on the general framework for the deployment of intelligent transport systems in the road transport sector and in the interfaces with other modes of transport.

Commission White Paper on "Roadmap to a Single European Transport Area - For a competitive and sustainable transport policy ", with which the European Commission has adopted a global strategy (Transport 2050) for a competitive transport system able to increase mobility, to remove the main obstacles in the main areas and to fuel growth and employment. At the same time, the proposals will drastically reduce the dependence of the Europe on oil imports and carbon emissions in transport will decrease by 60%within 2050.

COMMISSION DELEGATED REGULATION (EU) No 305/2013 of 26 November 2012 which integrates the Directive 2010/40 / EU of the European Parliament and of the Council as concerns the harmonized preparation throughout the European Union of an electronic service of interoperable emergency call (eCall).

COMMISSION DELEGATED REGULATION (EU) No 885/2013 of 15 May 2013 integrating the directive 2010/40 / EU of the European Parliament and of the Council on intelligent transport systems, with regard to the provision of information services for safe parking areas for heavy goods vehicles and commercial vehicles.

DELEGATED REGULATION (EU) No 886/2013 OF THE COMMISSION of 15 May 2013 integrating the Directive 2010/40 / EU of the European Parliament and of the Council as concerns the data and procedures for the provision, where possible, of road safety related minimum universal traffic information free of charge to users on roads connected to road safety.

DELEGATED REGULATION (EU) No. 962/2015 OF THE COMMISSION of 18 December 2014, which integrates the Directive 2010/40 / EU of the European Parliament and of the Council as concerns the provision of real-time traffic information services throughout the European Union.

A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperatives, connected and automated mobility Brussels, 30.11.2016 COM (2016) 766 final. The European Commission issued, on August 5, 2008, the Decision 671 as concerns the harmonised use of radio spectrum in the 5875-5905 MHz frequency band for safety-related applications of ITS (Intelligent Transport Systems). The safety of ITS (intelligent transport systems). In its report of 21 December 2007 CEPT has concluded that frequencies between 5875 and 5905 MHz is appropriate for safety-related ITS applications by increasing the information to the driver of the vehicle on the environment, on other vehicles and other road users.

ITS transmitters are expected to maximise the use of the spectrum and control their transmitted power to the minimum level to use the spectrum allocated to intelligent transport effectively to avoid harmful interference.

A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperatives, connected and automated mobility Brussels, 30.11.2016 COM (2016) 766 final.

Decrees, Laws and National Guidelines

Ministerial Decree 24/11/1984 "Fire protection regulations for transport, distribution, accumulation and use of natural gas with a density not exceeding 0.8 ". Legislative Decree 285/92 new Highway code.

Decree of the Ministry of the Environment 381/98 "Regulations containing rules for calculating the thresholds of the radio frequency roofs compatible with human health".

Decree of the President of the Republic 5 October 2001, n.447 "Regulations containing provisions as regards to individual licenses and general authorizations for telecommunications services for private use".

ITS Action Plan, December 2008.

Presidential Decree 151/11 of 1 August 2011- Regulation on the simplification of the rules on procedures relating to fire prevention.

Legislative Decree 387/2003 "Implementation of Directive 2001/77 / EC on the promotion electricity produced from renewable energy sources in the internal electricity market "; Legislative Decree 28/2011 "Implementation of Directive 2009/28 / EC on the promotion of use of energy from renewable sources, amending and subsequently repealing the directives 2001/77 / EC and 2003/30 / EC ".

Legislative Decree 152/2006 "Environmental safety regulations"

Note of the DCPREV (National Firefighters Corp, Public Aid and Civil Defense) n. 1324 of 7 February 2012: "Guide for the installation of photovoltaic systems".

Note DCPREV (National Firefighters Corp, Public Aid and Civil Defense) n. 6334 of 4 May 2012

Decree Law of 18 October 2012 n. 179 amended and enacted by law n. 221of 17 December 2012, "Further urgent measures for the growth of the country", under Article 8 - "Measures for the innovation of transport systems "is the decree with which Italy has implemented the ITS Directive 2010/40 / EU.

Interministerial decree 1 February 2013, on "Deployment of intelligent transport systems (ITS) in Italy ", which constitutes the methodological and operational basis of the National Action Plan.

"National Plan for ITS Systems Development" 12 February 2014.

"National Plan of Frequency allocation of the Ministry of Economic Development – 27 May 2015.

DECREE 16 January 2015 MINISTRY OF INFRASTRUCTURE AND TRANSPORT Transposition of the Directive 2014/103 / EU of the Commission of 21 November 2014 adapting for the third time to the scientific and technical progress the Annexes to Directive 2008/68 / EC of the European Parliament and of the Council concerning the inland transport of dangerous goods.

Legislative Decree 50/2016 New procurement code.

"FUNCTIONAL STANDARDS FOR SMART-ROAD" Ministry of Infrastructures and Transport Position Paper of 06/22/2016.

Budget Law 2018 (published in the Official Journal of 29 December 2017)

Technical provisions

Standard UNI CEI EN 16001: 2009 Energy management systems - Requirements and guidelines for use.

UNI CEI EN 15900 Standard Energy efficiency of services - Definitions and requirements.

UNI CEI EN 11339 Standard Energy Management - Experts in Energy Management.

UNI CEI EN 60332-3 Standard Fire spreading and electric cables test procedure and requirements.

UNI CEI EN 60754 Standard Test on the emission of gas during the combustion of materials from cables.

UNI CEI EN 61537 Standard Systems of cable trays and cable ladders for laying the cables. **UNI 10772 - CLASS A** Road transport and traffic telematics. Systems for the elaboration of video images suitable for the recognition of license plates for telematics applications aiming at verifying the violations of the rules of the Highway Code and the toll criteria.

UNI 5649-1 Types of plastic processing unalloyed copper. Quality. Prescriptions and tests

ISO 8528-5 International standards for internal combustion engines of power generators.

ISO / IEC 11801- second edition Generic telecommunication cabling systems.

CEI 11-17 Standard Production, transmission and public distribution of electricity systems - Cable lines.

CEI Standard 11-20 Electricity production plants and uninterruptible power supplies connected to I and II Category.

CEI 20-22 Standards Fire tests on electric cables.

CEI 20-37 / 4-0 Standard Common test methods for cables in fire conditions - Tests on the gases evolved during the combustion of materials from the cables. Part 4: Determination of toxicity index of the gases emitted.

CEI 82-25 Guide to the realization of photovoltaic generation systems connected to the electricity networks of medium and low voltage.

CEI standard 64-8 "Electrical user installations with a rated voltage not exceeding 1,000 V in alternating current and 1,500 V in direct current".

EC Regulations 771/2006 Commission Decision of 9 November 2006 on harmonization of the radio spectrum for use by short-range devices.

EC Regulations 671/2008 Commission Decision of 5 August 2008 on the harmonized use of the radio spectrum in the 5875 - 5905 MHz frequency band for safety related applications of ITS intelligent transport systems.

ECC / DEC / (02) 01 decision of the ELECTRONIC COMMUNICATIONS COMMITTEE of 15 March 2002 on the frequency bands to be reserved for the coordinated introduction of road and traffic transport telematic systems.

MD 14/01/2008 "Technical Standards for Constructions"

ERC / REC 70-03 **Recommendations on the use of short-range devices.**

Restriction of Hazardous Substances (RoHS) in electrical and electronic equipment.

EN 50173-1 2nd edition European standard providing the general requirements concerning the structure and the configuration of structured cabling systems within various types of rooms defined in the others standards of the 50173 series.

EN 61558-2-4 Safety of transformers, power supply units and similar Part 2-4: Detailed requirements for isolating transformers for general purpose.

EIA-TIA 568 C Telecommunications standard in revision C for the wiring of products and services of telecommunication.

ITU-G.655 Characteristics of Non-zero dispersion-shifted optycal fiber cables.

DATEX-II (CEN / TS 16157 and subsequent amendments). Standard for ITS on European roads.

IEEE Standard (Institute of Electrical and Electronic Engineers)

IEEE 1609 - Standard family for vehicle communication systems. IEEE 802.11 standard of transmission for WLAN networks, local networks using wireless technology, rather than cable wired connection, in the form of various releases, developed by group 11 of the IEEE 802 provides for 1 and 2 Mbps broadcasts.

IEEE 802.3-2015 - IEEE standards for Ethernet networks.

IEEE 802.11 a, 802.11 release which allows obtaining a high broadband capacity (54 Mbps theoretical,30 Mbps real) and specifies 8 radio channels in the 5 GHz frequency band. IEEE 802.11 b

802.11 release proposing a theoretical band capacity of 11 Mbps (6 real) with a range that can go up to 300 meters in an open and free space and uses the 2.4 GHz band, with 3 radio channels available.

IEEE 802.11 g, 802.11 release that allows obtaining a high broadband capacity (54 Mbps theoretical, 30 real) on the 3.4 GHz frequency band. It has a rising compatibility with the 802.11b standard that is the 802.11g compliant hardware can work in 802.11b.

IEEE 802.11 i releases of 802.11, which aims to improve the security of transmissions. IEEE 802.11 n 802.11 release which includes the possibility of using MIMO technology, which will allow using more aerials to transmit and more aerials to receive increasing the available bandwidth.

IEEE 802.11p amendment approved for the IEEE 802.11 standard to introduce the DSRC frequency band (5.85-5.925 GHz) that allows providing services in Vehicle-to-Vehicle communications (V2V) and Vehicle to Infrastructure (V2I) communications.

IEEE 802.11 r also known as fast BSS transition (FT) is a change to the IEEE 802.11 standard aiming at allowing the continuity of connection between wireless devices in motion through rapid and safe transfers between the different access points.

IEEE 802.11 k 802.11 release that allows the management and maintenance of wireless networks.

IEEE 802.1q standard that allows multiple VLAN virtual networks to share the same physical connection without losing information between a device and another.

IEEE 802.1x generic term, which refers to the IEEE 802.11 standard for defining the communication on a WLAN network.

IEEE 802.15.4 standard for regulating the physical layer and MAC level of short-range networks, typically lower than 30 m, which work with low data transfer speed.

IEEE 802.15.4e WPAN standard free from EM interferences.

ETSI (European Telecommunications Standard Institute) **Standard**

ETSI EN 300 065 direct printing narrowband telegraph equipment receiving meteorological or navigational information (NAVTEX); Harmonized standard covering the essential requirements of Articles 3.2 and 3.3 (g) of Directive 2014/53 / EU.

ETSI EN 302 637 - 2: the document provides the specifications of the Cooperative Awareness Message (CAM).

ETSI EN 302 637 - 3: the document provides the specifications of the Decentralized Environmental Notification Message.

ETSI EN 302 571: the document describes the communication through radiofrequency between OBU and RSU.

ETSI EN 302 665: the document describes the global communication architecture in ITS (ITSC).

ETSI TR 102 638: the document describes the global architecture of communication in ITS focusing on the Basic Set of Applications (BSA).

ETSI EN 302 663: the document describes the frequency bands of the ETSI G5 and defines the architecture of the Access Layers (Physical Access and Medium Access Control).

ETSI EN 300 647-2-1 Harmonized standard pursuant to Article 3.2 of the R & TTE Directive (European Directive on Radio Equipment and Telecommunications Terminals); Sub-part 1: Requirements for the roadside units (RSU).

ETSI EN 300 647-2-2 Harmonized standard pursuant to Article 3.2 of the R & TTE (European directive on Radio Equipment and Telecommunications Terminals). Sub-part 2: On-Board Unit (OBU).

UNI EN 1194; UNI EN 14080; UNI EN 386 UNI EN 387 replaced by EN 14080: 2013 "Wooden structures, glued laminated timber and glued hardwood ".

UNI EN 338 "Structural Timber-Resistance categories".

UNI EN 1912 "Structural timber- Resistance categories - Assignment of visual categories and types".

DEFINITIONS AND ABBREVIATIONS

Acronym	Meaning	Definition
AC	Alternative Current	Alternative Current
ADC	Analog to Digital Converter	Notation indicating the Analog to Digital Converter
Transport of Dangerous Goods	Agreement concerning the international carriage of Dangerous goods by Road	European Agreement concerning the International Carriage of Dangerous Goods by Road. The original agreement was signed in Geneva on September 30, 1957 as a European Agreement concerning the International Carriage of Dangerous Goods by Road. The text is updated every two years and today the 2015 ADR is in force.
AISI	American Iron and Steel Institute.	Notation that, through a three-digit code, identifies the class of steel.
AP	Access Point	Electronic telecommunications device that, connected to a wired network, or even, for example, to a router, allows the mobile user to access it wirelessly directly through its terminal, if equipped with a special card. If it is physically connected to a wired network (or via radio to another access point), it can receive and send a radio signal to the user thanks to antennas and transceiver equipment, thus allowing connection in the form of radio access.
Captive Portal authentication		Technique that forces an http client connected to the network to visit a special web page (usually for authentication) before being able to access the web browsing.
BACKHAUL	Literally "return cargo"	In the field of telecommunications, a backhaul network or return network is the portion of a hierarchical network that includes the intermediate links between the central network (or core or backbone) and the small subnets to the "margins" of the same hierarchical network.
Backhaul Mesh		In a hierarchical structure of network telecommunications, the backhaul part of the Network includes the intermediate links between the main network, or the backbone network and the small subnetworks "on board" of the entire hierarchical network.
Backup		Total or partial saving of the contents of a mass memory

Best effort		It is said of a network service in which the user is not provided with any guarantee on the quality of the service, on the actual speed of the transfer or on its correct execution.
Big Data		Term used to describe a data collection so extensive in terms of volume, speed and variety that requires specific analytical technologies and methods for value extraction.
Bit	Binary digit	In computer science, the bit is the elementary unit of information, which is represented alternately with the digits 0 and 1, as it corresponds to a choice between two equally possible alternatives (symbol b).
BLE	Bluetooth Low Energy	The BLE technology, compared to the classic Bluetooth, is characterized by a considerable reduction in energy consumption, while maintaining a similar range of communication.
BOS	Balance Of System	Sets of devices that allow to regulate the production of electricity and to transfer it to the network or in storage with the necessary quality and safety standards.
BSA	Basic Set of Application	Group of mature applications (regrouped use cases), supported by a mature, relevant vehicular communication system NOTE: basic set of applications can be deployed simultaneously at a targeted time (day 1) with the objective to serve societal and business objectives of private and public road transport stakeholders.
LV	Low Voltage	
CAM	Cooperative Awareness Message	Messages exchanged between vehicles and infrastructure, defined by the ETSI EN 302 665 standard.
DC / AC	Inverter	Notation indicating the Direct Current to Alternative Current Converter
LCC	Local Network Control Centre	
RCC	Remote Control Centre	Control centre corresponding to those of RMT supplied either centrally or in local offices
CEI	Italian Electro-technical Committee.	The CEI is an association recognized both by the Italian State and by the European Union for regulatory activities and the dissemination of technical-scientific culture

CEPT	European Committee of Postal and Telecommunications Administrations	Organization founded on 26 June, 1959 in France to carry out coordination tasks, standardizing procedural and technical rules, and organization in Europe with regard to telecommunication standards and postal services. The CEPT in 1988 then established the ETSI, which is responsible for drafting the rules relating to Data Communication.
C-ITS	Cooperative Intelligent Transport Systems	The C-ITS are systems that enable the efficient exchange of data through wireless technologies so that vehicles can connect with each other, with the road infrastructure and with other road users.
CLI	Command Line Interface	In computer science the command line interface, also known as CLI, sometimes simply called command line, indicates a type of user interface characterized by a textual interaction between user and computer: the user gives text commands in input by means of an alphanumeric keyboard and receives textual responses in output from the computer through an alphanumeric display or printer.
Client		Client A client, in computer science, indicates a component that accesses services or resources of another component called server. In this context, one can therefore speak of clients referring to the hardware or al software. It is therefore part of the logical network architecture called client-server.
Cloud		We indicate a paradigm for the provision of IT resources, such as archiving and processing or data transmission, characterized by on demand availability through the Internet starting from a set of pre-Existing and configurable resources.
Cloud Computing		Provision of IT resources through the Internet
Clustering		Clustering or cluster analysis is a set of multivariate data analysis techniques aimed at selecting and grouping homogeneous elements in a set of data.
Data link		It is the means of connecting one station to another for the purpose of transmitting receiving digital information.
DATEX-II		Standard developed for the Exchange of information Between the traffic

		Management centres developed in line with the ITS action plan
DB	Database	A set of data organized into tables linked by relationships, having a predefined structure and known characteristics and on which insertion, updating, deletion and consultation operations can be performed.
DC	Direct Current	Low Voltage
DENM	Decentralized Environmental Notification Message	Messages exchanged between vehicles, related to alarm events occurring on the road.
DHCP	Dynamic Host Configuration Protocol	Network protocol of application level which allows devices or terminals of a local network to automatically receive for each request to access an IP network (such as a LAN) the IP configuration necessary to establish a connection and operate on a wider network based on Internet Protocol, i.e. interoperate with all other subnets by exchanging data, provided they are also integrated in the same way with the IP protocol.
DLL	Data Link Layer	It is the second level of the network architecture based on the ISO/OSI model for the interconnection of open systems. This level in transmission receives data packets from the network layer and forms the frames that are passed to the underlying physical layer with the aim of allowing the reliable transfer of data through the underlying channel.
DSRC	Dedicated Short Range Communications	Two-way short-range and medium-range wireless communication system that allows data transmission for intelligentapplications in the transport and mobility sectors.
DSS	Decision Support System	Software to support internal decisions at the Anas.
EAP	Extensible Authentication Protocol	Framework of authentication used on access point and in the connections PPP. The use of EAP within a wireless network provides that it is not the access point to authenticate the client: it redirects the client authentication request to a specific server.
eCall		Electronic service of interoperable emergency call.
EIA/TIA 568 C	Electronic Industries Alliance/Telecommunications Industry Association	Series of standards concerning the wiring of telecommunications products and services.

EIRP	Equivalent Isotropic Radiated Power	Measurement of radio power density radiated by an antenna,independently from the radio bandwidth used. It is expressed in Watt or milliwatt; it is often convenient to measure it in dBm.
EN	European Norm	This code identifies the standards developed by the CEN (Comité Européen de Normalization), the European Standardization Body. CEN member countries must comply with the EN standards (in the case of Italy they become UNI EN).
ERC	European Research Commission	
ETSI	European Telecommunications Standard Institute	European standardization body that produces globally applicable standards for information and communication technologies.
ETSI ITS G5	European Telecommunications Standard Institute - Intelligent Transport Systems	European standard for vehicular communication in dedicated frequency bands for the European intelligent transport system (ITS).
FCC	Federal Communications Commission	Federal Communications Commission of an independent Administrative authority charged with all non-governmental uses of the radio spectrum (including radio and television broadcasts), all interstate telecommunications (cable, telephone and satellite) and international communications originating and destined from the United States.
FEC	Forward Error Correction	
Firewall	Firewall Fire barrier wall	(a) A special type of doors, with automatic closing in case of fire. (b) Security system for controlling access to a network.
Firmware		Program, or a sequence of instructions, integrated directly into an electronic component in the broadest sense of the term (integrated, electronic cards, peripherals). Its purpose is to start the component itself and allow it to interact with other hardware components through the implementation communicationprotocols programming interfaces.

Frame Aggregation		A station with one or more frames to send can choose to transmit them as a single frame. The resulting frame contains a single Radio-Preamble and a single Radio-Header, thus reducing the overhead and increasing the playload, and since a single transmission is made, the time of contention and backoff on the wireless medium and the number of potential collisions are reduced.
FTP	File Transfer Protocol	Protocol that operation of transferring from a computer to another.
Gateway	Transit knot	Protocol converter. A specific application node that links together otherwise incompatible networks. It converts data codes and transmission protocols to ensure interoperability or transfers data or messages between programs or networks that are normally incompatible.
GE	Gigabit Ethernet	Ethernet network with a bit rate of the order of Gigabit per second (Gb / s).
GHz	Gigahertz	Unit of measurement of frequency, equal to one billion Hertz, that is, cycles per second.
GPS	Global Positioning System	Civil satellite positioning and navigation system that, through a dedicated network of artificial satellites in orbit, provides a mobile terminal or GPS receiver with information on its geographical coordinates and time, in any meteorological condition, anywhere on Earth where there is a contact without obstacles.
GUI	Graphical user interface	A graphical interface gives the possibility to interact with the computer through the "choose and click" technique or to otherwise manipulate images and icons on the screen.
Handover		In the field of wireless Telematics communications, Handover refers to the Procedure for which the channel used is changed from the connection of a mobile terminal to the wireless network while keeping the communication active.
HD	High Definition	
HF	High Frequency	
Hop		Subsequent "hops" from a MAP (Mesh Access Point) that allow reaching from a RAP node (Root Access Point) not only the other adjacent nodes, but also the more distant ones.

Host		Host node that indicates each connected terminal, through a communication link, to a computer network (e.g. Internet).
Hosting		Service that hosts the pages of a site on a Web server, making them visible on the Internet.
ICT	Information and Communication Technology	The set of information and telecommunications technologies and their integration.
IEC	International Electrotechnical Commission	International organization for the definition of standards for electricity, electronics and related technologies.
IEEE	Institute of Electrical and Electronic Engineers	International association of professional scientists with the aim of promoting technological sciences.
IoT	Internet of Things	Neologism in telecommunications that refers to the extension of the Internet to the world of objects and concrete places that become recognizable and acquire intelligence thanks to the fact of being able to communicate data about themselves and access aggregated information from others.
IP	Internet Protocol	Internet protocol that defines the units of information passed from one system to another to guarantee a basic service for forwarding data packets.
Ipv6		Sixth version of the evolution of the IP protocol, Internet Protocol.
ISM	Industrial Scientific and Medical	Industrial Scientific and medical applications.
ISO	International Organization for Standardization	It is the most important organization in the world for the definition of technical standards.
ITP	Intelligent Truck Parking	Intelligent parking for heavy goods vehicles
ITS	Intelligent Transport Systems	Systems that, following national and international standards, present advanced information and communication technologies in order to improve the safety of driving and the safety of people, vehicles and goods, as well as the efficiency of transport systems for passengers and goods.
ITSC	Intelligent Transportation Systems Society	Communication system dedicated to transport.

ITU	International Telecommunication Union	United Nations Agency specialized in the field of telecommunications and information and communication technologies.
Jitter		In electronics and telecommunications, the term jitter indicates the variation of one or more characteristics of a signal, such as, for example, amplitude, frequency, and phase.
KEMLER		The Kemler-UN is an international code placed on the sides and back of vehicles carrying dangerous goods. Identifies the type of material transported and the type of dangerousness of the same. In case of an accident, the timely communication to the Fire Brigade, of the numbers shown on the panel, allows to establish quickly the type of intervention.
Kernel	Core	It is the core of an operating system or software with the task of providing the processes running on the computer a secure and controlled access to the hardware.
LAN	Local Area Network	
Layer		Level, e.g.: in vector graphics or in the stratification of the OSI Model.
LEACH	Low Energy Adaptive Clustering Hierarchy	
LED	Light Emitting Diode	
Li-Po	Lithium Ion Polymer	
LLC	Logical Link Control	
LoRa	Long Range	
LoRa WAN	Long Range Wide Area Network	
LPWAN	Low Power-Wide Area Network	
M2M	Machine to Machine	
MAC	Medium Access Control	
MAP	Mesh Access Point	
MEMS	Micro Electro Mechanical Systems	
MIB	Management Information Base	

MID	Metrological Instruments Devices	
MID	Energy meter	
MIMO		In telecommunications, it indicates the use of a multiple antenna system both on the emitter side and on the receiving side, in order to improve the performance of the communication channel. It is one of the possible topologies of "smart antenna": an array of single antennas elaborates the signal, in this case taking advantage of the idea of "constructive interference of multipath" (other possible techniques are, for example, irradiation lobes variable in time, on demand, or antenna diversity).
MIT	Ministry of Infrastructure and Transport	
Mobile device		Electronic devices that are fully usable following the user's mobility such as mobile phones, handhelds, smartphones, tablets.
MPLS	Multi Protocol Label Switching	Technology for IP networks that allows the routing of multiprotocol traffic flows between the source node and the destination node using identifiers between pairs of adjacent routers and simple operations on the labels themselves.
MT	Medium Voltage	
Multicast Frames		Method for data transmission over networks, from a single point that transmits a single data stream to multiple receiving points. Optimize the use of the network, compared to unicast methods (many data streams, one for each point that wants to receive it) and broadcast (a single data stream for all receivers, even if they do not want to receive it.
Multipath Fading		In telecommunications, multipath fading is a form of distortion of a signal that reaches its destination in the form of a number of replicas, out of phase with time, originated by the various paths (multipath) that the signal itself may have followed during its propagation and that add up among them in reception. Furthermore, each replica, having completed a course of a certain length and characterized by a reflection on generally different surfaces, will therefore be subject to an attenuation in general different from that suffered by other replicas. It is a typical

		problem of both fixed and mobile radio communication in a deterministic way in the first case and with typical characteristics of a random process in the second case. The arrival of the various replicas within a symbol time is not a serious problem; on the contrary, delays comparable to the duration of the symbol time cause harmful interference phenomena.
NAT	Network Address Translation	Translation of network addresses, also known as network masquerading, native address translation, is a technique that involves modifying the IP addresses of packets in transit on a system that acts as a router within a communication between two or more hosts.
NDEF	NFC Data Exchange Format	It defines the format of encapsulation of the reports for the exchange of information between devices respecting the recommendations of the NFC Forum that is between two active NFC devices or active devices and passive devices (tags). It is a binary message that can be used to encapsulate any application data protocols in a single report. The purpose of the NDEF specification is to define the structure and rules of data to build valid reports. It also defines the types of application data encapsulated in NDEF relationships.
NFC	Near Field Communication	Technology that allows obtaining short-distance bi-directional wireless connections.
Node		In information technology and telecommunications, it is any hardware device in the system that can communicate with other devices that are part of the network.
NC	Centre node	
NS	Segment node	
OBU	On board Unit	Communication device mounted on the vehicle that allows communication with other OBUs or RSUs.
OCPP	Open Charge Point Protocol	Application protocol for communication between electric vehicle charging stations and a centralized management system.

Open Data		Data freely accessible to all whose possible restrictions are the obligation to mention the source or to keep the database always open.
OSI	Open Systems Interconnection	Known as an ISO / OSI model, it is a law standard for computer networks established in 1978 by the International Organization for Standardization (ISO), the leading international standardization body. It establishes for the network logical architecture a layered structure composed of a stack of network communication protocols divided into 7 levels, which together perform all the network functions, following a logical-hierarchical model.
OTDR	Optical Time Domain Reflectometer	Optoelectronic measuring instrument, mainly used in the field of telecommunications for the analysis and diagnosis of optical fibre failures.
Overhead		In computer science, the English word Overhead (literally above, which is above) is used to define the complementary resources, overlapped with respect to those strictly necessary to achieve a certain purpose following the introduction of a method or a process more evolved or more general.
P2P	Pear to Pear	Network architecture in which, unlike the client-server structure, all nodes can indifferently act as applicants or as suppliers of data and applications.
PEAP	Protected EAP	
PHY	Physical Layer	
PoE	Power over Ethernet	
QoS	Quality of Service	
QR code	Quick Response Code	
Rack		Frame for electronic devices with modular structure.
RAP	Root Access Point	
Flat network	pg 63	
RF	Radio frequency	
RFID	Radio Frequency Identification	

RLAN	Lan Radio	Local network that communicates via radio instead of cable and provides broadband connectivity.
RMT	Road Management Tool	
Roaming		Agreement between two or more mobile phone service management companies, operating in the same territory or in different countries, according to which users of one company may use the network of the others.
RoHS	Restriction of Hazardous Substances	
Routing		In the field of telecommunications networks, it is the function of a switch (router, switch) deciding on which port or interface to send a received communication element (telephone conversation data packet, data flow). The term is a metaphor that refers to the act of routing (directing, addressing).
RS	Segment Router	
RS232	Electronic Industries Alliance Recommended Standard 232	EIA standard serial port equivalent to the European standard CCITT V21 / V24, which defines a serial interface with a low transmission rate for the exchange of data between digital devices.
RS422	Recommended Standard 422	Protocol for serial data communication that involves the use of two wires with a differential and multi-point line (balanced differential).
RS485	Communication Interface	
RSU	Road-side Unit	Device located on the edge of the road, which provides support for connectivity to the passage of vehicles.
SAP	Service Access Point	Point of access to a service that an OSI level offers at its highest level, in an architecture in which each level offers a series of services to the hierarchically superior one and benefits from the services offered by the underlying one.
SCADA	Supervisory Control And Data Acquisition	Indicates a computer system distributed for the electronic physical systems.
Server		High performance computers that in a network provide a service to other connected computers, called clients.

Shutter	Charging sockets	
SIM	Subscriber Identity Module	It is a smart card, inserted inside a cellular phone allowing securely filing the MSI with a single number associated to all mobile phone users that represents the international identity of a mobile phone user. The telephone operator the SIM cards to provide the subscribers with voice and data connections uses.
SM o SMX	Spatial Multiplexing	It is a transmission technique in MIMO wireless communication to transmit separately coded independent data signals, so-called flows, from each of the multiple transmission antennas. Therefore, the size of the space is reused more than once (multiplexing).
SMACS	Self-Organizing Medium Access Control for Sensornets	
Smartdust Network		It consists of a network with Microscopic electro-mechanical systems (sensors) put into communication by means of a wireless system capable of detecting, for example, light, temperature or vibrations.
SMS	Short Message Service	Mobile phone service to send short text messages from one mobile phone to another, and is by extension commonly used in Italian to indicate every single message sent with such services.
SOA	Web services	
SOAP	Simple Object Access Protocol	It is a specific protocol for the exchange of structured information in the creation of web services in computer networks.
SPD	Overvoltage protection device	
SSH		In computer science and telecommunications SSH (Secure SHell, secure shell) is a protocol that allows to establish an encrypted remote session via command line interface with another host of a computer network.

SSID	Service Set Identifiers	The service set identifier, or SSID, is the name by which a Wi-Fi network or in general a WLAN identifies itself to its users. Access points are often configured to announce continuously their SSIDs, so that mobile Wi-Fi transceiver devices can create a list of wireless networks available in the area where they are located. This list can then be shown to the user in order to choose the network to connect to (provide that the device does not automatically take this decision).
Standalone		Object or software capable of functioning alone or regardless of other objects or software, with which it could otherwise interact.
Stateful		Static Current Direct Current to Alternating Current Converter
STIG	Telecontrol system in tunnels	The technological system makes it possible to monitor in real time the functioning of the technological systems in operation inside the road tunnels insistent on Anas network.
Switch	Commutatore	Active network equipment capable of switching that is, redirecting calls on one port to another single specific port, using level 2 of the ISO-OSI scheme.
Layer 2 switch		Device that uses the MAC address of the host interface ports to decide where to forward the frames it receives.
System.Web.UI		The System.Web.UI of the namespace provides classes and interfaces that allow you to create ASP.NET server controls and ASP.NET Web pages for the user interface of ASP.NET Web applications.
TACACS	Terminal Access Controller Access Control System	It refers to a type of computer protocol for authentication and remote authorization (not therefore AAA), with related services, for the control of network access through a centralized server.
TAG NFC	Tag Near Field Communication	Chips stored on small adhesive plates or similar on which you can write data and information that can be interpreted by a mobile device.
TAG RFID	Tag Radio Frequency Identification	

TCP/IP	Transmission Control Protocol/Internet Protocol	Agreed communication method of Internet machines that interact with each other by sending packets across multiple networks until they reach their destinations.
Tera-Play	Multiple broadband connectivity	
Throughput	Tag Identifier	Within the telecommunication area, the throughput is the "actually used". Transmission capacity of a communication channel. The throughput is usually indicated with THR. It must not be confused with the "capacity" of the link: both the capacity and the throughput are expressed in bit/s, but if the first expresses the maximum transmission frequency of the transferred data, the throughput is an index of the "actual" use of the link capacity. The throughput is the quantity of data transmitted in a time unit while the capacity depends only on the quantity of data available on the transmission data.
TIA	Telecommunications Industry Association	An association accredited by the American National Standards Institute to develop standard for a large series of technologies and communication products.
TID	Tag Identifier	Radio frequency identification labels for gathering information.
TLS	Transport Layer Security	
T-MAC	Timeout-MAC	
TPC	Transmitter Power Control	
Triple play		In the telecommunications sector, the Triple Play service is a marketing term for the provisioning of two bandwidth services on a single broadband connection.
Troubleshooting	"elimination of the problem"	Logical research process of the causes of a problem on a product or process in order to make the system be re-operational and that the malfunction/failure does not reappear anymore.
TTLS	Tunneled Transport Layer Security	
TVCC	Closed-circuit television	Cameras that transmit the signal to specific or limited sets of monitors and/or video recorders.

UID	Unique Identification	In Unix and Unix-like operating systems, UID is the number, which identifies uniquely a system user.
UNI	Italian unification body	Private association that Develops and publishes voluntary technical standards for all industrial, commercial and tertiary sectors.
UV	Ultra Violet	
V2I	Vehicle to Infrastructure	Connectivity between vehicles and infrastructure.
V2V	Vehicle to Vehicle	Connectivity between vehicle and vehicle
VMS		Platform able to manage up to 50 cameras equipped with client/server software for a virtual video matrix management system. The VMS system allows the management of users, priorities, alarms and system configuration.
VOIP	Voice Over Internet Protocol	Technology, for telephone service, with Internet connection or other IP-based data network.
Wearable device	Wearable device	
Wi-Fi		Technology that through the related devices allows to users terminals connecting wireless (WLAN) among each other through a local network based on the specifications of the standard IEEE 802.11
Wi-Fi in motion	Wi-Fi on the go	
WIM	Weigh in Motion	Dynamic weighing systems, designed to capture and record the gross weight of each individual vehicle in transit at any travel speed, without requiring the vehicle to stop.
Wired		Traditional systems based on wired connections.
Wireless		Communication between electronic devices that does not use cables.
WLAN	Wireless Local Area Network	Local network that uses wireless technology, instead of a wired connection.
WMM	Wi-Fi Multimedia	
WPA2-CCMP (AES)		The CCMP, initials of Counter-Mode / CBC-Mac Protocol, is a method of encryption used by the IEEE 802.11i standard for key management and message integrity. The CCMP is part of the WPA2 certification program. Wi-Fi Protected Access (WPA and

		WPA 2) is a certification program managed by the Wi-Fi alliance as data protection exchanged in a wireless computer networks.
WPA2-TKIP		WPA2 is replacing WPA. As it happened for WPA, WPA2 requires testing and certification by the Wi-Fi Alliance. WPA2 implements the optional elements of the IEEE 802.11i standard.
WPA-TKIP		The TKIP protocol dynamically changes the key in use and combines it with an initialization vector (IVS) that is twice the size of the WEP (in order to make the attacks similar to those expected for WEP vain) and can be implemented in the pre-WPA interface cards wireless.
WSN	Wireless Sensor Network	Determined type of network that, characterized by a distributed architecture, is realized by a set of autonomous electronic devices able to collect data from the surrounding environment and to communicate with each other.
XBEE		Wireless connection device-to-cloud technology.
ZigBee	IEEE 802.15.4 (Zig Bee)	ZigBee is one of the main standards of communication, edited by the ZigBee Alliance. Using small, low-power and low consumption digital antennas based on the IEEE 802.15.4 standard for wireless Personal area networks (WPAN), the standard specifies a series of application profiles that allow realizing a specific communication for the different typical profiles in the Wireless Sensor Networks field.

In this unique publication on the international level, Anas interprets the concept of Smart Road as a road connected with users and vehicles, ready for autonomous driving.

anas
GRUPPO FS ITALIANE

Anas S.p.A. (Gruppo FS Italiane) Directorate General
Via Monzambano, 10 - 00185 ROME
Tel. 800841148 - servizioclienti@stradeanas.it