CYBER & SECURITY SOLUTIONS

genesiX

towards a new control room concept

LEONARDO

Complexity is what security operators must face in everyday work; operational context is characterized by availability of many heterogeneous data flows that need to be processed, synthetized, contextualized in a timely way in order to be translated into actionable information enabling operators to make the right decision at the right time.

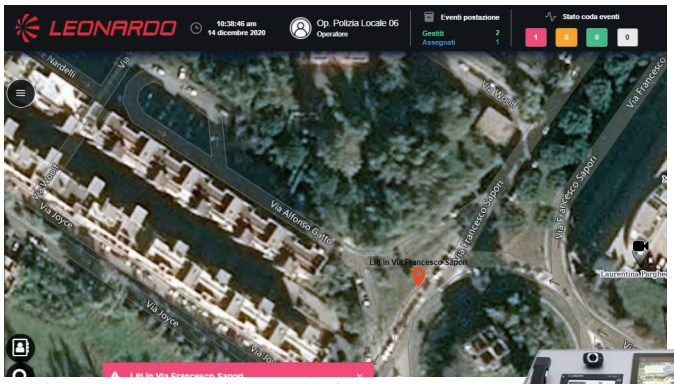
Failing to do this, may mark the difference between success and failure for a mission that, in mission critical contexts such as public safety or defence, can imply risk for human lives.

New command and control applications, as well as new control rooms more and more digitalized, need to master the “information deluge” in order to:

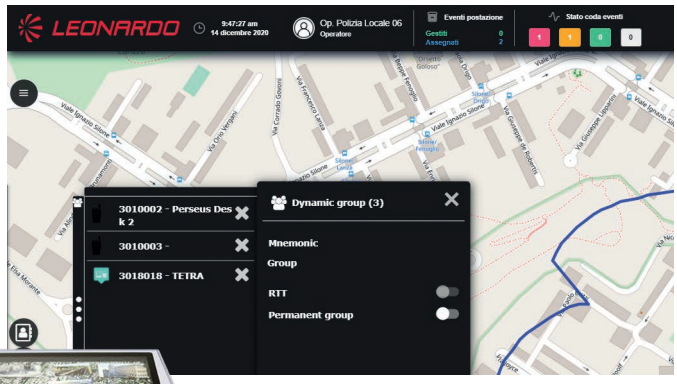
→ extract relevant information from a huge amount of heterogeneous data (even leveraging past experiences by means of artificial intelligent engines) and convert them into
→ convert them in useful indications for operations management
→ be able to disseminate on field in a secure and effective way.

CONTROL ROOM EVOLUTION

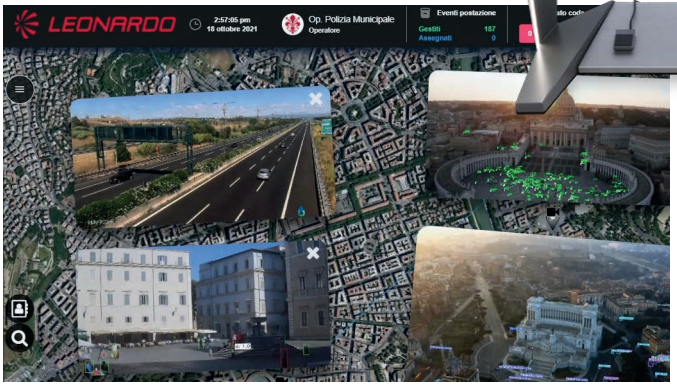
Control room is the place for management of public safety events, investigations of police operations: it represents the logic point of convergence for field sensors, applications elaborating data characterized by different format, reliability and confidence and systems devoted to resource planning and management



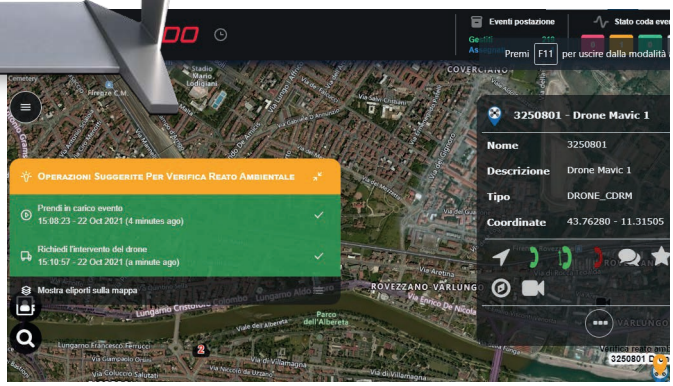
Road map and pop up window with family quarrel address indications



Creation of dynamic group



Area map with potential ambiental crime viewed from drone



City map and pop up video for surveillance of the main places

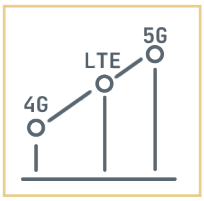
Traditional voice based information exchange between control room operators and on field officers, as well as control room structure, need to change both as a consequence of evolution and in order to supply effective and innovative answers to evolving requirements:

- → Data sources diversification and channel amount increment (video cameras, intelligence, simulations, social, historical data) until recently unimaginable.
- → Need of automated data elaboration in order to extract useful information, analyse them according to current context correlating with other relevant sources.
- → Versatility of communication channel taking advantage of multimedia thanks to 4G and 5G broadband technologies allowing new information acquisition/dissemination ways supporting bi-directional information flows with on field operator that becomes an additional sensor capable to increase overall situational awareness.
- → New man-machine interaction ways supporting enhanced communication and increased contents availability (evolved gesture based GUIs, augmented reality, virtual reality, natural languages).

MAIN FUNCTIONALITIES

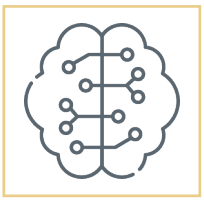
In mission critical applications, the reliability of overall solution and the full compliance with existing operating procedures take precedence over availability of advanced and sophisticated functions. Because of this, a conservative approach is generally taken for usage of emerging or nnovative technologies (as an example the relatively slow adoption of broadband with respect of commercial environment can be considered) keeping "professional"solutions behind current technological state of the art.

Evolutions in communications and computer science led to availability of technologies capable to overcome some blocking problems, making the design of a real new generation system possible.
Such technologies essentially are:



4G and 5G allowing to overcome some functional limits of broadband technologies (priority control) and in perspective allow to build a communication system scalable, dynamically adaptable to required performance and supporting integration with previous generation networks

Big Data: capabilities of new networks, massive IoT, multi megapixel video surveillance cameras, social media and Big Internet (controlled) usage in control room, Open Data, massive databanks and historical archive access, cause an increment of orders of magnitudes in the amount of data that need to be accessed and processed requiring suitable technologies for proper management.



Artificial intelligence: radical data amount increase in control room requires automated intelligent processing both to offload operator from cumbersome surveillance tasks (as may happen using video analytics) and to provide decision support (using simulations, what-if projections and leveraging past experiences in similar experiences with automated reasoning systems).

Cyber security: a set of technologies rather than a single one. New control rooms are connected and exposed to threats that need to be counteracted with a complete approach starting from design (secure & resilient by design) extending to real-time proactive monitoring and management (also leveraging cyber threat intelligence).

Cloud Computing (possibly private cloud) new computing models are needed to cope a distributed and dynamically variable workload. Cloud computing allows physical resources optimization allocating computing power whenever and wherever required leveraging an architectural model also used by new generation communications networks.

Business intelligence for the generation of dashboards for the monitoring of service levels and the analysis of operations and requirements.

LEONARDO genesiX PLATFORM

Taking advantage of proven technological capabilities and long lasting domain expertise, Leonardo designed genesiX a new generation product for Command and Control aiming at equip our Customers with versatile and scalable solutions supporting the evolution of Command and Control concept towards a new "Data & Experience-Centric Operating Model" paradigm.

Leonardo solution implements a federated architecture that can span several sites and be accessed in a secure way by different organizations (multi tenancy) capable to:

- → Integrate all existing systems and applications in control room adding new functions and services if needed.
- → Collect information from structured (data bases, archives) and not structured (video, sensors, media) data sources.
- → Guarantee information superiority to operators by searching and supplying in an automated way all useful information for effective event monitoring/surveillance/ management, also providing operational suggestions generated by analytics background activities (datamining, data correlation, video analysis) and taking advantage of virtual assistants and natural language interactions.
- → Optimize logistics and resource management (skill, equipment, weapons) by interacting with all available structured and not structured databases.
- → Support investigation analysis for monitored phenomen by analysing large data amount and providing simulations.

genesiX is built on a micro services architecture, support a cloud deployment and a web based access. From a logical architecture point of view, it is organized in the following layers:

- → Integration layer: includes all sub-systems and sensor that acquire information directly from the field. At this level, the information obtained may already be subjected to a first elaboration according to the business logic of its domain.
- → Core layer: it is the core logic level and it is the kernelof genesiX. Here, data and events coming from the integration layer are collected through a microservices software infrastructure and made available to the various processing engines, in order to "apply intelligence" to the system according to the rules and algorithms oriented to specific domains
- → Presentation layer: this level is based on an innovative HMI, built up to simplify the information displayed by the operator. The level, (GIS-based, principally) allows to be used to entry in the different sub-levels providing different services offered by the system

genesiX versatility and the possibility to integrate with existing or specific applications give the possibility to design and deploy command and control solutions in several applications domains such as:

- → Public Safety and Police Forces
- → Defence operations
- → City governance

Common hardware approach, micro services architecture and innovative interface allow:

- → Flexibility and portability with different deployment options such as public cloud, private cloud, local installation also allowing deeply customized solutions.
- → Open standard approach that allow to access (and integrated) all existing legacy applications.
- → Extensibility allowing to add specialized capabilities and functions whenever needed.
- → Automation for maintenance procedures thus diminishing manual operation.

By means of an evolved CAD (Computer Aided Dispatch) function, the platform can interact with on field resources using network infrastructures that best suits the required task. According to on field availability the platform can use narrowband or broadband network leveraging LTE and in perspective 5G.

GIS (Geographic Information System) has a key role both in information presentation and in service access. Services are profiled according top operator's role.
A suitable integration layer supplied with the platform virtualizes the network infrastructure and support communications technology interoperability according to mission critical integrated network model.

genesiX platform takes advantage of Leonardo current professional communications systems, security and territory control systems as well as cyber security and intelligence infrastructures integrated and constantly evolving to supply an innovative solution.

USE CASES

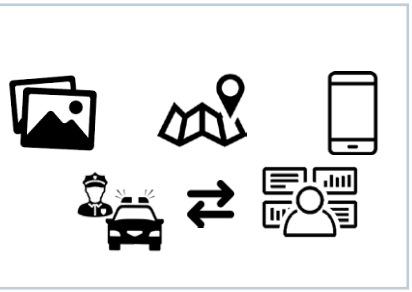
Following the description of two possible use case showing the characteristics of the platform: the management of a police operation and the management of an emergency rescue operation.

PLANNED EVENT MANAGEMENT
PUBLIC ORDER ENFORCEMENT OR INVESTIGATION OPERATION

Event planning: virtual site inspection on a 3D map supported by virtual/augmented reality (relevant information collection such near interest point, weapon holders/police known people home location). Possible event simulation in order to verify forecast/assumptions correctness and figure out possible effects.

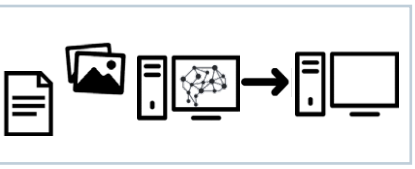
Available resource identification and location on the map including all available information (skill, equipment,...).
Continuous tracking of relevant resources on the map.
Automated best path suggestion by virtual assistant.

Instructions/information dissemination on field (including pictures, best path, etc.) by means of broadband radio. A single click on graphical info needed for information transfer.
In the same way multimedia info collected by on field operators enriched by reports or additional data can be transmitted to control room.

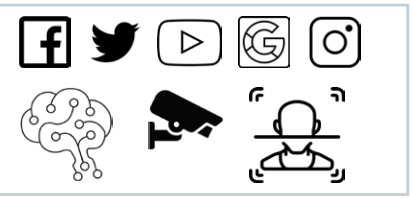


Decision support system can identify relevant additional information/ resources and present them by support of virtual assistant (e.g. neighboring video cameras addressed area highlight and relate streaming).
Drones (if any) payload visualization and streaming on on-field operator smartphones or tablets.

Synthetic data extraction and forward to federated systems (including additional control rooms and/or decision makers) in order to share information and enforce coordination



Social media monitoring for possible relevant information extraction that can contribute to increase situational awareness (e.g. information related to interest people, area, time).
Video analysis used to detect potential interesting events such as forbidden movements/presence in banned areas or hostile presences in operation theatre.



CRITICAL INFRASTRUCTURE MONITORING MANAGEMENT

The workflow begins with the constant monitoring of a critical infrastructure for structural health control (e.g. bridges, viaducts, dams, etc.). The system allows you to maintain the operational focus on the event:

Monitored infrastructures are georeferenced on a cartographic map. Installed sensors information can be visualized on request.

Structural health applications (not part of the system but integrated with it) can periodically check the status of the infrastructure reporting results on the map. Asynchronous checks may be triggered by major solicitations generating alert reported to operators.

Infrastructure digital twin may be integrated within the solution and queried to check if strain and stress can compromise the structural integrity resulting in an immediate danger.

System is able to look for relevant documents (project plans, reports...<) in federated databases providing operator with the possibility to consult for a better situational awareness.

Video cameras (if existing in monotored location) possibly enhanced by video analysis can be used to enhance situation evaluation. System allow a gesture based simply access to cameras.

Ancillary meteorological information (e.g. wind or rainfall) or traffic conditions that could cause additional risk for the infrastructure can be visualized accessing suitable cartographic layers.

Satellite imagery can be accessed (also comparing different time periods) to assess infrastructure movements or other possible anomalies.

Social media content addressing monitored infrastructure can be accessed to have an additional information channel.

Operator can request and coordinate the intervention of a squad on team for additional. Integration with telecommunications infrastructures allow to be in constant contact also taking advantage of additional mobile sensors (drones) whose information can be transparently forwarded to the system.

WHY LEONARDO

Leonardo aims to be a strategic partner for Governments and Institutions for resilient solutions in Command and Control, Mission Critical Communications leveraging his proven competencies shown in domestic and international projects.

Leonardo has strong technological competencies in main solution domains, has the “vision” needed to build long lasting systems, a proven attitude to system integration that enables our Company to lead a team of partners.

Leonardo is a specialist in physical and logical security; our secure by design approach allows us to implement a certified solution compliant with main national and international standards taking also care of monitoring and management of deployed system.

For more information:
cyberandsecurity@leonardo.com

Leonardo Cyber & Security Solutions Division
Via R. Pieragostini, 80 - Genova 16151 - Italy

MM09077 10-25

leonardo.com