LEONARDO ELECTRONICS

AEROMACS

BROADBAND DATALINK FOREGROUND NETWORK AEROMACS SOLUTION

The Broadband Data Link Infrastructure Foreground Networks AeroMacs concept supports different Airport Surface Operational needs and heterogeneous data exchange in delivering a secure wireless data network. AeroMacs gathers data from fixed or mobile sources, flight service vehicles, and weather stations, sharing the same infrastructure with optimized performances and reduced efforts.
AeroMacs satisfies international market needs and the development of the Airport Concept of Operations (CONOPS) for the Total Airport Management.

OPERATIONAL CONTEXT

The increase of Airport traffic movements demands:

- Surface Data Sharing to support huge data exchange for effective and efficient airport operations
- New Data Communications infrastructure to reduce ATC Workload, avoiding misunderstandings and improving efficiency
- Advanced Collaborative Decision Making (A-CDM) to support ANSPs, Pilots and airport Operators in optimizing performances using the same operational picture

Within this context, The Broadband Data Link Infrastructure Foreground Networks AeroMacs Solution conveys direct benefits in terms of:
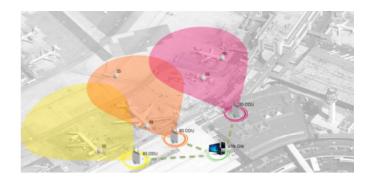
- Sustaining the increasing demand for data exchange among aircrafts, vehicles, and GND infrastructures
- Support Airport Data Gathering coming from different functional domain categories which have completely different operational features and performances
- Improve Data Integrity to guarantee the requested Safety and Security Target Levels
- Support Real Seamless communication Systems in managing Terminal and Surface movements (aircraft and vehicles) by frequency hand-over

PERFORMANCE OUTLINES

- Mobile applications:
  - ATC Communication with any aircraft everywhere in the AirSide (RWY and Taxiways included)
  - TWR Datalinks for clearance management
  - Airlines Operational Communication Services (AoC) as CDM messages
  - Surface management (including ramp and gate control)
- Stationary Mobile Applications:
  - Weather Data Gathering and monitoring
  - Airport Surveillance, which entails a high level of Airport awareness
- Network level 3 oriented to multiple Wide Area Network (WAN) for multiple Operators
- High speed mobility
- Support to multiple CSNs (e.g. Airport users, CSPs networks, etc...) by Unique Airport Infrastructure Solution
- Prioritization Service flows to ensure time constraints satisfaction according to different operational needs
- Support of both ATN/IPS connectivity and ATN/OSI connectivity via usage of proper convergence function (e.g. SNDCF) with no further network developments
- Optimization of deployment and Maintenance costs by a wireless infrastructure capable to ensure best cost-benefit ratio
- Secure and dependable support for both unclassified and classified airport communications for military Agencies and Wing Operating Centres (WOC); e.g. mission planning

SYSTEM ARCHITECTURE

AeroMacs is an interoperable wideband system which allows current and future stationary and mobile Operational services including Airline Operational Communications (AOC). AeroMacs integrates the following sub-systems:

- Ground Stations with variable configurations, according to siting, safety and coverage needs (Single sector/multisector or redounded configuration)
- Subscriber Stations which can be used as basic elements for:
  - Vehicular subsystems that can be configured for any type of airport vehicle
  - Fixed station subsystems that can be used as AeroMACS access points for airport subsystems
  - Handheld mobile subsystems, composed by a COTS smart device plus an AeroMACS adapter
- ASN Gateway providing proper access to various Stakeholder Networks (e.g. multiple AOC Gateways)
- CSN providing required connectivity towards ATN-OSI and ATN-IPS/SWIM nodes, and enabling both IPv4 and IPv6/IPSEC connectivity for integration into PENS and Military Agencies for ATM data sharing through SWIM
- Security service modules capable to implement different countermeasures in order to protect data in terms of Confidentiality, Integrity, Denial of service and Trustworthiness. Those shall be negotiated upon the required security level for the specific service. The security architecture provides authentication and encryption protocols (EAP-TLS, PKMv2), and VPN tunneling capability. The security architecture is based on the following components:
  - AAA server (Authentication, Authorization Accounting)
  - PKI, implementing the X.509 certificate issue, renewal and withdrawal functions
- Network and Performance Management (ONM-ATC) capable to give to each Stakeholder the expected SLA management

LEONARDO