GAMMA

GLOBAL ATM SECURITY MANAGEMENT

A New Vision for ATM Security Management

The Security Management Platform

Claudio Porretti

LEONARDO

SECURITY & INFORMATION SYSTEMS

Salzburg, 31 August – 02 September, 2016

GAMMA: Global AtM security MAnagement

- ***GAMMA project:*** FP7-SEC-2012-1
- ***Start Date / Duration:*** September 2013 – 48 months
- The GAMMA project stems from the growing need to address new air traffic management threats and vulnerabilities
- The goal of the GAMMA project is to develop solutions able to manage emerging ATM vulnerabilities, backed up by practical proposals for the implementation of these solutions.
- The GAMMA vision recognises the opportunities opened by a collaborative framework for managing security, building a solution based on the self-protection and resilience of the ATM system
- The project will also consider the new scenarios created by the Single European Sky programme

Consortium composition

- **8 Countries:**

- **19 partners:**

10 Large Industries

FINMECCANICA | AIRBUS | AIRBUS DEFENCE & SPACE | AIRBUS GROUP
BOEING | AIRBUS DEFENCE & SPACE CyberSecurity | THALES
Isdefe | THALES | ThalesAlenia Space

3 SMEs

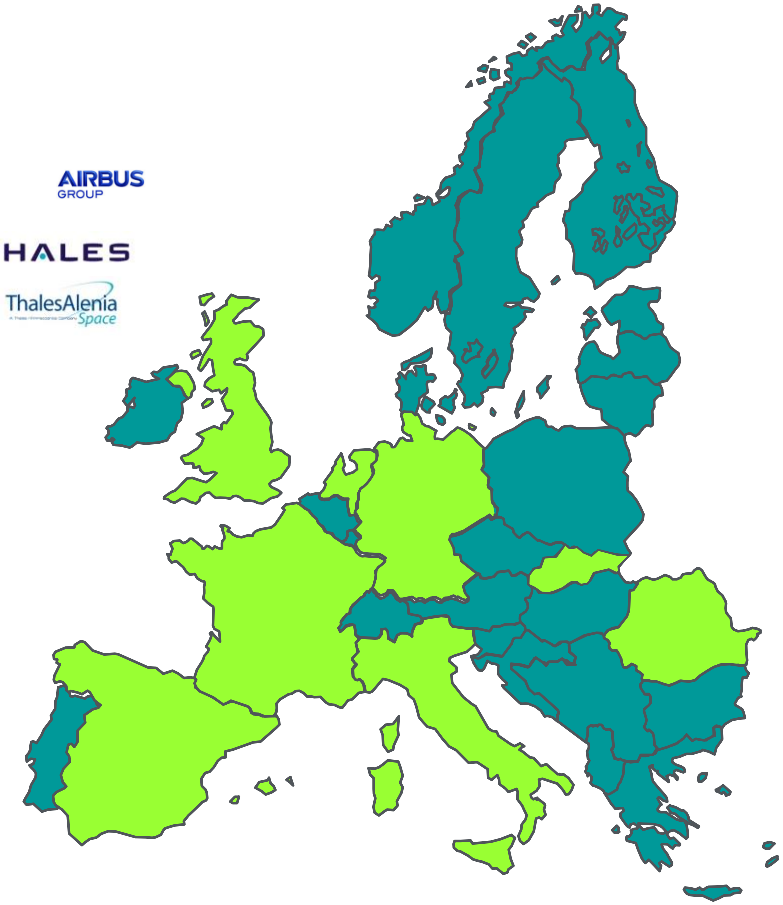
4i2 Solutions The ultimate answer | CiaoTech | RNC AVIONICS

3 Research org. and Universities

DLR | LANCASTER UNIVERSITY | INSTITUTE OF INFORMATICS SLOVAK ACADEMY OF SCIENCES

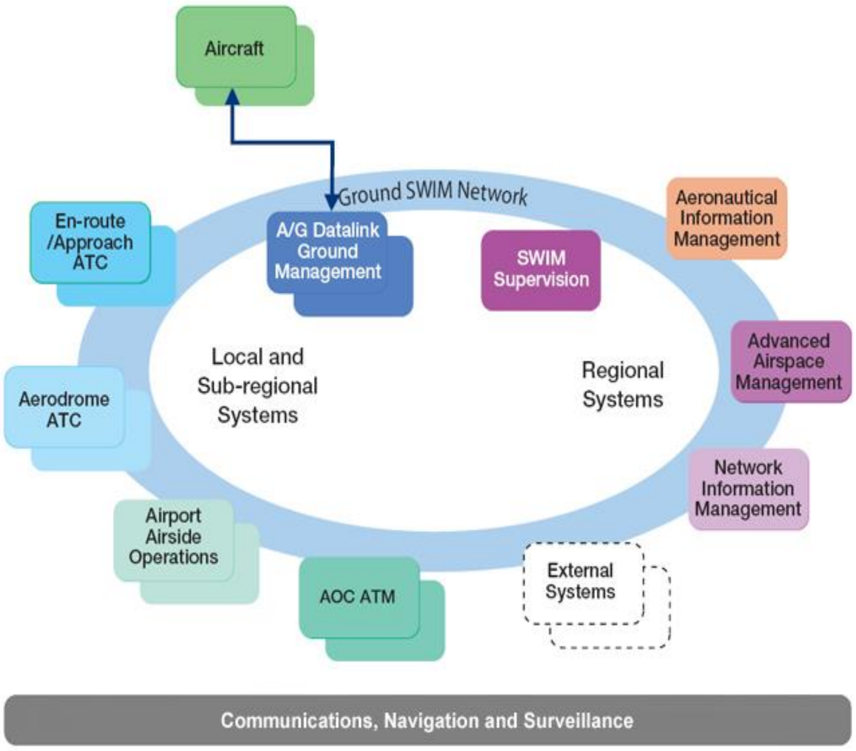
3 End-users

romatsa | ENAV | SEA



Why GAMMA?

The need for a holistic approach


Aircraft
Ground SWIM Network
En-route /Approach ATC
A/G Datalink Ground Management
SWIM Supervision
Aeronautical Information Management
Advanced Airspace Management
Local and Sub-regional Systems
Regional Systems
Aerodrome ATC
Network Information Management
Airport Airside Operations
AOC ATM
External Systems
Communications, Navigation and Surveillance

- ATM as a system of system
- Domino effects spreading security threats within ATM and beyond
- Security Life cycle: from threat prevention to crisis management

Security Threats in the ATM world

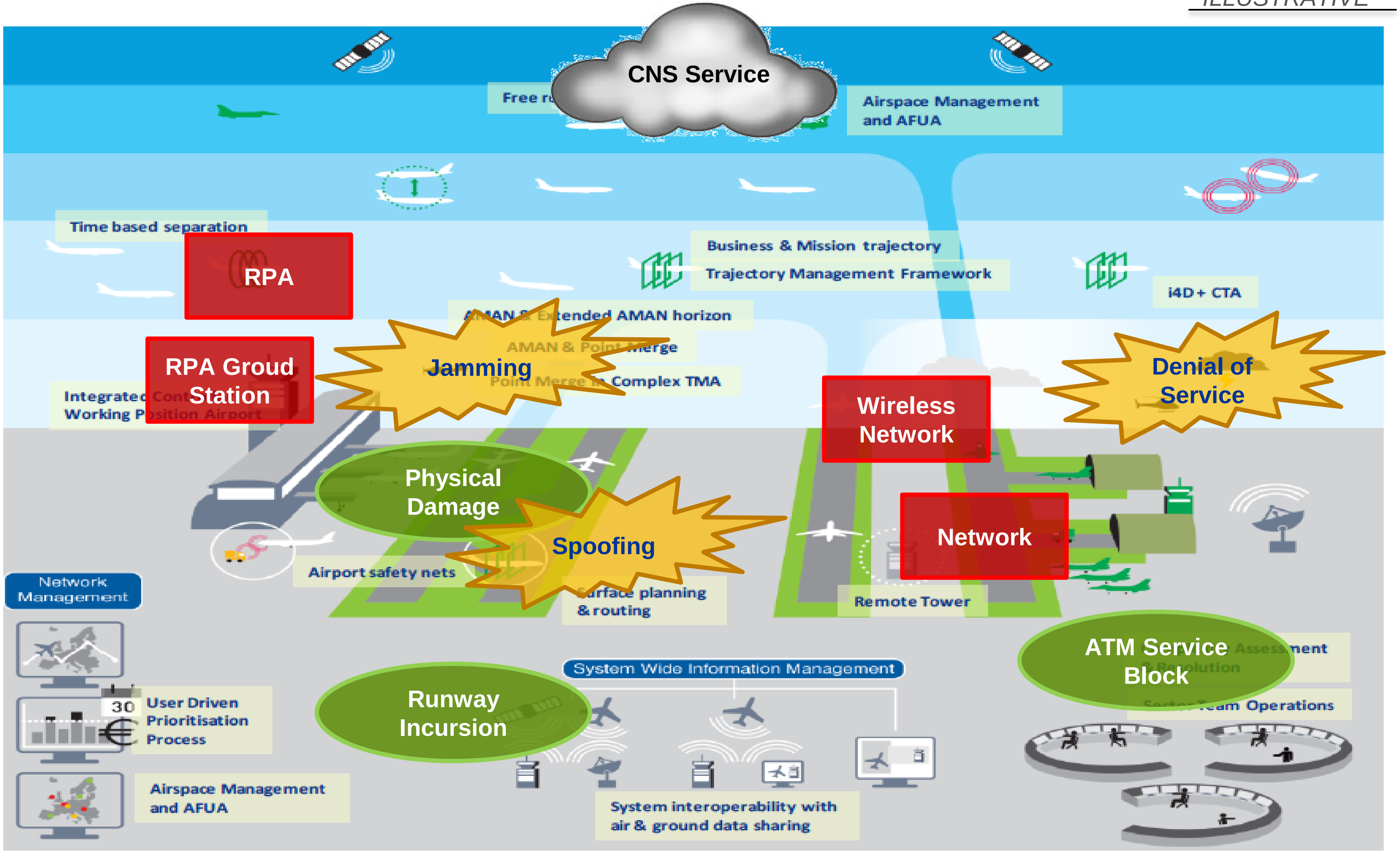
Primary asset

Supporting Assets

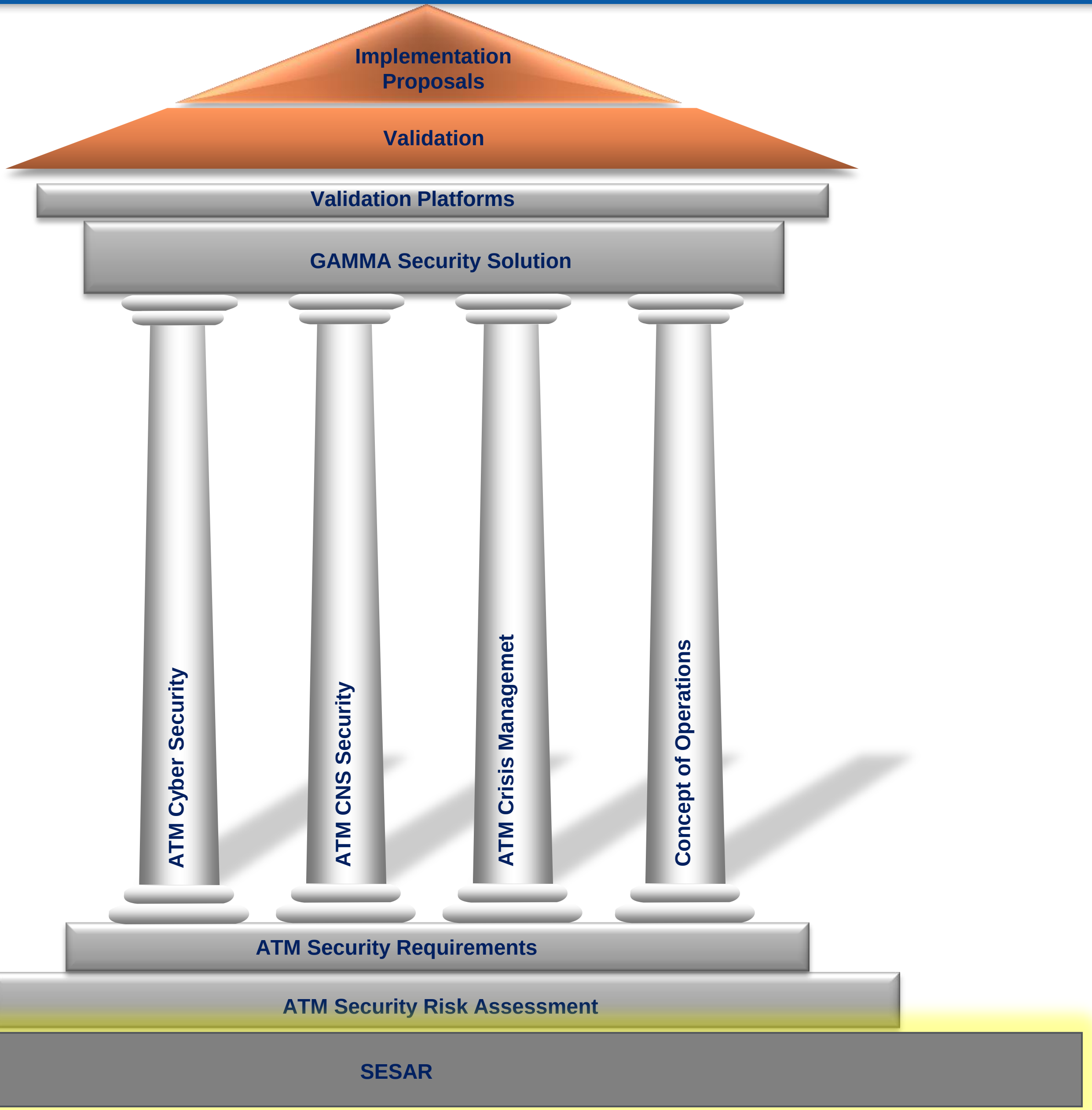
Threats

Impacts

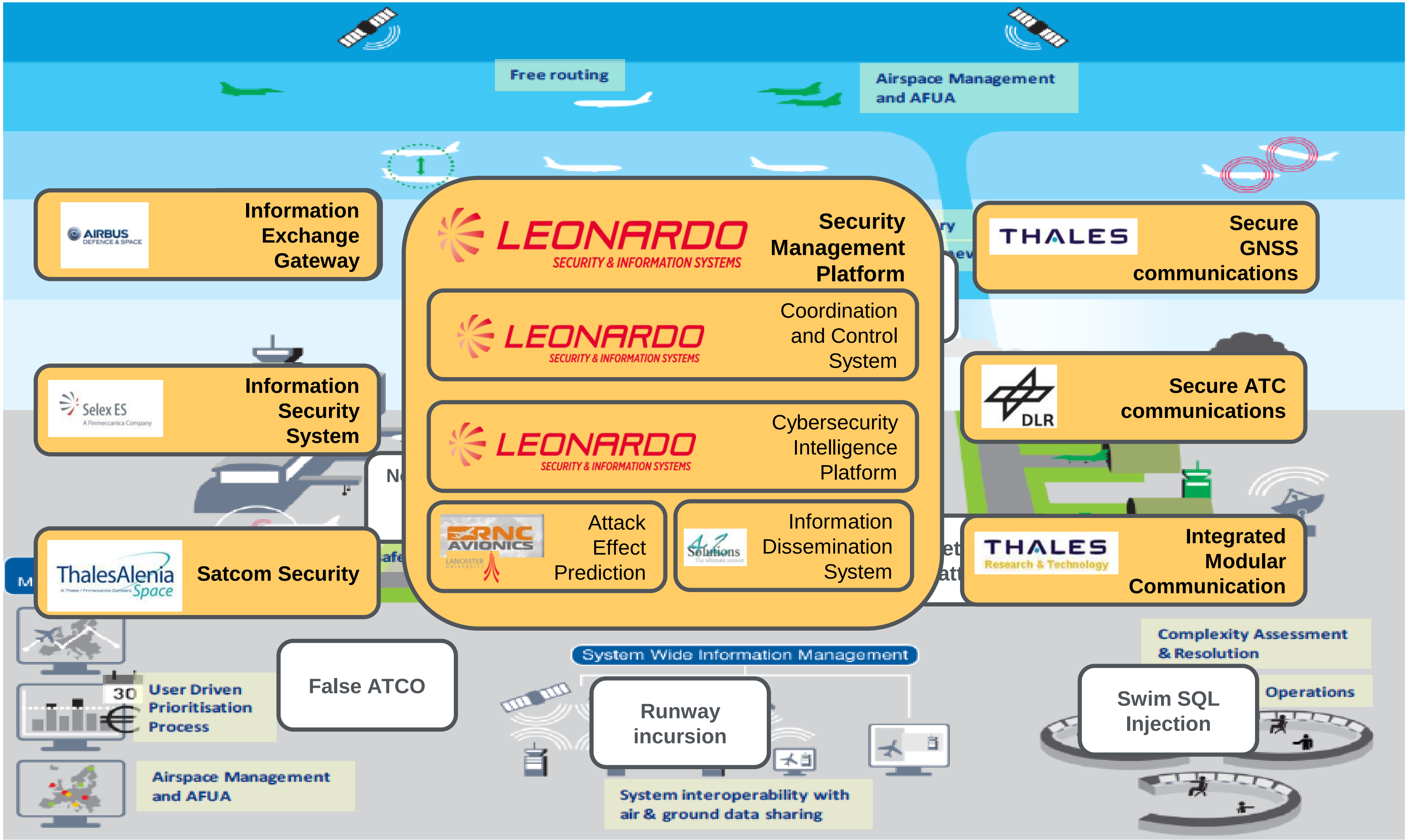
ILLUSTRATIVE


CNS Service
Free r
Airspace Management and AFUA
Time based separation
RPA
Business & Mission trajectory
Trajectory Management Framework
i4D + CTA
AMAN & Extended AMAN horizon
AMAN & Point Merge
Point Merge in Complex TMA
RPA Groud Station
Jamming
Integrated Controller Working Position Airport
Wireless Network
Denial of Service
Physical Damage
Spoofing
Network
Airport safety nets
Surface planning & routing
Remote Tower
Network Management
ATM Service Block
Assessment & Resolution
Sector Team Operations
System Wide Information Management
Runway Incursion
30
User Driven Prioritisation Process
Airspace Management and AFUA
System interoperability with air & ground data sharing

GAMMA building blocks



GAMMA prototypes



AIRBUS DEFENCE & SPACE – Information Exchange Gateway

Selex ES – Information Security System

ThalesAlenia Space – Satcom Security

LEONARDO SECURITY & INFORMATION SYSTEMS – Security Management Platform

LEONARDO SECURITY & INFORMATION SYSTEMS – Coordination and Control System

LEONARDO SECURITY & INFORMATION SYSTEMS – Cybersecurity Intelligence Platform

ERNC AVIONICS / LANCASTER UNIVERSITY – Attack Effect Prediction

4Solutions – Information Dissemination System

THALES – Secure GNSS communications

DLR – Secure ATC communications

THALES Research & Technology – Integrated Modular Communication

False ATCO

Runway incursion

Swim SQL Injection

Free routing
Airspace Management and AFUA
System Wide Information Management
Complexity Assessment & Resolution
Operations
30
User Driven Prioritisation Process
Airspace Management and AFUA
System interoperability with air & ground data sharing

The GAMMA Concept Of Operations

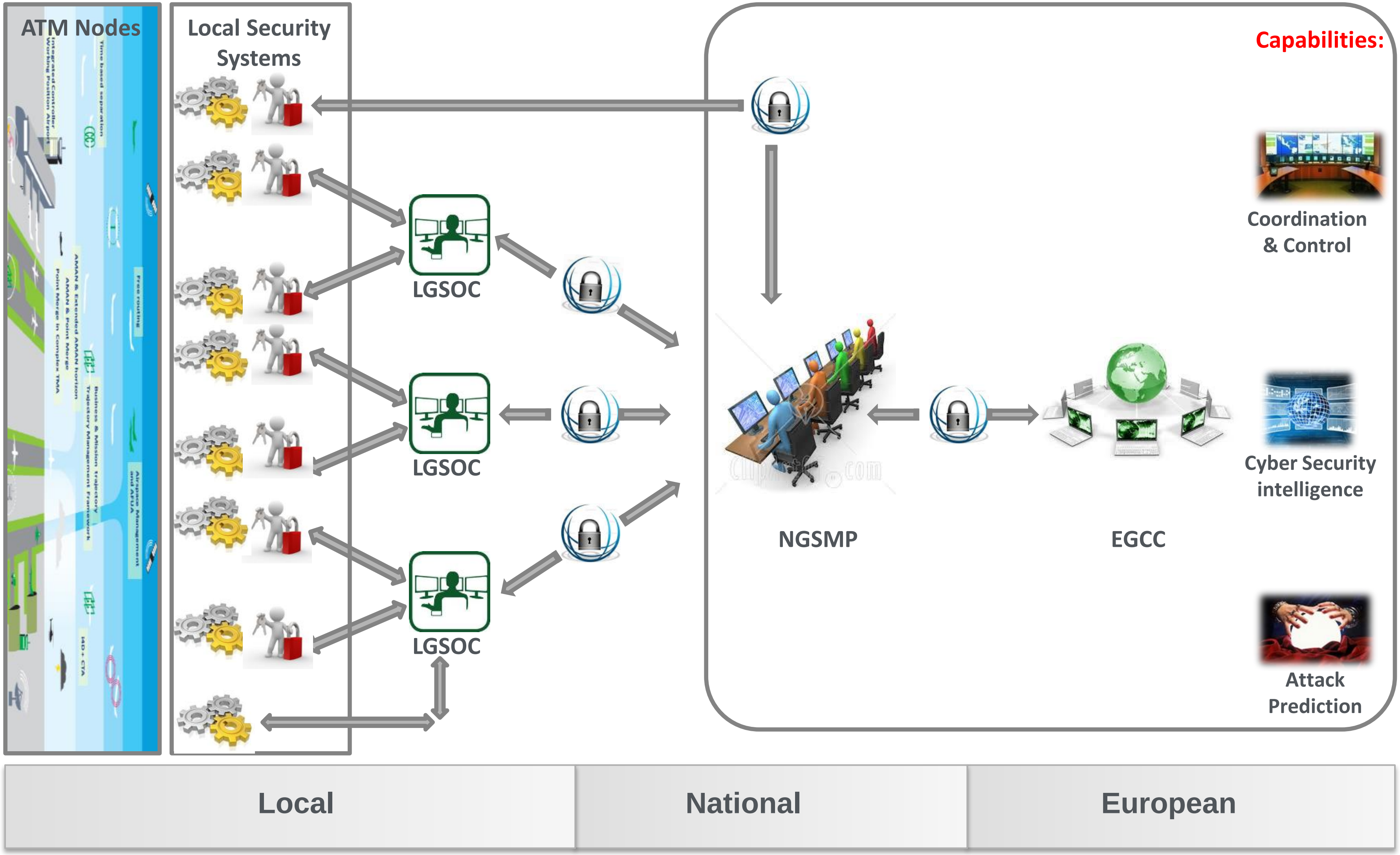
- The GAMMA Concept has been defined having in mind principles and concepts related to Security Management in a collaborative multi stakeholder environment

- The GAMMA solution can be conceptualised as a network of distributed nodes embedded within the ATM system and providing interfaces to (ATM) internal and external security stakeholders.

- GAMMA establishes three different levels for managing security:
  - ✓the **European** level represented by the European GAMMA Coordination Centre (EGCC),
  - ✓the **National** level represented by the National GAMMA Security Management Platform (NGSMP)
  - ✓the **local** level represented by local security systems as well as Local GAMMA Security Operation Centres (LGSOC).

GAMMA
GLOBAL ATM SECURITY MANAGEMENT

The GAMMA Concept



ATM Nodes

Local Security Systems

LGSOC

LGSOC

LGSOC

NGSMP

EGCC

Capabilities:

Coordination & Control

Cyber Security intelligence

Attack Prediction

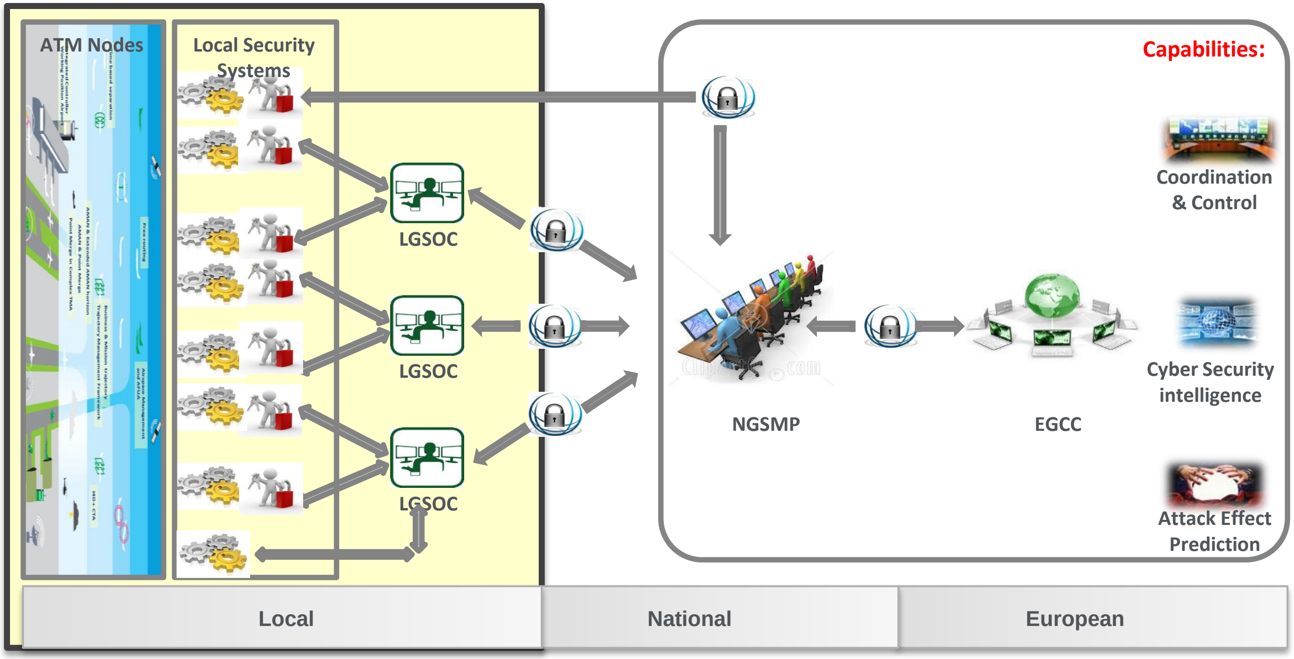
Local

National

European

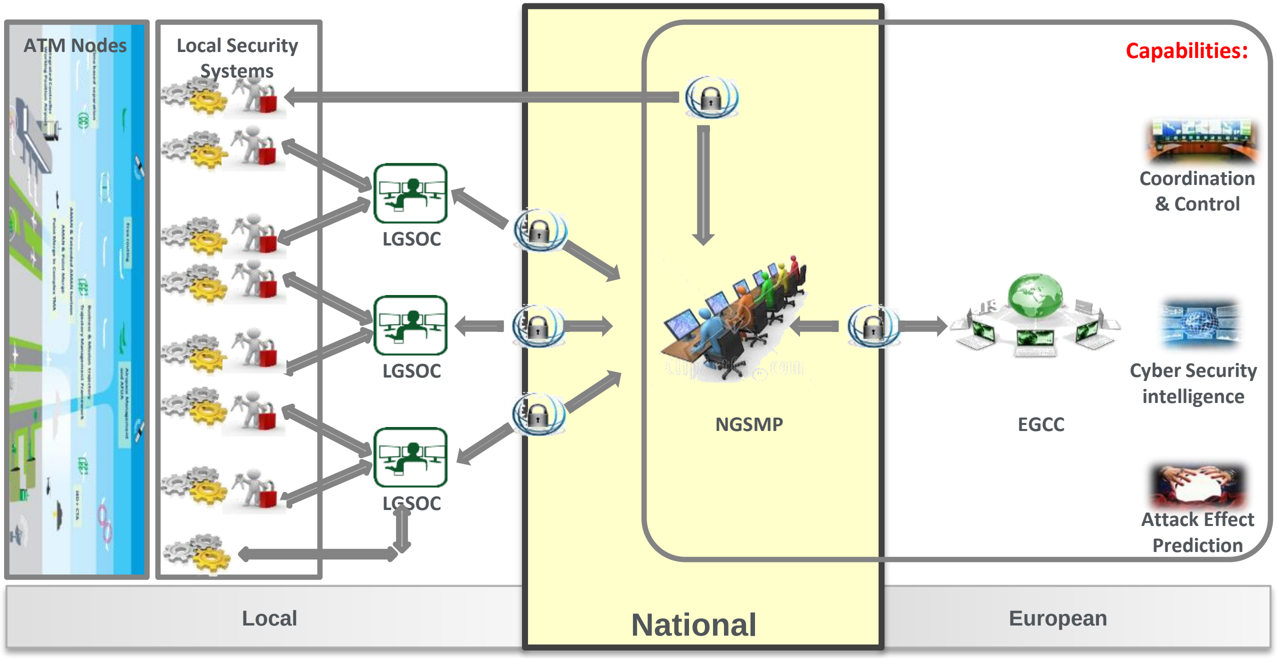
The GAMMA Concept: Local level

- The GAMMA solution is designed for seamless adaption and integration into the local ATM systems. For this reason the **local level** is represented by two types of solutions:
  - Local security systems embedded in the current or future ATM systems (and/or procedures) that address security aspects operating independently.
  - A specific GAMMA system (LGSOC) with access to the information defined within GAMMA to support the local security activities.



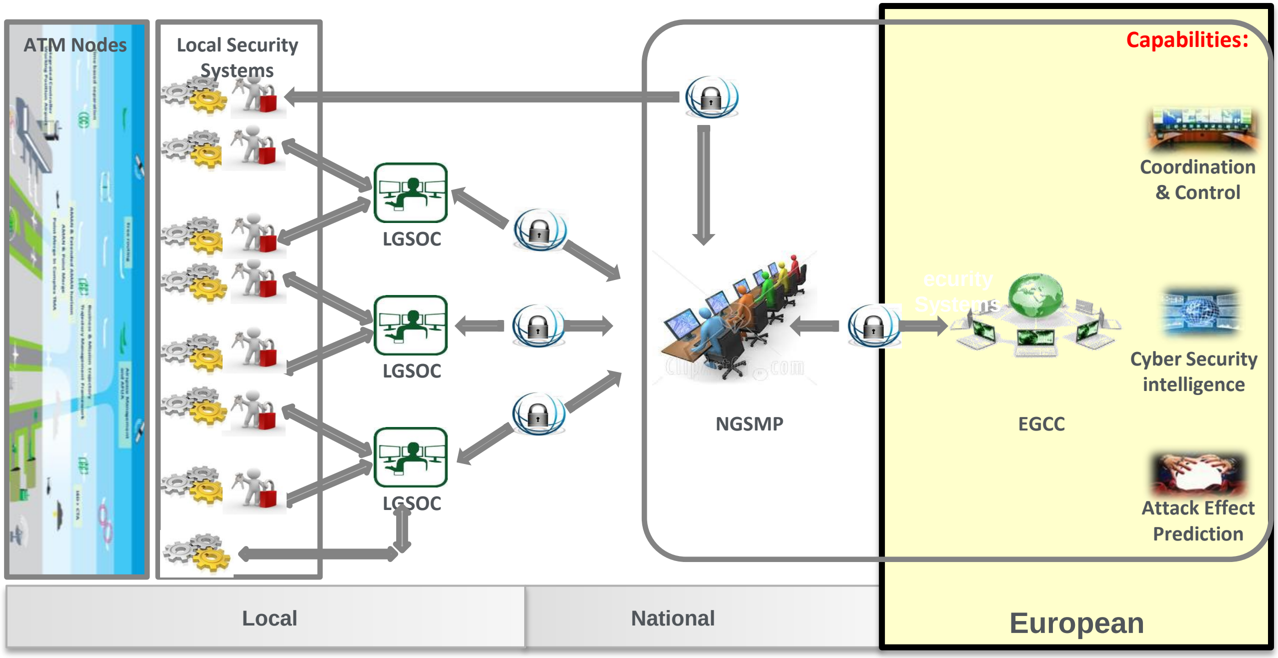
The GAMMA Concept: National level

- The **National level** will have the capability of processing and analysing the information received from the lower level through the operation of an information sharing platform (NGSMP) allowing the detection and prediction of attacks as well as proposing the corresponding alerts, actions or countermeasures and predicting corresponding impacts.



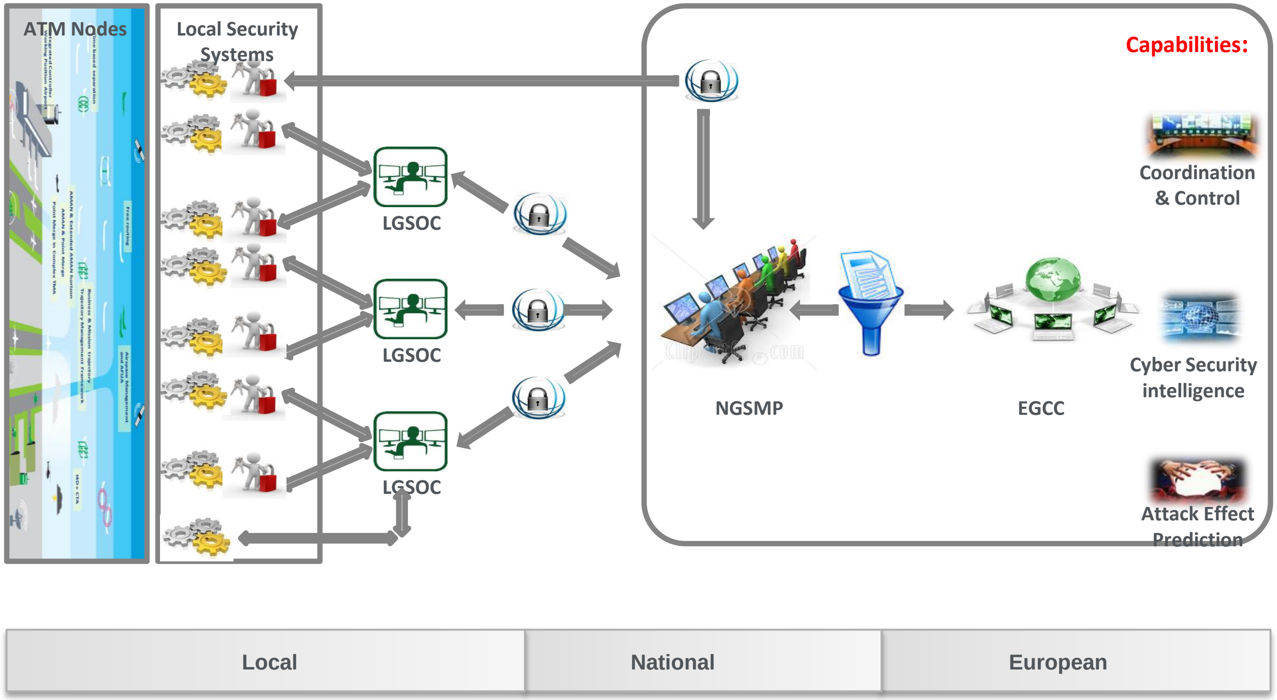
The GAMMA Concept: European level

- The **European Level** (EGCC) will enrich the opportunely sanitized information derived from the National level extending the cooperation platform through the operation of Cyber Intelligence functionalities in order to discover possible external threats related not only to the ATM environment but also to other services/systems whose disruption or destruction could cause domino effect on ATM.
- The EGCC will then be responsible for feeding such information to the NGSMP for further dissemination to the local levels.



The GAMMA Concept: The need for Sanitisation

- Sanitisation of information to be disseminated to European level should be seen as a prerequisite for the successful exploitation of collaborative environments within the existing regulatory framework.
- The sensitive information, generated at local and national level, that has to be disseminated to European level, can be (if necessary) opportunely modified so as to eliminate sensitive aspects. In the picture below the filter symbol represents where the sanitization process can be performed.



GAMMA

GLOBAL ATM SECURITY MANAGEMENT

Instantiation of GAMMA concept :

The Security Management Platform prototype

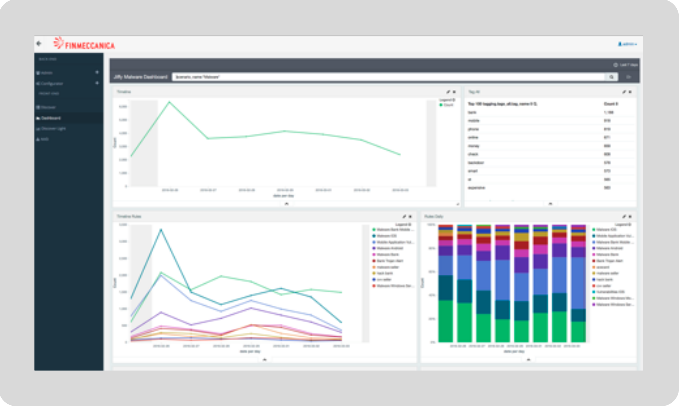
The role of SMP inside GAMMA solution

- SMP is the “core” of GAMMA concept, and will provide a basis for the management of security throughout the phases, from prevention to the identification of security incidents and the efficient resolution of the resulting ATM crises.
- The SMP is intended to provide Situational Awareness (applying cross-correlation techniques of events) and Decision Support functionalities supporting the coordinated management of ATM security.
- For this purpose the shared platform includes specific capabilities such as Cyber Security Intelligence and Attack Effect Prediction, in order to provide decision support to GAMMA operators.
- Moreover, the SMP includes an Information Dissemination System that allows the dissemination of security information through the multilevel architecture proposed by the GAMMA solution.

Security Management Platform: main functions (1/2)

- Coordination & Control System:
  - Provides Alarm Correlation, Security Monitoring and Decision Support for Incident/Crisis Management
  - A decision support function allows the operator to provide possible countermeasures to Local Security Systems or other SMPs.
  - A sanitization function is also available in order to opportunely modify sensitive information before transferring them to the IDS module for dissemination.

- Cyber Security Intelligence Platform:
  - provides GAMMA operators the possibility to obtain relevant information about possible (cyber) attacks on ATM systems, crawling the internet though open sources such as social networks, in order to determine the threats related to a particular target.
  - It allows also to identify the motivation, the characteristics and the identities of the attackers.

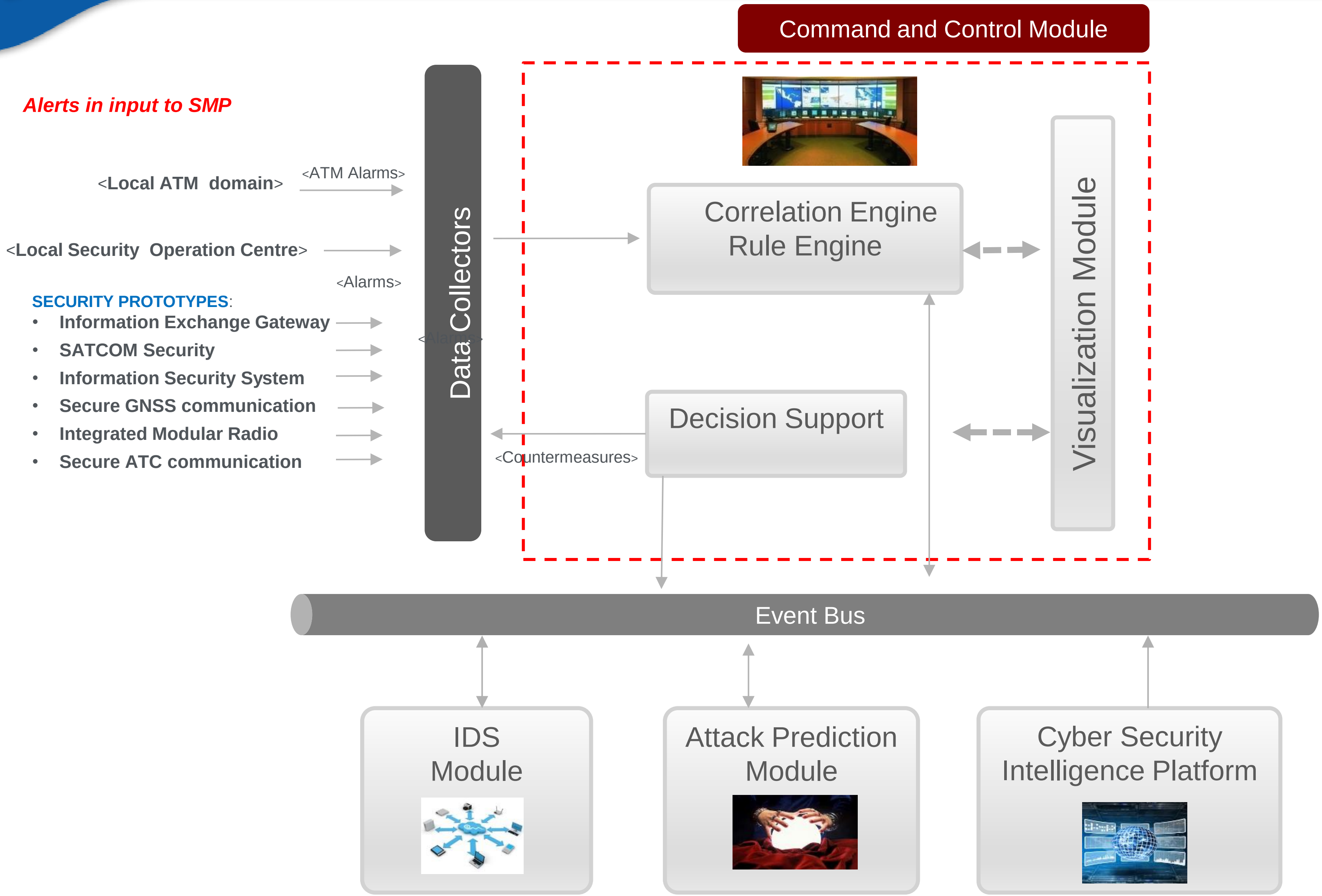


Security Management Platform: main functions (2/2)

- ## Attack Effect Prediction
  - Is a decision support SMP sub-system that provides a joint assessment of the information received from different sensors (event detectors)
  - It creates a directed graph structure to describe the ATM system encoding all Supporting Assets (SA) as a subset of nodes and all threat scenarios as a set of paths to the SAs, that form the graph
  - Additionally, an impact value for each type of attack for each security control is given (or a set of values for different Impact Areas).

- ## Information Dissemination System:
  - Disseminate automatically security reports from the SMP at European level to connected SMPs at National levels, applying (automatic) filtering conditions
  - Allow the SMP operator at National level to disseminate manually security reports to other connected Security Management Platforms at national or European level
  - Show security reports on both tabular and geographical presentations and security critical subjects (e.g. aircraft, network trunk/nodes, critical infrastructures) on the concise situational awareness display allowing for early detection of potential causality/escalation.

Security Management Platform architectural lay out



Alerts in input to SMP

<Local ATM domain> <ATM Alarms>

<Local Security Operation Centre> <Alarms>

SECURITY PROTOTYPES:

- Information Exchange Gateway
- SATCOM Security
- Information Security System
- Secure GNSS communication
- Integrated Modular Radio
- Secure ATC communication

SMP inputs-outputs

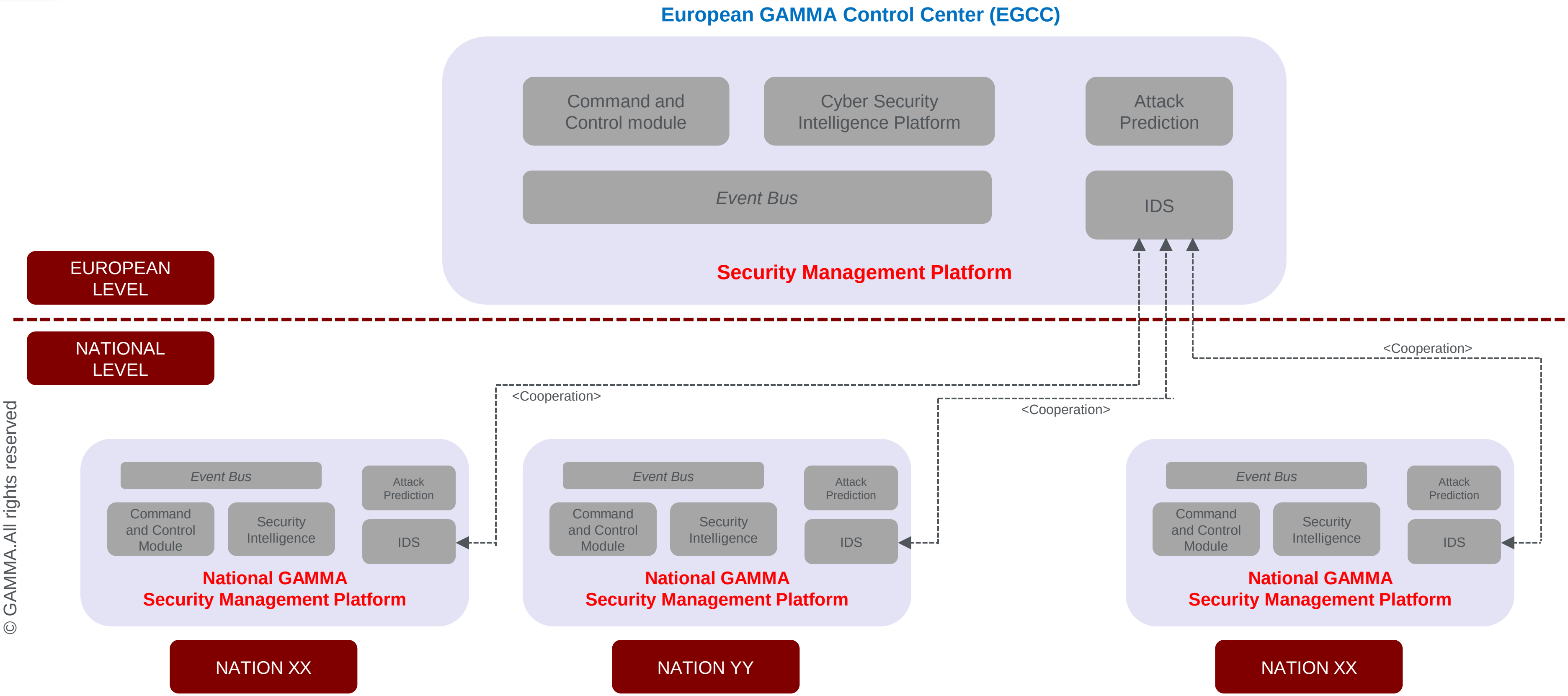
- SMP receives input from:
  - ✓ Local Security Systems (LGSOC or other Prototypes) (security events / detections)
  - ✓ ATC systems (alerts from systems within the ATM domain)
  - ✓ Other SMPs (disseminated alerts / messages)
  - ✓ The internet (open source information about possible attacks in social networks, chats, etc.)

- SMP ouputs are
  - ✓ Security reports (to Local Security Systems or to other SMP)
  - ✓ Correlated alarms due to the correlation function
  - ✓ Recommended Countermeasures (to Local Security Systems or to other SMP)
  - ✓ Attack effect prediction reports (to Local Security Systems or to other SMPs)
  - ✓ Alarm clearing (to some other Prototypes)

The role of SMP in the GAMMA solution

- The SMP plays a central role in the GAMMA concept
- The GAMMA concept can be conceptualised as a network of distributed nodes embedded within the ATM system and providing interfaces to (ATM) internal and external security stakeholders.
- As described before, GAMMA establishes three different levels for managing security:
  - ✓the **European** level represented by the European GAMMA Coordination Centre (EGCC),
  - ✓the **National** level represented by the National GAMMA Security Management Platform (NGSMP)
  - ✓the **Local** level represented by local security systems as well as Local GAMMA Security Operation Centers (LGSOC).
- SMP deployment:
  - ✓ One instance at **European** Level in the European GAMMA Coordination Centre (EGCC)
  - ✓One instance **for each Nation** (NGSMP)

The SMP in the multilayer approach of GAMMA solution


European GAMMA Control Center (EGCC)
Command and Control module
Cyber Security Intelligence Platform
Attack Prediction
Event Bus
IDS
Security Management Platform
EUROPEAN LEVEL
NATIONAL LEVEL
<Cooperation>
<Cooperation>
<Cooperation>
Event Bus
Attack Prediction
Command and Control Module
Security Intelligence
IDS
National GAMMA Security Management Platform
NATION XX
Event Bus
Attack Prediction
Command and Control Module
Security Intelligence
IDS
National GAMMA Security Management Platform
NATION YY
Event Bus
Attack Prediction
Command and Control Module
Security Intelligence
IDS
National GAMMA Security Management Platform
NATION XX

Conclusions: GAMMA Concept and Vision

- The most important concept of the GAMMA project, implemented by the federated architecture of the Security Management Platforms, is the sharing of security information between ATM stakeholders.
- The SMP architectural vision enlarges the scope for cooperative management of ATM security while assuring controlled sharing of information, which is fundamental for its acceptance in a multinational context
- The GAMMA concept opens the way for managing ATM security at European level, proposing (but not enforcing) recommendations on actions or measures to be taken at lower levels, in line with existing principles of national sovereignty and responsibilities over security issues.
- The SMP is an enabler for the implementation of this concept, and can be adopted for the management of ATM security as well as the management of security in any federated environment (i.e. military domain)

Contact Info

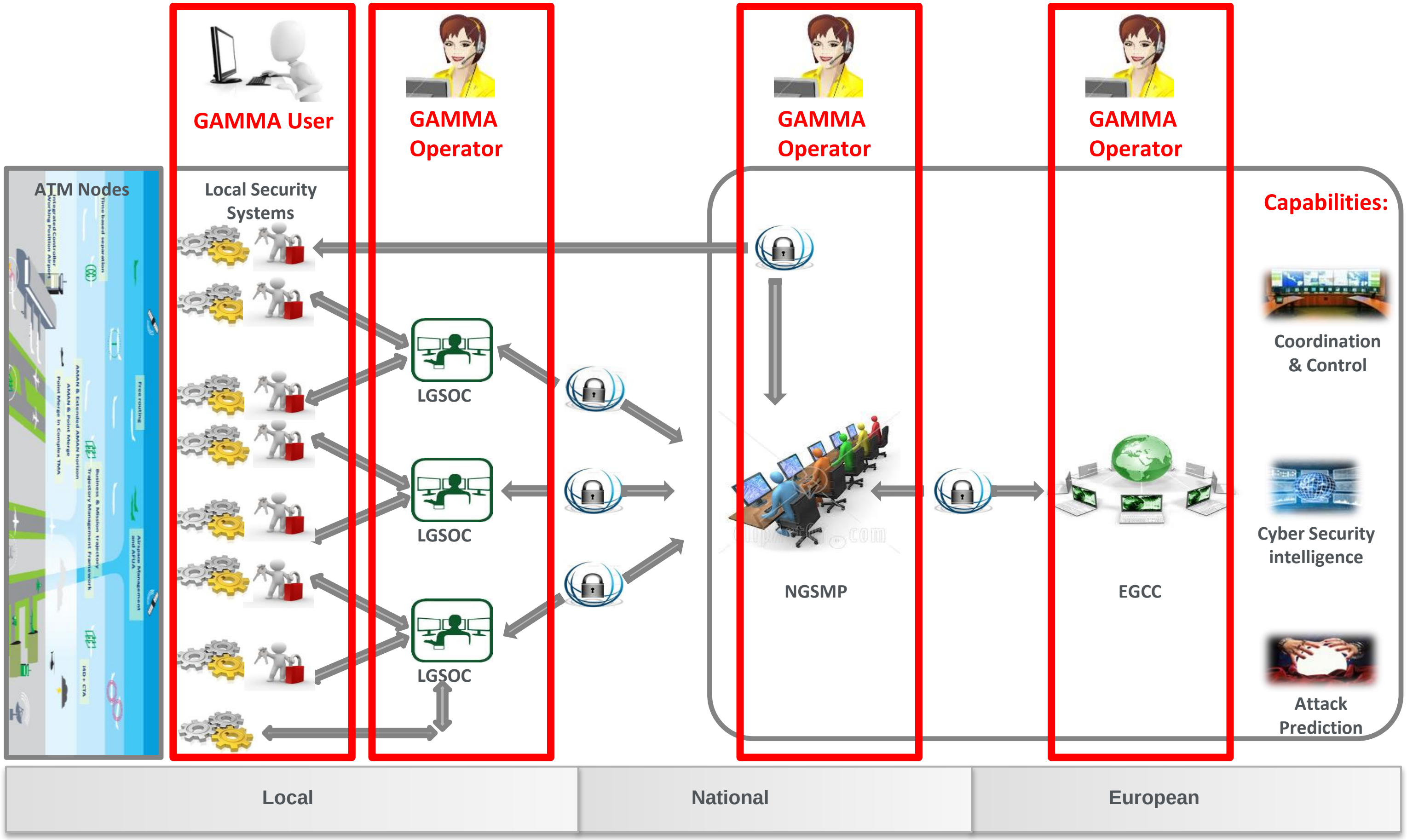
Claudio Porretti
Leonardo S.p.A. – Security and Information Systems division
CTO/Capability – Cyber Security & ICT Solutions
Via Laurentina, 760 – Roma - 00143 - Italy
Tel. +39 06 5027 4634 / +39 335 7743574
claudio.porretti@leodardocompany.com

Company web site: www.leodardocompanycom

Project web site: www.gamma-project.eu

The GAMMA Concept: human roles

- Two different human roles are considered within the GAMMA concept:
  - GAMMA Operators, represented by actors performing functions within the LGSOC, NGSMP and EGCC
  - GAMMA Users, represented by Users of the local security systems.


GAMMA User
GAMMA Operator
GAMMA Operator
GAMMA Operator
ATM Nodes
Local Security Systems
Capabilities:
LGSOC
LGSOC
LGSOC
NGSMP
EGCC
Coordination & Control
Cyber Security intelligence
Attack Prediction
Local
National
European