GAMMA

GLOBAL ATM SECURITY MANAGEMENT

GAMMA Overview

Consortium Composition

- **8 Countries**

- **19 partners:**

10 Large Industries

Selex ES
A Finmeccanica Company

AIRBUS

AIRBUS
DEFENCE & SPACE

AIRBUS
GROUP

BOEING

AIRBUS
DEFENCE & SPACE
CyberSecurity

THALES

Isdefe

THALES

ThalesAlenia
Space

3 SMEs

4-Solutions
The ultimate answer

CiaoTech

RNC
AVIONICS

3 Research org. and Universities

DLR

LANCASTER
UNIVERSITY

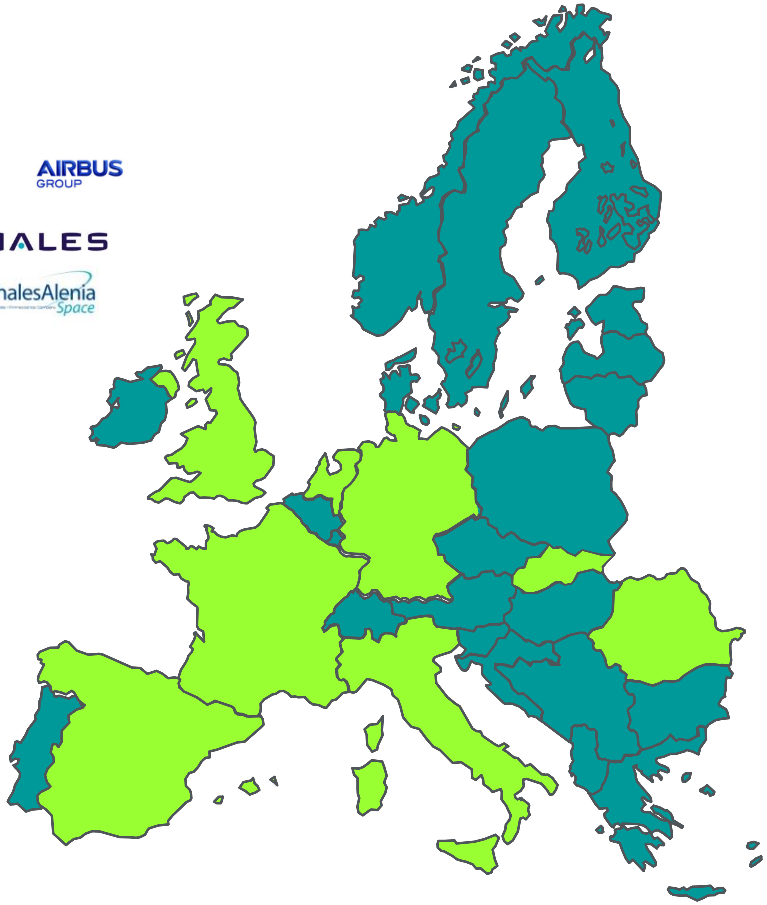
INSTITUTE OF INFORMATICS
SLOVAK ACADEMY OF SCIENCES

3 End-users

romatsa

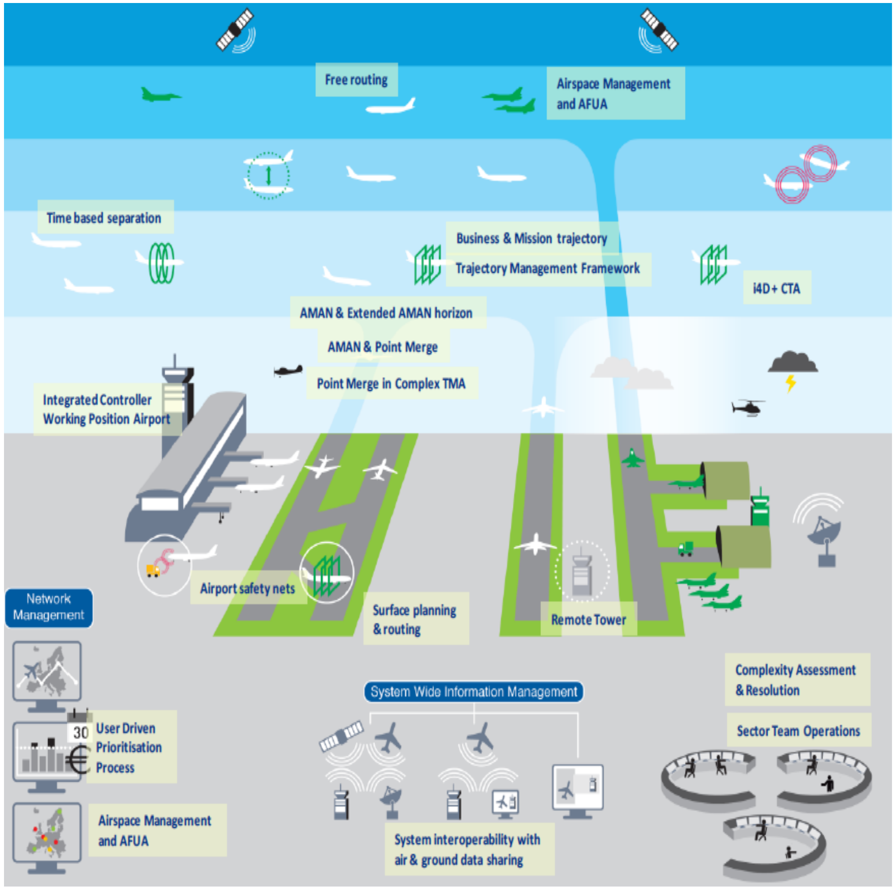
ENAV

SEA



Why GAMMA?

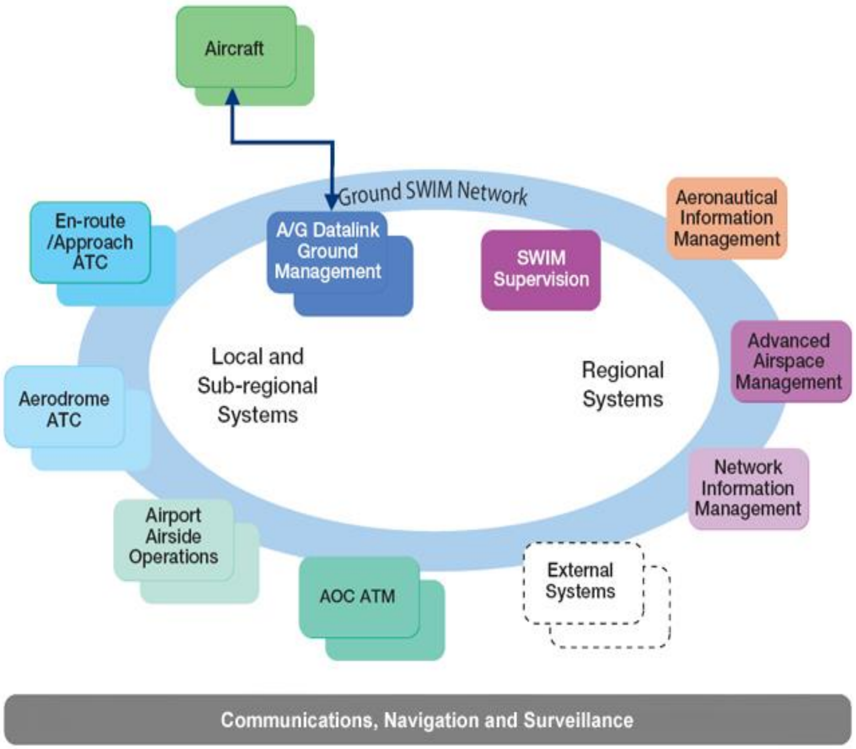
New Vulnerabilities


Free routing
Airspace Management and AFUA
Time based separation
Business & Mission trajectory
Trajectory Management Framework
i4D+ CTA
AMAN & Extended AMAN horizon
AMAN & Point Merge
Point Merge in Complex TMA
Integrated Controller Working Position Airport
Airport safety nets
Surface planning & routing
Remote Tower
Network Management
System Wide Information Management
Complexity Assessment & Resolution
Sector Team Operations
30 User Driven Prioritisation Process
Airspace Management and AFUA
System interoperability with air & ground data sharing

- While SESAR will improve performance and dependability of ATM, it will open the way to new vulnerabilities due, for instance, to:
  - increased reliance on distributed enterprise computing
  - automated flow of information across a ground and airborne network
- Cyber attacks will come from many sources and will have a range of possible targets, including civilian, commercial and military systems to damage critical services

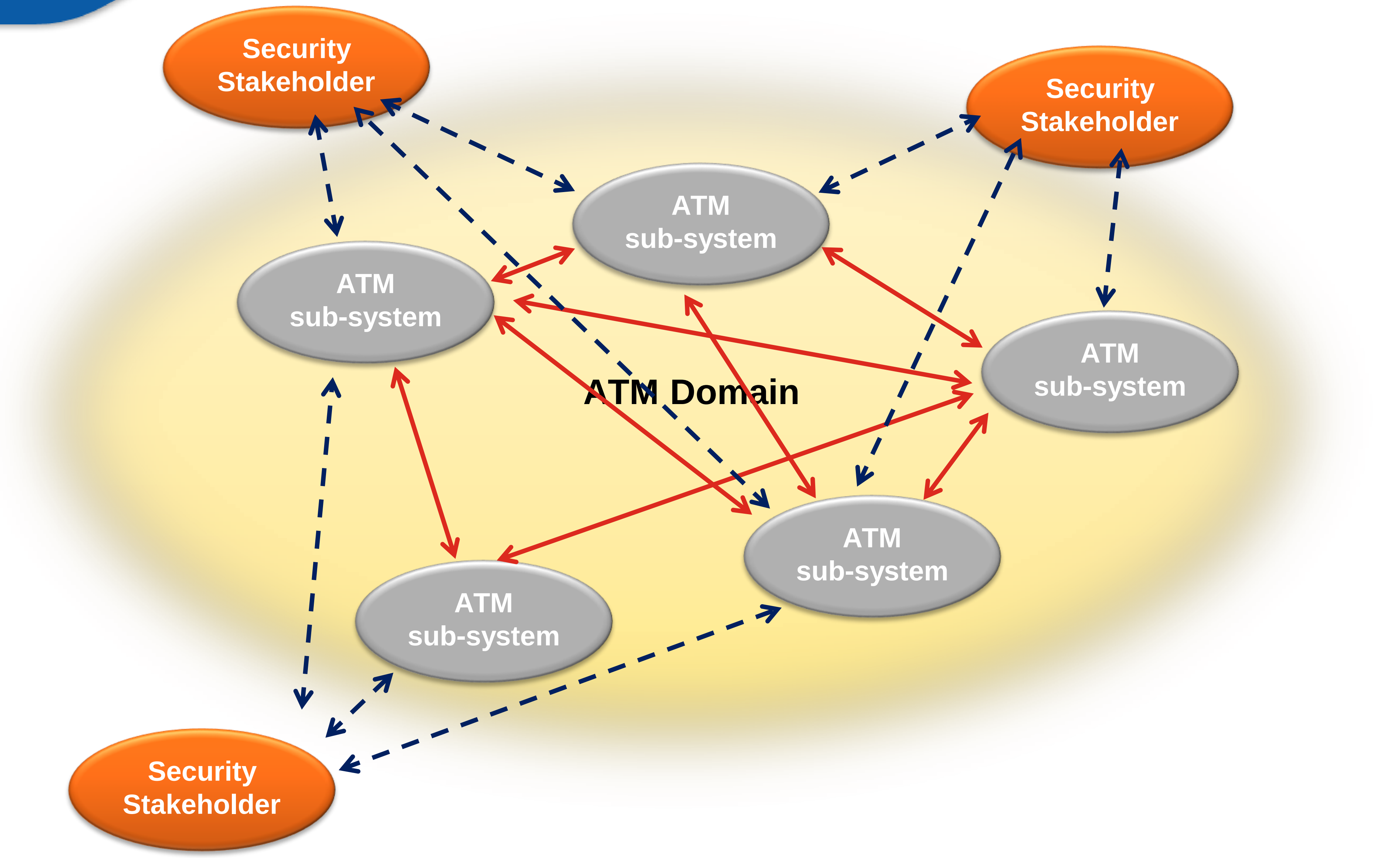
Why GAMMA?

The need for a holistic approach

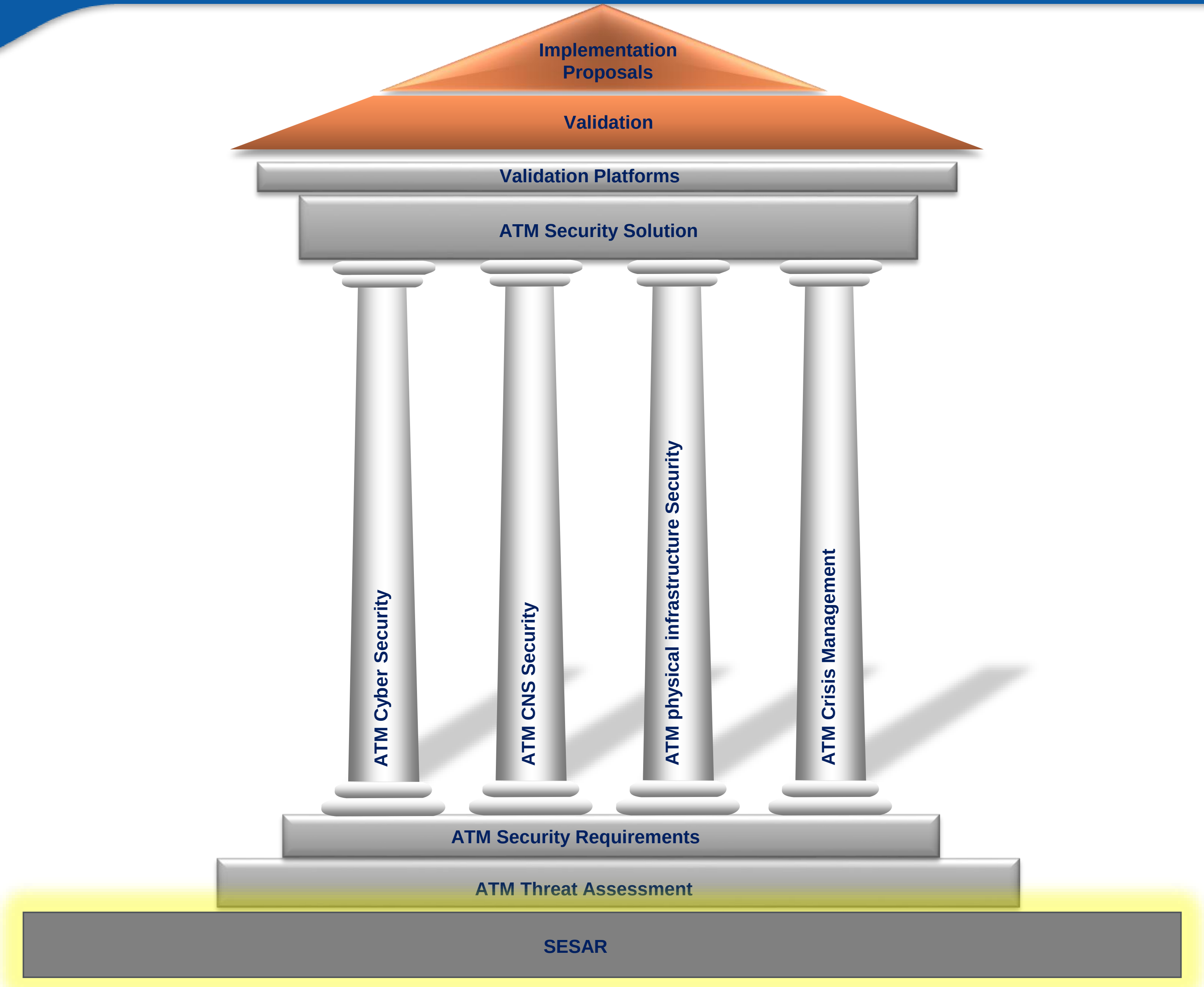

Aircraft
Ground SWIM Network
En-route /Approach ATC
A/G Datalink Ground Management
SWIM Supervision
Aeronautical Information Management
Advanced Airspace Management
Local and Sub-regional Systems
Regional Systems
Aerodrome ATC
Network Information Management
Airport Airside Operations
AOC ATM
External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

GAMMA scope and positioning: an end to end approach



GAMMA: a Helicopter view


Implementation Proposals

Validation

Validation Platforms

ATM Security Solution

ATM Cyber Security

ATM CNS Security

ATM physical infrastructure Security

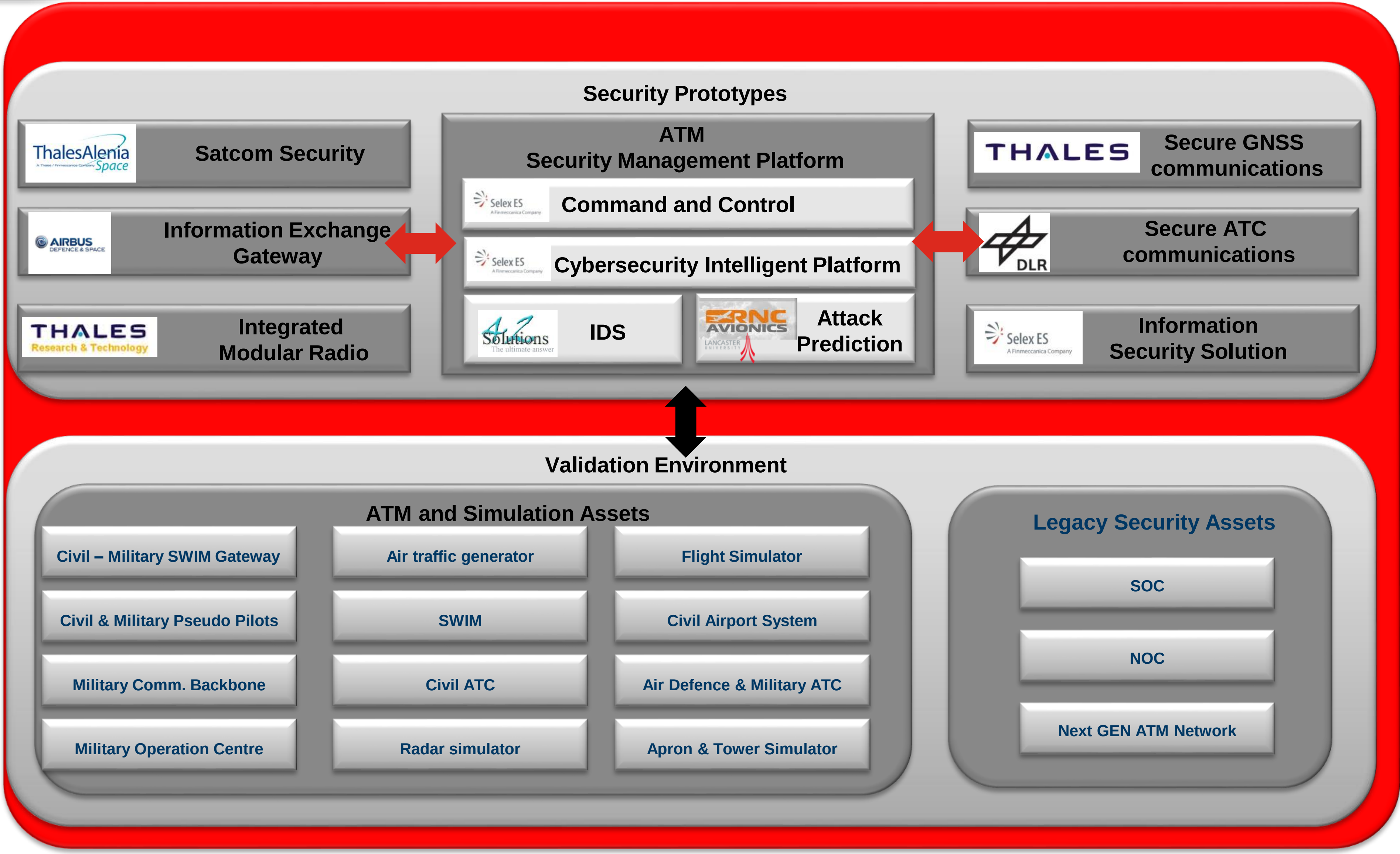
ATM Crisis Management

ATM Security Requirements

ATM Threat Assessment

SESAR

GAMMA Validation Platform



Security Prototypes

- Satcom Security
- Information Exchange Gateway
- Integrated Modular Radio

ATM Security Management Platform

- Command and Control
- Cybersecurity Intelligent Platform
- IDS
- Attack Prediction

- Secure GNSS communications
- Secure ATC communications
- Information Security Solution

Validation Environment

ATM and Simulation Assets

Civil – Military SWIM Gateway	Air traffic generator	Flight Simulator
Civil & Military Pseudo Pilots	SWIM	Civil Airport System
Military Comm. Backbone	Civil ATC	Air Defence & Military ATC
Military Operation Centre	Radar simulator	Apron & Tower Simulator

Legacy Security Assets

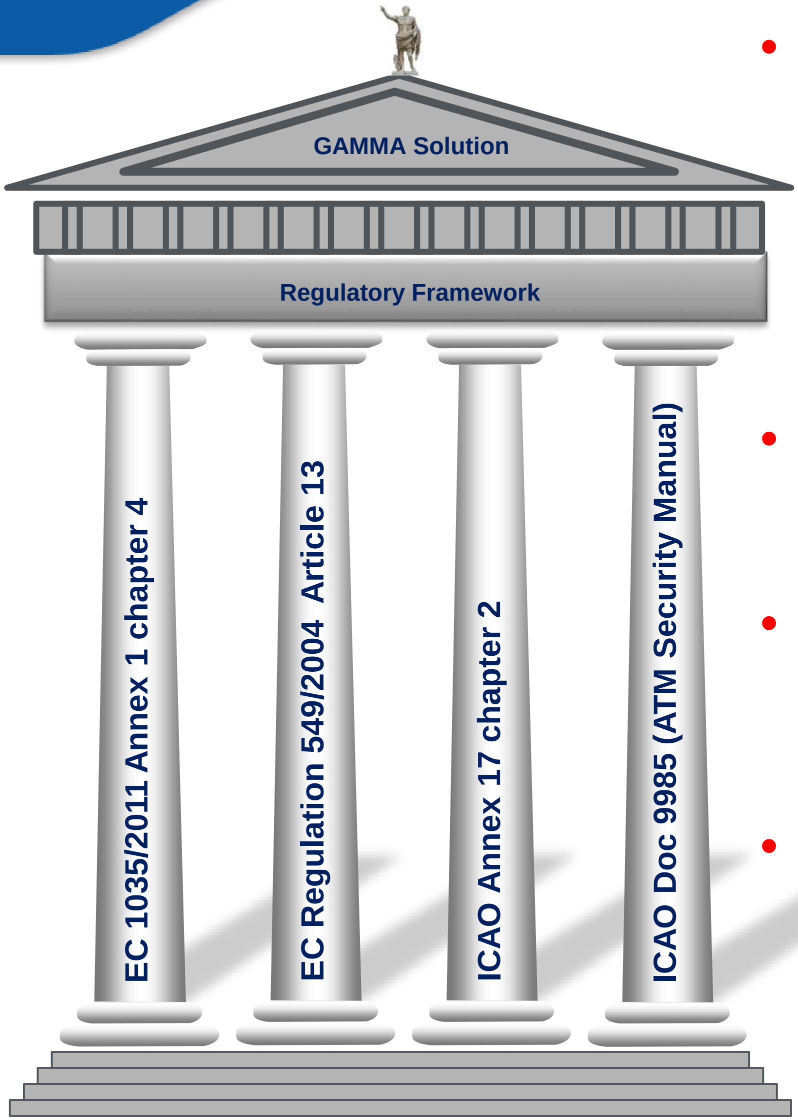
- SOC
- NOC
- Next GEN ATM Network

GAMMA

GLOBAL ATM SECURITY MANAGEMENT

The GAMMA Vision:
Concept of Operations

ATM Security Regulatory Framework: GAMMA Pillars


GAMMA Solution
Regulatory Framework
EC 1035/2011 Annex 1 chapter 4
EC Regulation 549/2004 Article 13
ICAO Annex 17 chapter 2
ICAO Doc 9985 (ATM Security Manual)

- **EC 1035/2011 Annex 1 chapter 4:**

  «Air navigation service providers shall establish a security management system to ensure:

  - the security of their facilities and personnel so as to prevent unlawful interference with the provision of air navigation services;
  - the security of operational data they receive or produce or otherwise employ, so that access to it is restricted only to those authorized.“

- **EC Regulation 549/2004 Article 13:**

  Security governance is a State matter and Member States have the power to implement appropriate measures to safeguard the public.

- **ICAO Annex 17 chapter 2:**

  “Each Contracting State shall establish and implement procedures to share with other Contracting States threat information that applies to the aviation security interests of those States, to the extent practicable.”

- **ICAO Doc 9985 (ATM Security Manual)**

  ““It provides guidance on ATM security issues to assist States and ATSPs in implementing appropriate security provisions to meet the published requirements of the NCASP. It also provides guidance to the ATSP on provision of ATM security services in support of national security and law enforcement requirements, and guidance on protection of the ATM system infrastructure from threats and vulnerabilities”.

The GAMMA Solution

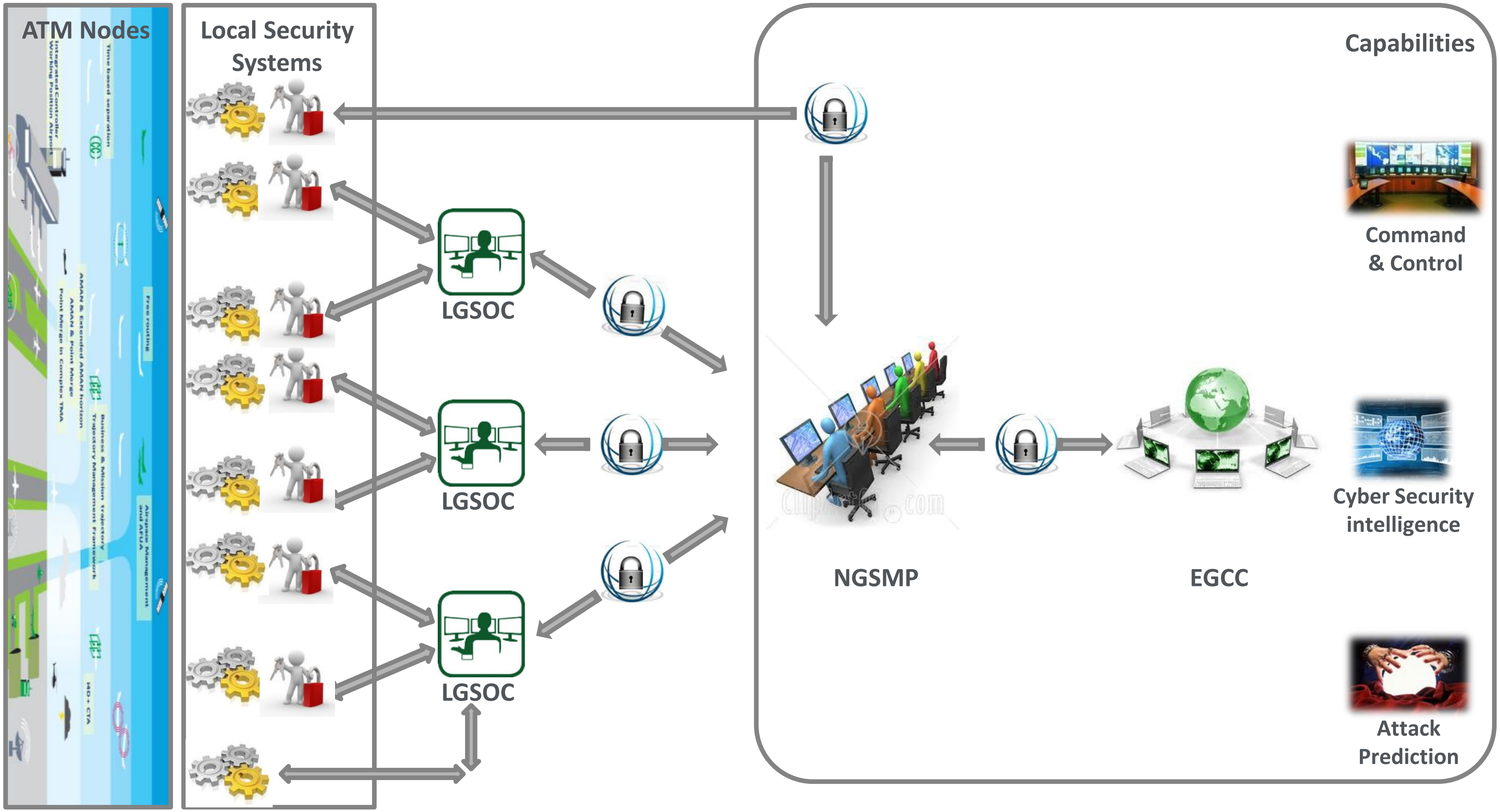
- The operational and technical scope of the GAMMA vision is given by the existing ATM system and its evolution foreseen within SESAR.

- 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 Solution



ATM Nodes

Local Security Systems

LGSOC

LGSOC

LGSOC

Capabilities

NGSMP

EGCC

Command & Control

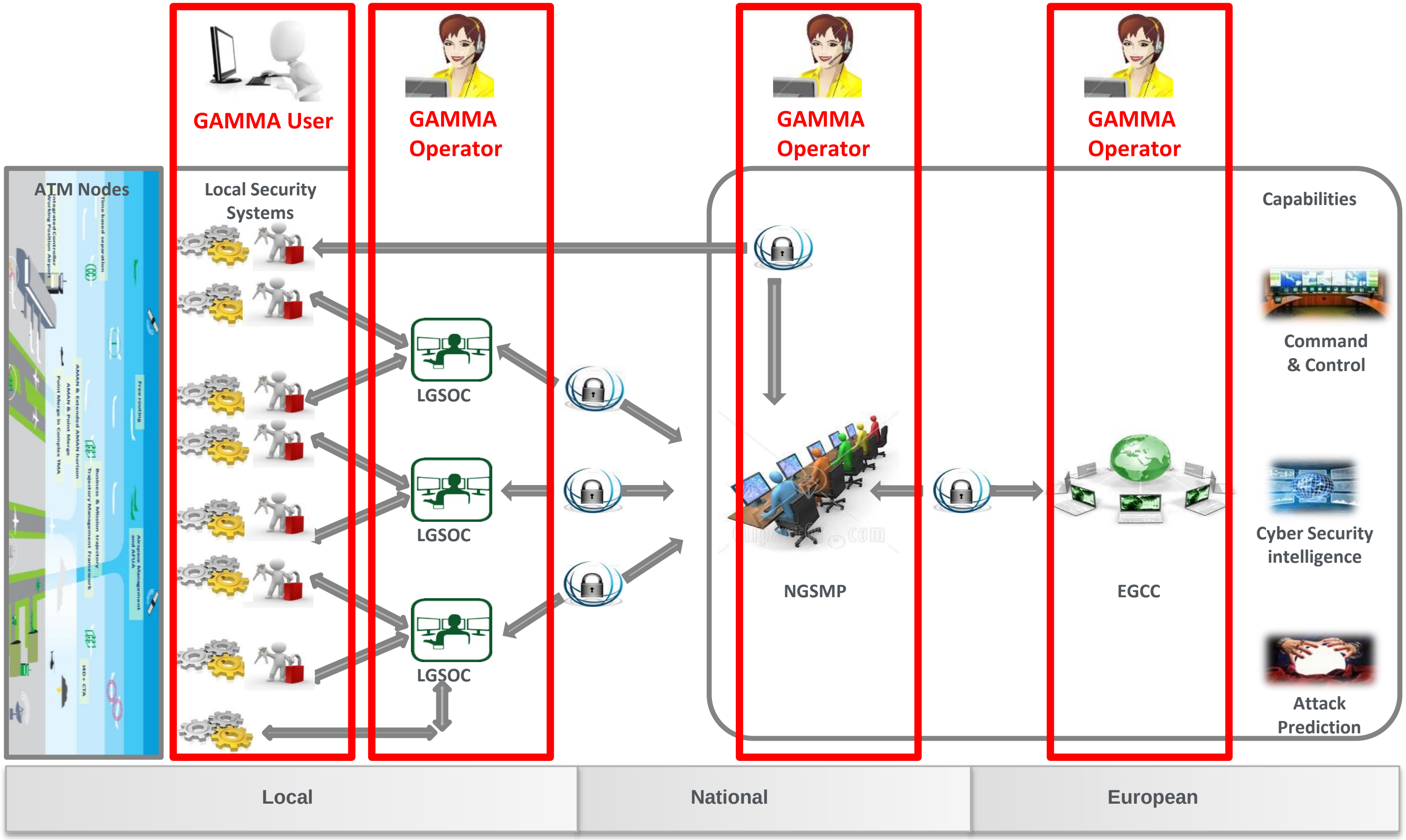
Cyber Security intelligence

Attack Prediction

Local	National	European

The GAMMA Solution

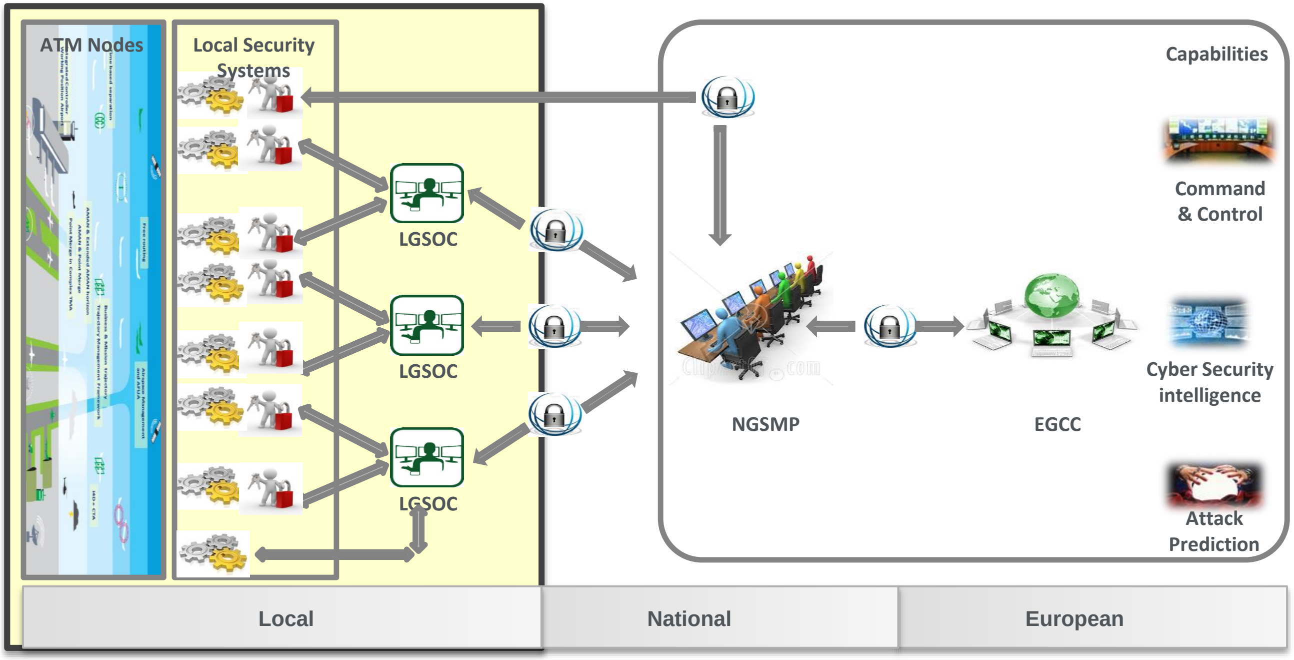
- Two different human roles are considered within the GAMMA concept:
  - GAMMA Operators, represented by actors performing functions within the LGSOC, NGSMP and EGCC
  - GAMMA Users, represented by Users of the local security systems.



GAMMA GLOBAL ATM SECURITY MANAGEMENT

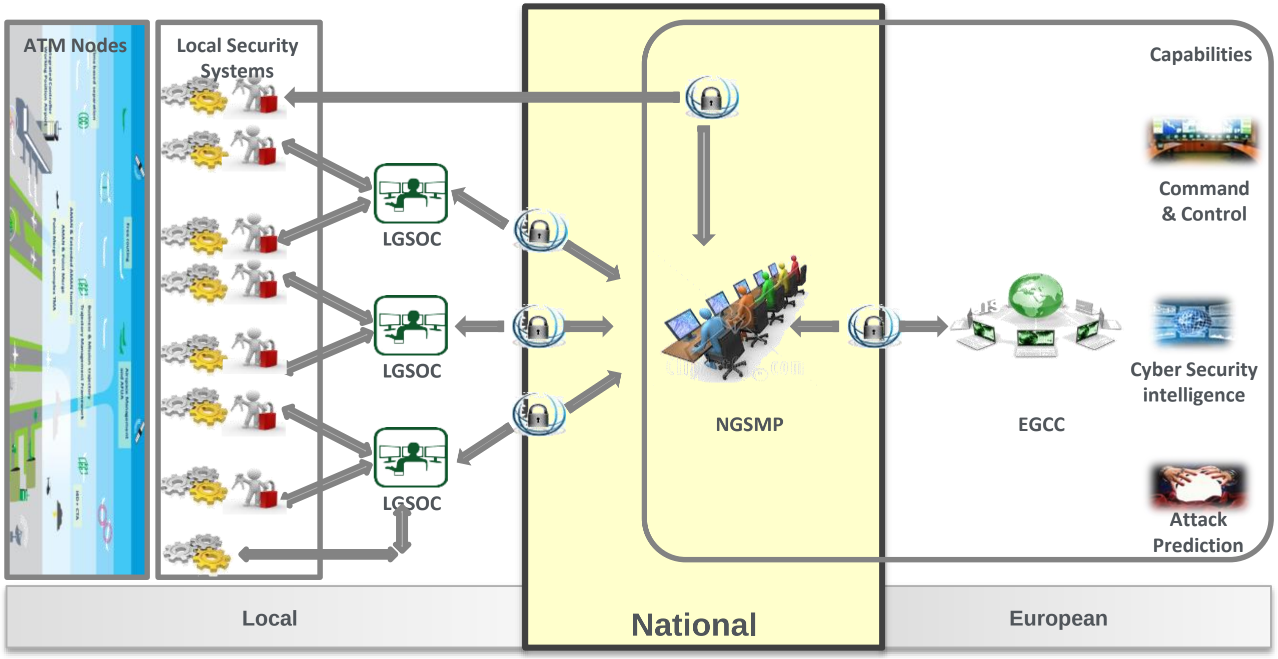
The GAMMA Solution: Local level

- 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.



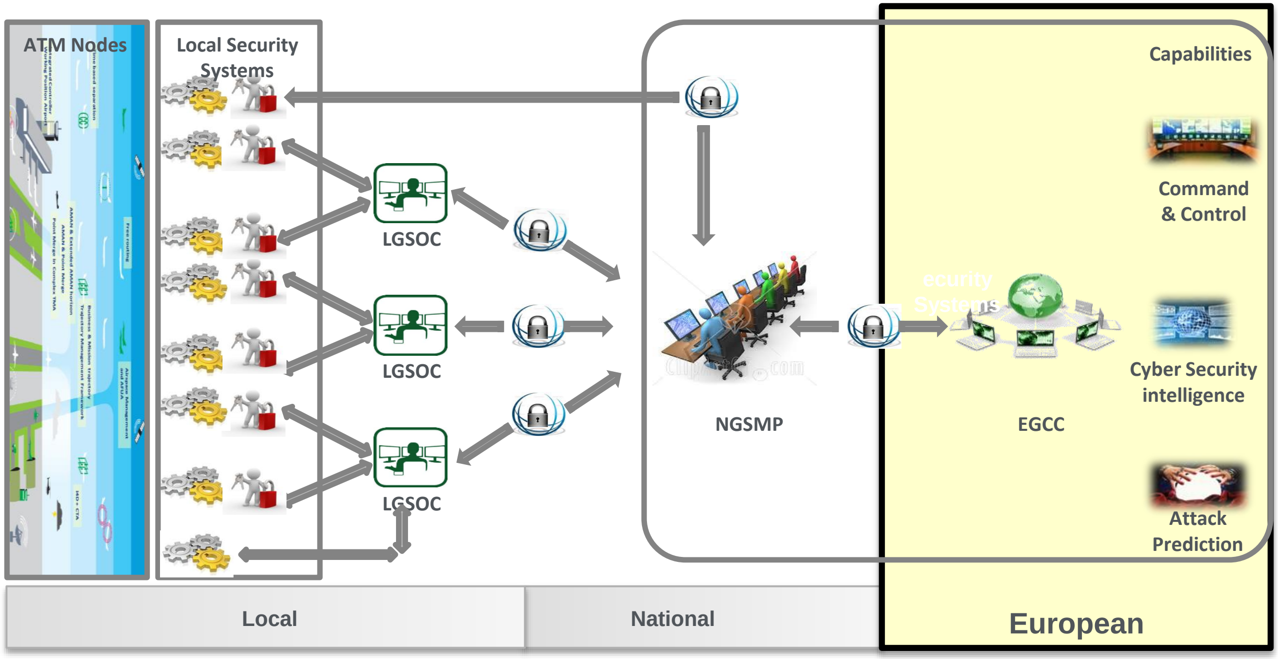
The GAMMA Solution: National level

- 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.



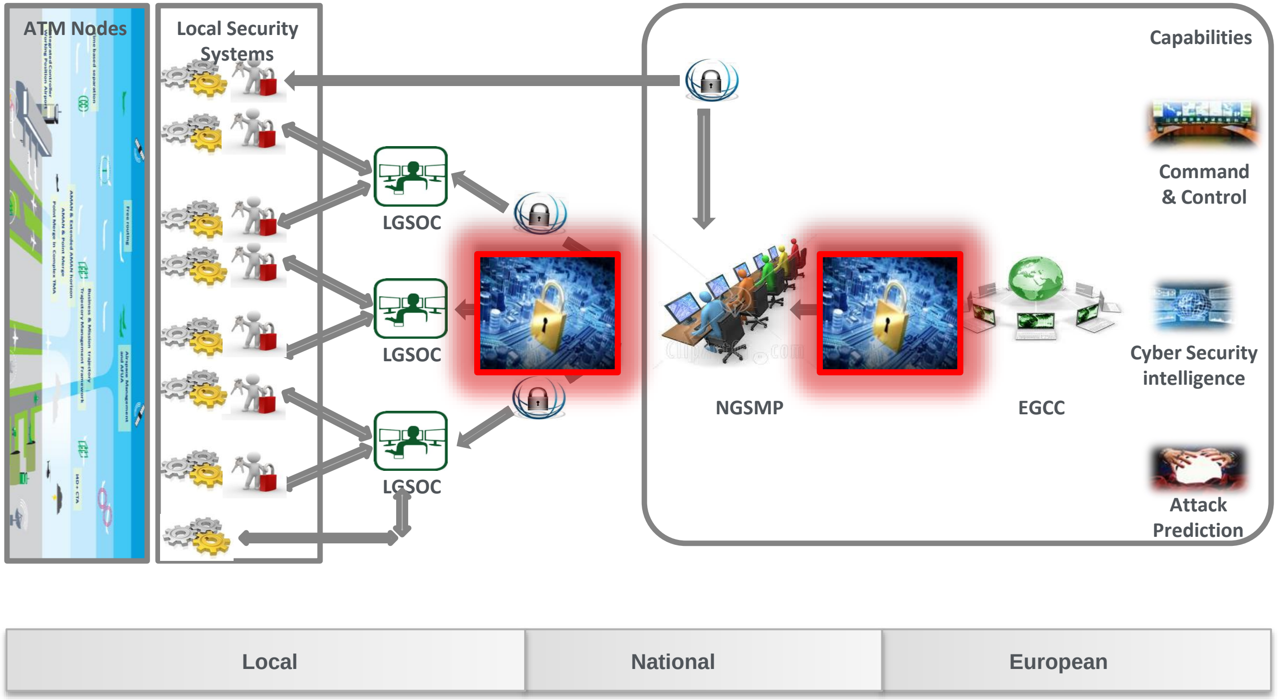
The GAMMA Solution: European level

- 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 Solution: 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.
- Sanitisation of the information aims to categorize the sensitive information, generated at local and national level that can be disseminated at European level, if necessary opportunely modified so as to eliminate sensitive aspects. In the picture below the padlock symbol represents where the sanitization process can be performed.



Conclusion

- The GAMMA solution therefore opens the way for the European level to propose (but not enforce) 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 GAMMA architectural vision therefore enlarges the scope for cooperative management of ATM security while remaining rooted in the fundamental principle that **Security cannot be outsourced or delegated.**

The GAMMA Solution can be considered a concrete and easily deployable proposal for the management of ATM security, exploiting innovative technologies and procedures while maintaining compatibility with the European ATM framework defined in the Single European Sky.

GAMMA
GLOBAL ATM SECURITY MANAGEMENT

GAMMA: first results

GAMMA 1st results

1. ATM Security Risk Assessment and Treatment

2. GAMMA Solution Architecture

3. Civil Military Cooperation Study

GAMMA

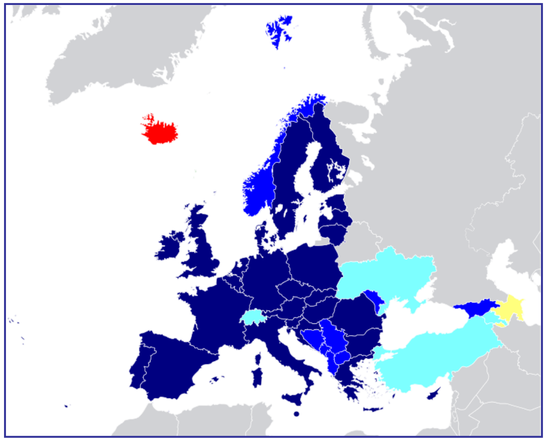
GLOBAL ATM SECURITY MANAGEMENT

GAMMA: first results

1. ATM Security Risk Assessment and Treatment

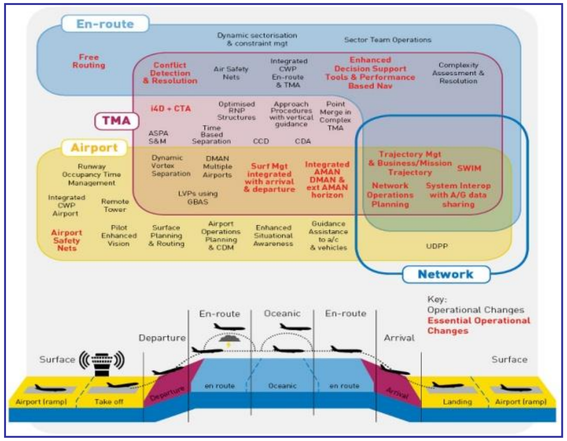
GAMMA ATM threat assessment model: SCOPE

Geographical



European Common Aviation Area

Functional


En-route
Dynamic sectorisation & constraint mgt
Sector Team Operations
Free Routing
Conflict Detection & Resolution
Air Safety Nets
Integrated CWP En-route & TMA
Enhanced Decision Support Tools & Performance Based Nav
Complexity Assessment & Resolution
TMA
i4D + CTA
Optimised RNP Structures
Approach Procedures with vertical guidance
Point Merge in Complex TMA
ASPA S&M
Time Based Separation
CCD
CDA
Airport
Runway Occupancy Time Management
Dynamic Vortex Separation
DMAN Multiple Airports
Surf Mgt integrated with arrival & departure
Integrated AMAN DMAN & ext AMAN horizon
Trajectory Mgt & Business/Mission Trajectory
SWIM
Network Operations Planning
System Interop with A/G data sharing
Integrated CWP Airport
Remote Tower
LVPs using GBAS
Airport Safety Nets
Pilot Enhanced Vision
Surface Planning & Routing
Airport Operations Planning & CDM
Enhanced Situational Awareness
Guidance Assistance to a/c & vehicles
UDPP
Network
Key:
Operational Changes
Essential Operational Changes
Surface
Departure
En-route
Oceanic
En-route
Arrival
Surface
Airport (ramp)
Take off
Departure
en route
Oceanic
en route
Arrival
Landing
Airport (ramp)

Air Traffic Management & SESAR step 1

Scenarios

Most Feared

GAMMA
GLOBAL ATM SECURITY MANAGEMENT

GAMMA
GLOBAL ATM SECURITY MANAGEMENT

Security Threats in the ATM world

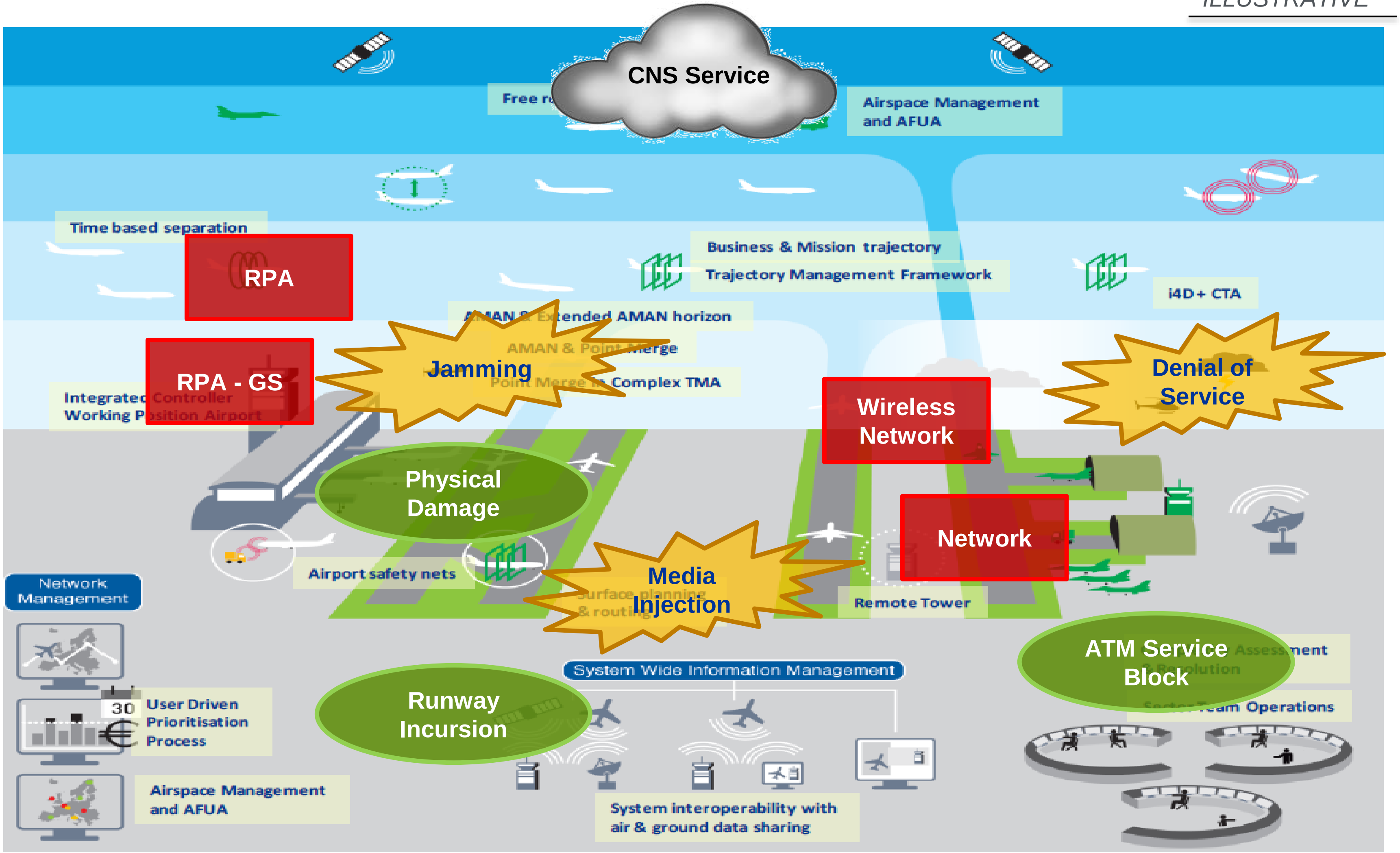
Primary asset

Supporting Assets

Threats

Impacts

ILLUSTRATIVE



CNS Service

Free ro

Airspace Management and AFUA

Time based separation

RPA

Business & Mission trajectory

Trajectory Management Framework

i4D + CTA

AMAN & Extended AMAN horizon

AMAN & Point Merge

Jamming

Point Merge in Complex TMA

RPA - GS

Integrated Controller Working Position Airport

Denial of Service

Wireless Network

Physical Damage

Network

Airport safety nets

Media Injection

Surface planning & routing

Remote Tower

Network Management

System Wide Information Management

ATM Service Block

Assessment & Resolution

Sector Team Operations

30

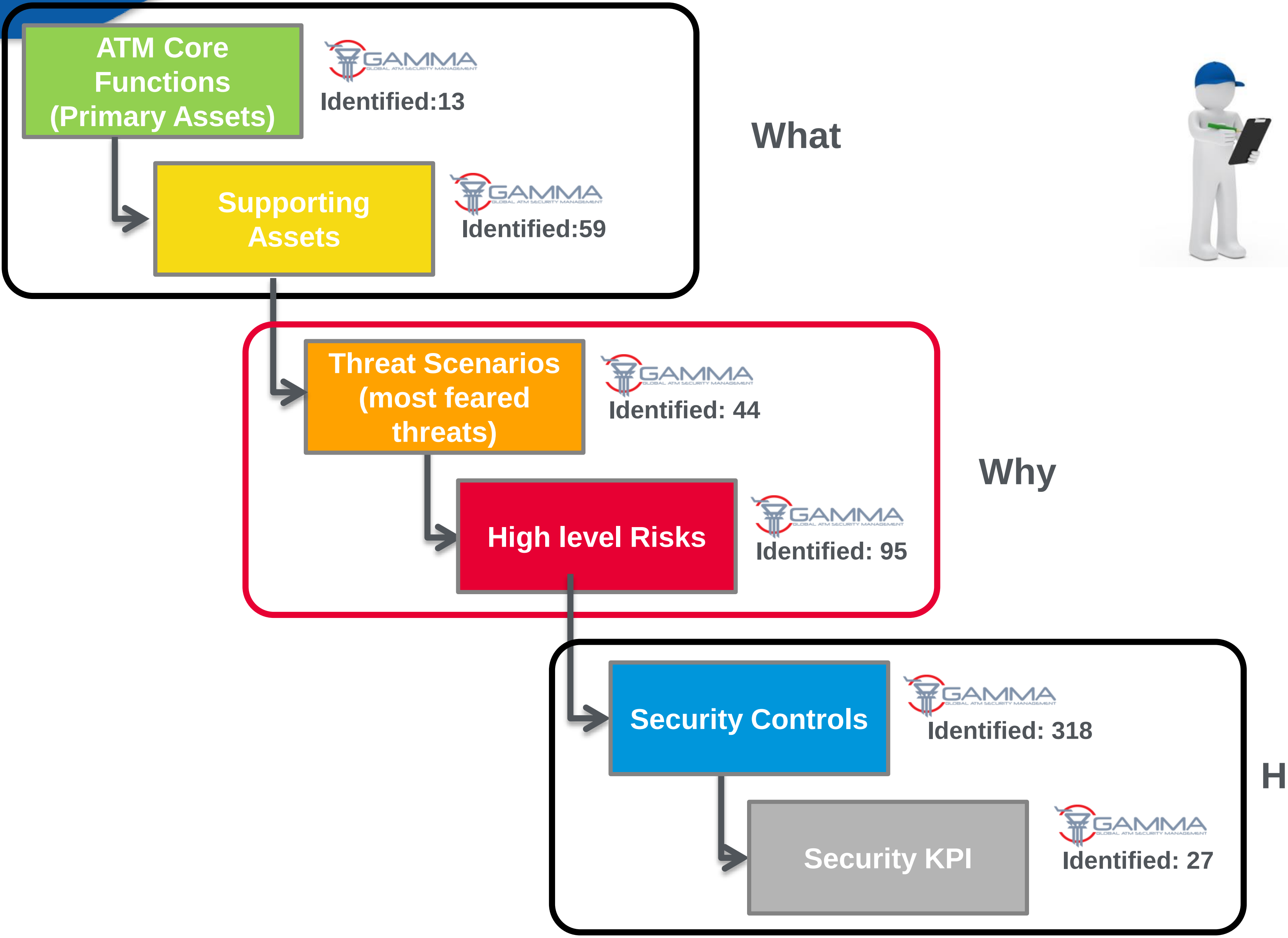
User Driven Prioritisation Process

Runway Incursion

Airspace Management and AFUA

System interoperability with air & ground data sharing

Security Risk Assessment and Treatment in GAMMA



ATM Core Functions (Primary Assets)

Identified:13

Supporting Assets

Identified:59

What

Threat Scenarios (most feared threats)

Identified: 44

High level Risks

Identified: 95

Why

Security Controls

Identified: 318

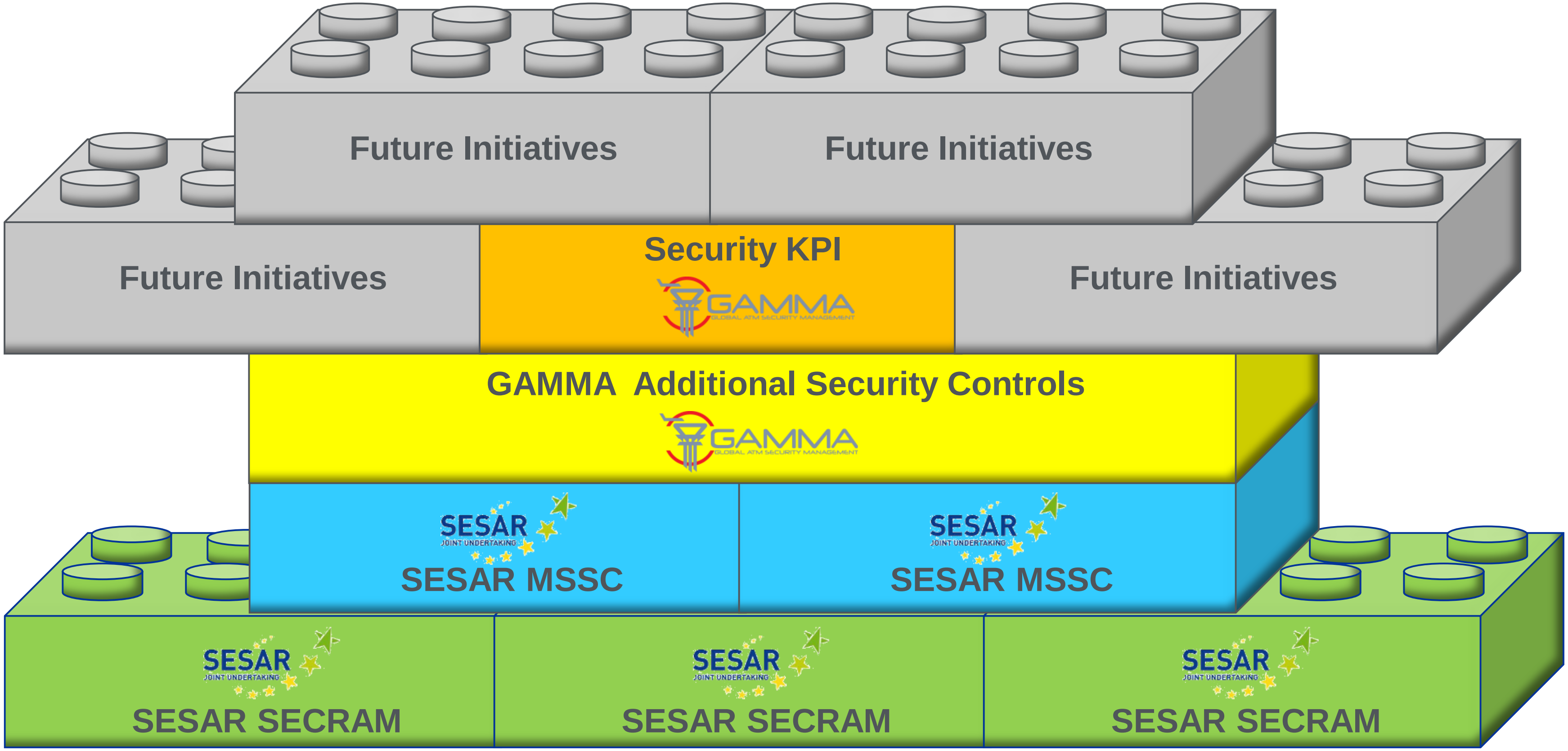
Security KPI

Identified: 27

How

Building the GAMMA Security Risk Assessment from SESAR

- Aligned with SESAR (SECRAM) methodology
- Building on SESAR Minimum Set of Security Controls (MSSC)
- Open for future extensions by SESAR 2020 and other initiatives



Future Initiatives

Future Initiatives

Future Initiatives

Security KPI

Future Initiatives

GAMMA Additional Security Controls

SESAR MSSC

SESAR MSSC

SESAR SECRAM

SESAR SECRAM

SESAR SECRAM

GAMMA

GLOBAL ATM SECURITY MANAGEMENT

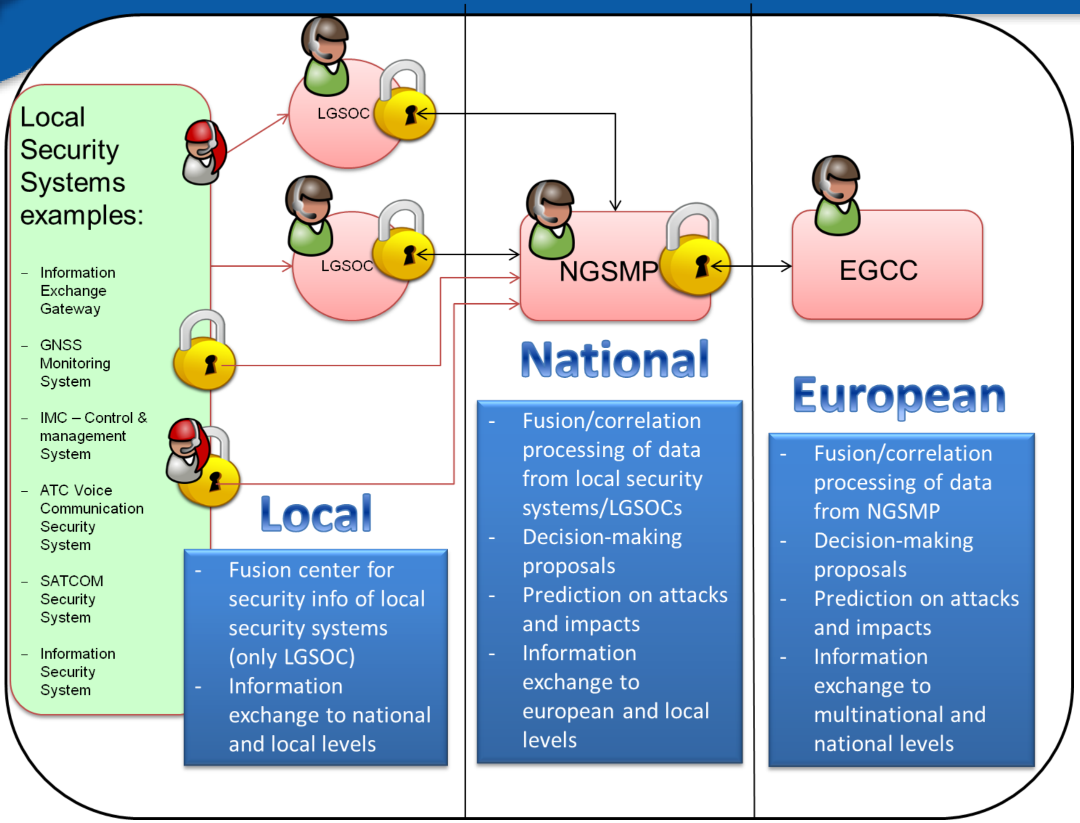
GAMMA: first results

2. GAMMA Solution Architecture

Objectives of the architecture

- Describe the **global** architecture of the ATM security solution, addressing all security controls identified in GAMMA risk treatment report
  - Link SESAR architecture assets with ATM assets to be protected by GAMMA solution.
  - Use the modelling approach consistently with the SESAR MBSE (Model-Based System Engineering) approach.
  - Produce the Operational and System Architectures using Enterprise Architecture views of the NATO Architecture Framework (NAF).
  - Provide the architecture of a global ATM security solution
    - to subsequent WPs to validate GAMMA concepts
    - to the wider ATM community for consideration in the development of the future European ATM.

Examples of operational views



Local Security Systems examples:

- Information Exchange Gateway
- GNSS Monitoring System
- IMC – Control & management System
- ATC Voice Communication Security System
- SATCOM Security System
- Information Security System

Local

- Fusion center for security info of local security systems (only LGSOC)
- Information exchange to national and local levels

National

- Fusion/correlation processing of data from local security systems/LGSOCs
- Decision-making proposals
- Prediction on attacks and impacts
- Information exchange to european and local levels

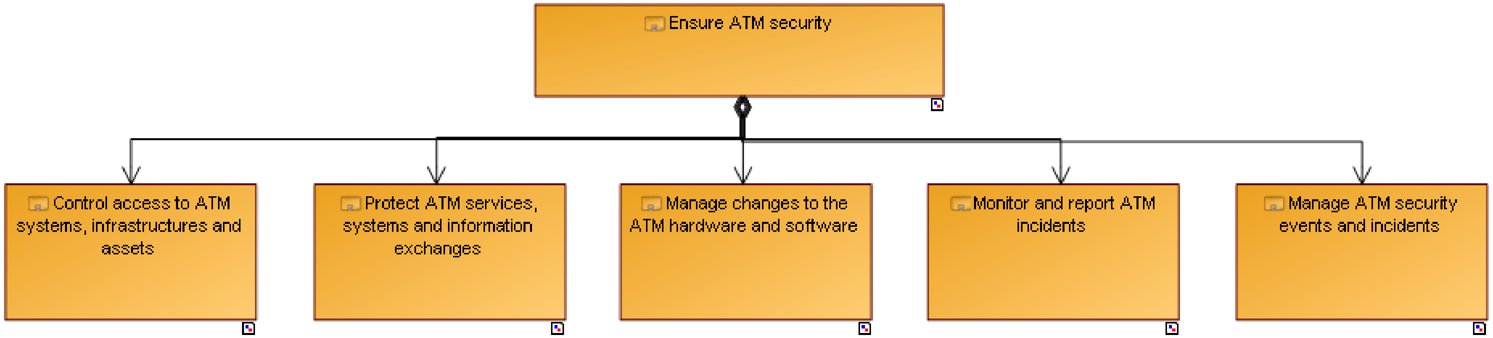
European

- Fusion/correlation processing of data from NGSMP
- Decision-making proposals
- Prediction on attacks and impacts
- Information exchange to multinational and national levels

EGCC:
European GAMMA Coordination Centre

NGSMP:
National GAMMA Security Management Platform

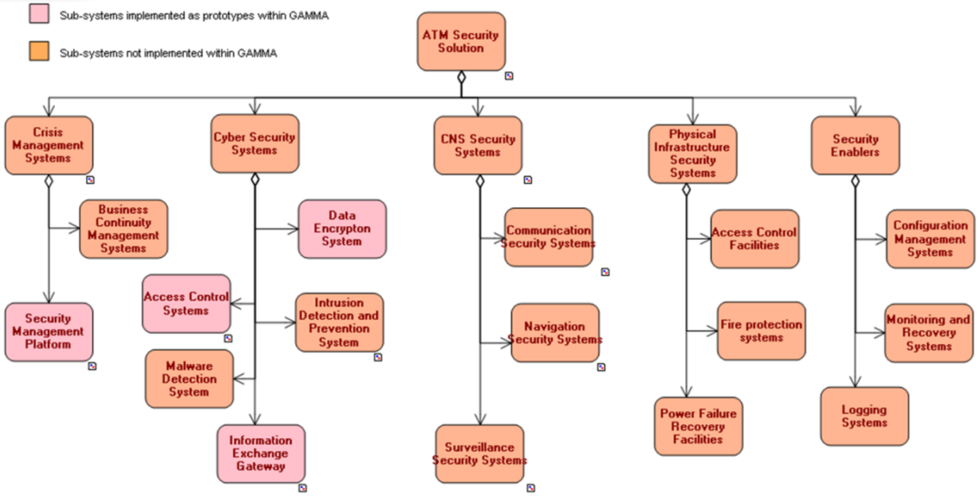
LGSOC:
Local GAMMA Security Operation Centre

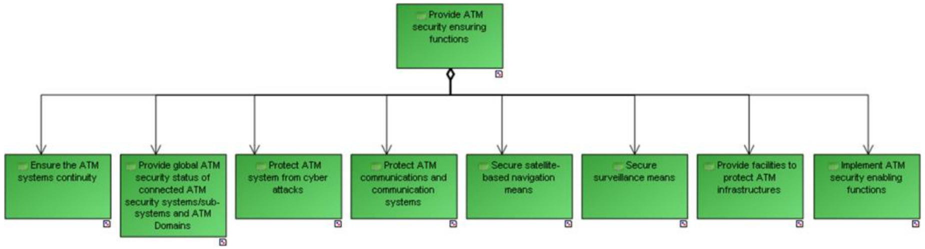

Ensure ATM security
Control access to ATM systems, infrastructures and assets
Protect ATM services, systems and information exchanges
Manage changes to the ATM hardware and software
Monitor and report ATM incidents
Manage ATM security events and incidents

These top-level generic operational processes are further decomposed into specific processes to produce the operational view of the architecture.

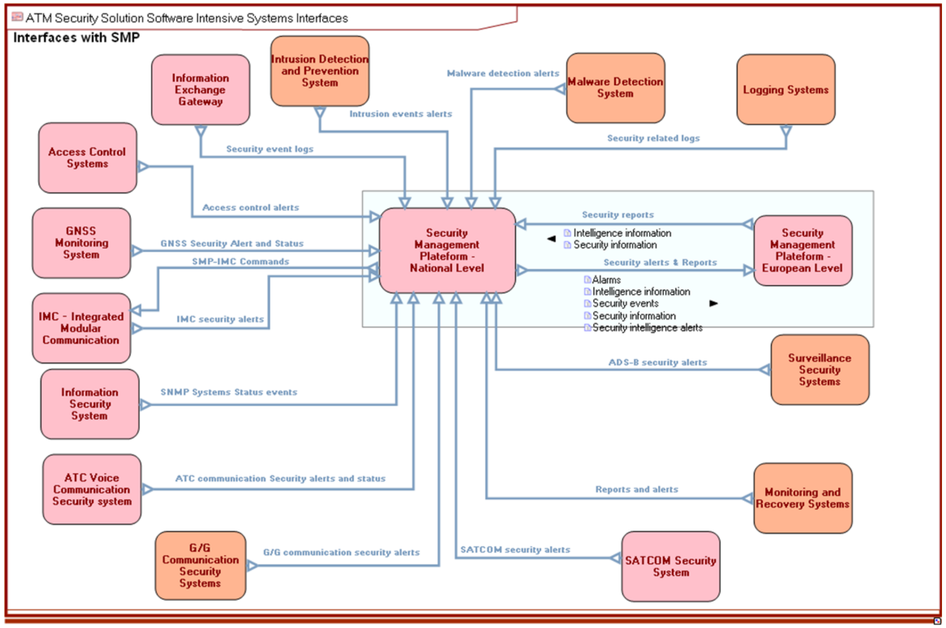
Examples of system views

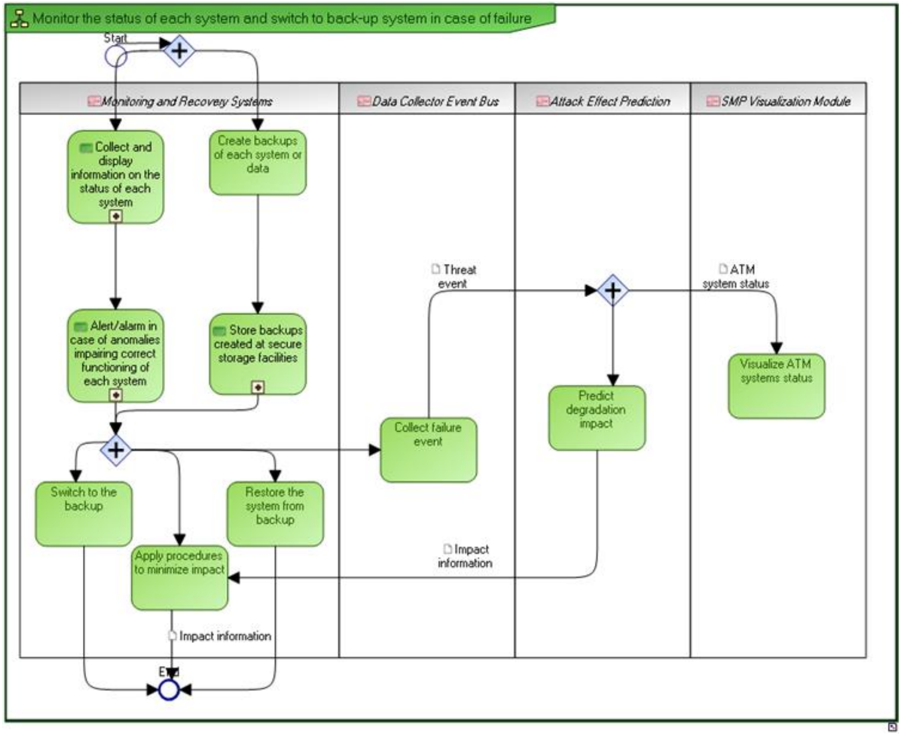
ATM Security Solution System Breakdown


Sub-systems implemented as prototypes within GAMMA
Sub-systems not implemented within GAMMA
ATM Security Solution
Crisis Management Systems
Business Continuity Management Systems
Security Management Platform
Cyber Security Systems
Data Encryption System
Access Control Systems
Intrusion Detection and Prevention System
Malware Detection System
Information Exchange Gateway
CNS Security Systems
Communication Security Systems
Navigation Security Systems
Surveillance Security Systems
Physical Infrastructure Security Systems
Access Control Facilities
Fire protection systems
Power Failure Recovery Facilities
Security Enablers
Configuration Management Systems
Monitoring and Recovery Systems
Logging Systems


Provide ATM security ensuring functions
Ensure the ATM systems continuity
Provide global ATM security status of connected ATM security systems/sub-systems and ATM Domains
Protect ATM system from cyber attacks
Protect ATM communications and communication systems
Secure satellite-based navigation means
Secure surveillance means
Provide facilities to protect ATM infrastructures
Implement ATM security enabling functions

System Behaviour


ATM Security Solution Software Intensive Systems Interfaces
Interfaces with SMP
Information Exchange Gateway
Intrusion Detection and Prevention System
Malware detection alerts
Malware Detection System
Logging Systems
Intrusion events alerts
Security event logs
Security related logs
Access Control Systems
Access control alerts
GNSS Monitoring System
GNSS Security Alert and Status
SMP-IMC Commands
IMC - Integrated Modular Communication
IMC security alerts
Security reports
Intelligence information
Security information
Security alerts & Reports
Alarms
Intelligence information
Security events
Security information
Security intelligence alerts
Security Management Plateform - National Level
Security Management Plateform - European Level
ADS-B security alerts
Surveillance Security Systems
Information Security System
SNMP Systems Status events
ATC Voice Communication Security system
ATC communication Security alerts and status
Reports and alerts
Monitoring and Recovery Systems
G/G Communication Security Systems
G/G communication security alerts
SATCOM security alerts
SATCOM Security System


Monitor the status of each system and switch to back-up system in case of failure
Start
Monitoring and Recovery Systems
Data Collector Event Bus
Attack Effect Prediction
SMP Visualization Module
Collect and display information on the status of each system
Create backups of each system or data
Threat event
ATM system status
Alert/alarm in case of anomalies impairing correct functioning of each system
Store backups created at secure storage facilities
Visualize ATM systems status
Predict degradation impact
Collect failure event
Switch to the backup
Restore the system from backup
Apply procedures to minimize impact
Impact information
Impact information
End

Conclusion & perspectives

- A solution is described to protect the systems constituting the current and future European ATM from the most feared events

- Threat scenarios identified in GAMMA Threat analysis (D2.1) are clarified by further analysing and modelling them.

- Operational processes implementing the additional security controls are defined in order to protect supporting assets of ATM systems

- Systems functions required to support the operational processes are defined

- Security systems providing these functions and their interactions are described

- Consistency reports are provided in order to ensure the consistency and completeness of the overall architecture

GAMMA

GLOBAL ATM SECURITY MANAGEMENT

GAMMA: first results

3. Civil-Military Cooperation Issues for ATM Security

Civil-military cooperation issues

- Aim of the task:
  - Establish the **as-is** situation regarding cooperation between civil and military bodies to prevent or handle ATM security events
  - Identify existing **best practices**
  - Identify list of possible **improvements**

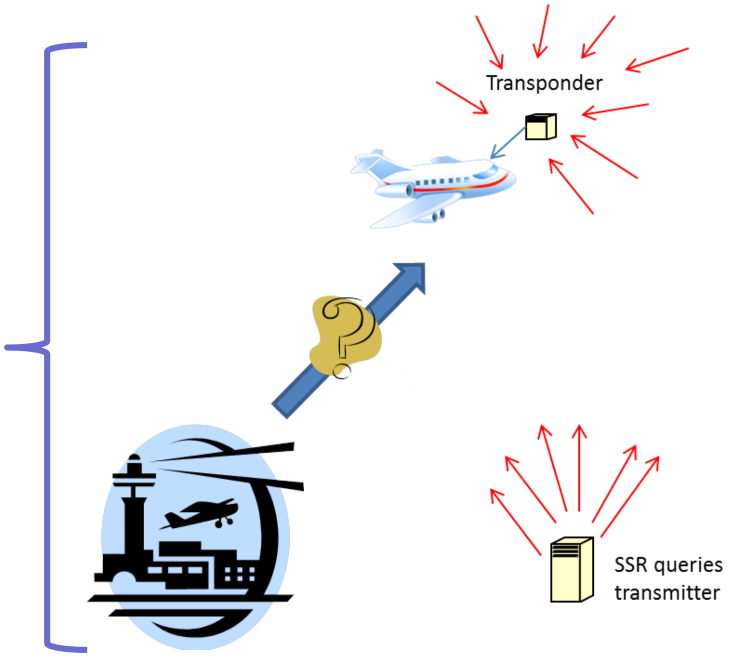
- Scope:
  - Both aspects of ATM Security are addressed:
    - **Self-Protection** of the ATM System to ensure the resilience of ATM Service provision
    - **Collaborative Support** to national authorities concerned with airspace/aviation security events

  - Threat Scenarios considered include:
    - Airborne threats (hijacking, renegade)
    - Technological threats (cyber-attacks, Jamming, Spoofing…)

Establishment of As-Is Situation

- Set up of a questionnaire to collect current practices and operational needs on a set of threat scenarios
- Sending of the questionnaire to military agencies selected by GAMMA partners and to EUROCONTROL MAB
- Consolidation through meetings with military agencies

Example of Threat Scenario:
Transponder Denial of service



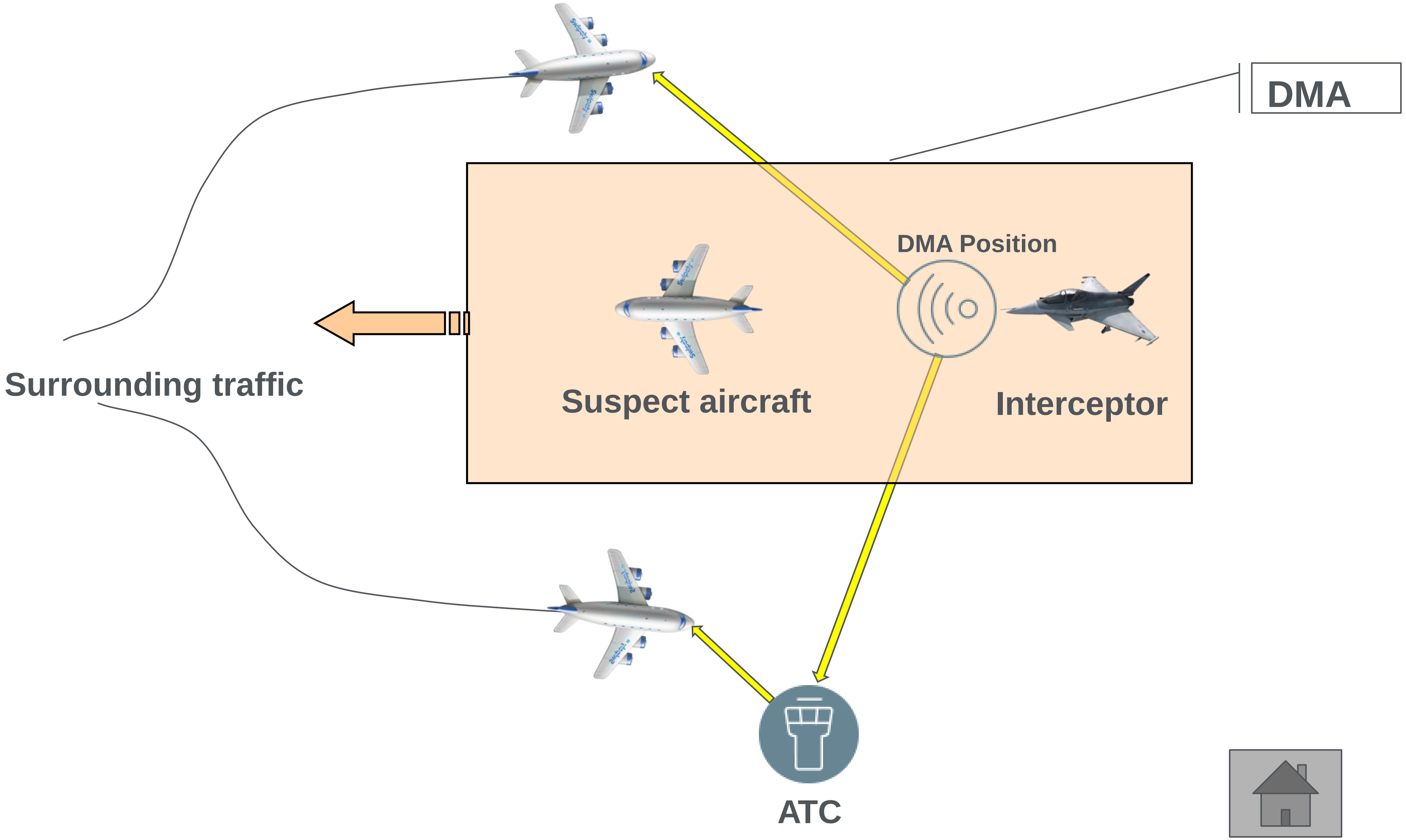
Best Practices *(examples)*

- Use a common tool to provide military with civil air situation awareness (e.g. CIMACT)
- Use secured lines of communication with the civil for incident management
- Involve the military in ANSP Contingency Plans to ensure the continuity of CNS services
- Set up regular live exercises, including cross-border incidents
- Deploy automatic systems to detect fake surveillance data

Proposed Improvements *(examples)*

- Harmonise ASSIM (Airspace Security Incident Management) implementation
- Transmit (declassified) primary tracks to civil ATC
- Improve RPAS Detection (e.g. using acoustic Doppler)
- Automatically detect pre-defined sets of aircraft behaviours triggering reports to Air Defence
- Set up joint Civil/Military training exercises for all types of threats, using distributed simulation platforms
- Use Dynamic Mobile Areas for ATM Security (see next slide)

Dynamic Mobile Area (DMA) moving with an interceptor



DMA

DMA Position

Surrounding traffic

Suspect aircraft

Interceptor

ATC

End of presentation

More information available at:
www.gamma-project.eu