Security Risk Assessment and Risk Treatment for Integrated Modular Communication

Hamid Asgari, Sarah Haines, Adrian Waller

Thales UK, Research & Technology

Hamid.Asgari@uk.thalesgroup.com

2nd Sept. 2016

ARES Conference, SecTM Workshop, Seccion II

Outline

- GAMMA Project
- ATM Context and IMC
- Risk Assessment Methodology
- Risk Treatment
- Modelling Attacks and Solution Architecture
- IMC Prototype for Validation
- Concluding Remarks

GAMMA

GLOBAL ATM SECURITY MANAGEMENT

GAMMA Project

Key Information

- EC FP7-Sec-Call 5 , Partialy Funded
- Duration: 2013-2017
- 19 Partners from 8 Countries

- 10 Large Industries

Selex ES A Finmeccanica Company · AIRBUS · CASSIDIAN AN EADS COMPANY
BOEING · ThalesAlenia Space A Thales / Finmeccanica Company · THALES
Isdefe · THALES · EADS

- 3 SME

4Solutions The ultimate answer · CiaoTech · RNC AVIONICS

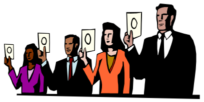
- 3 Research Organisations and Universities

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

- 3 End-Users

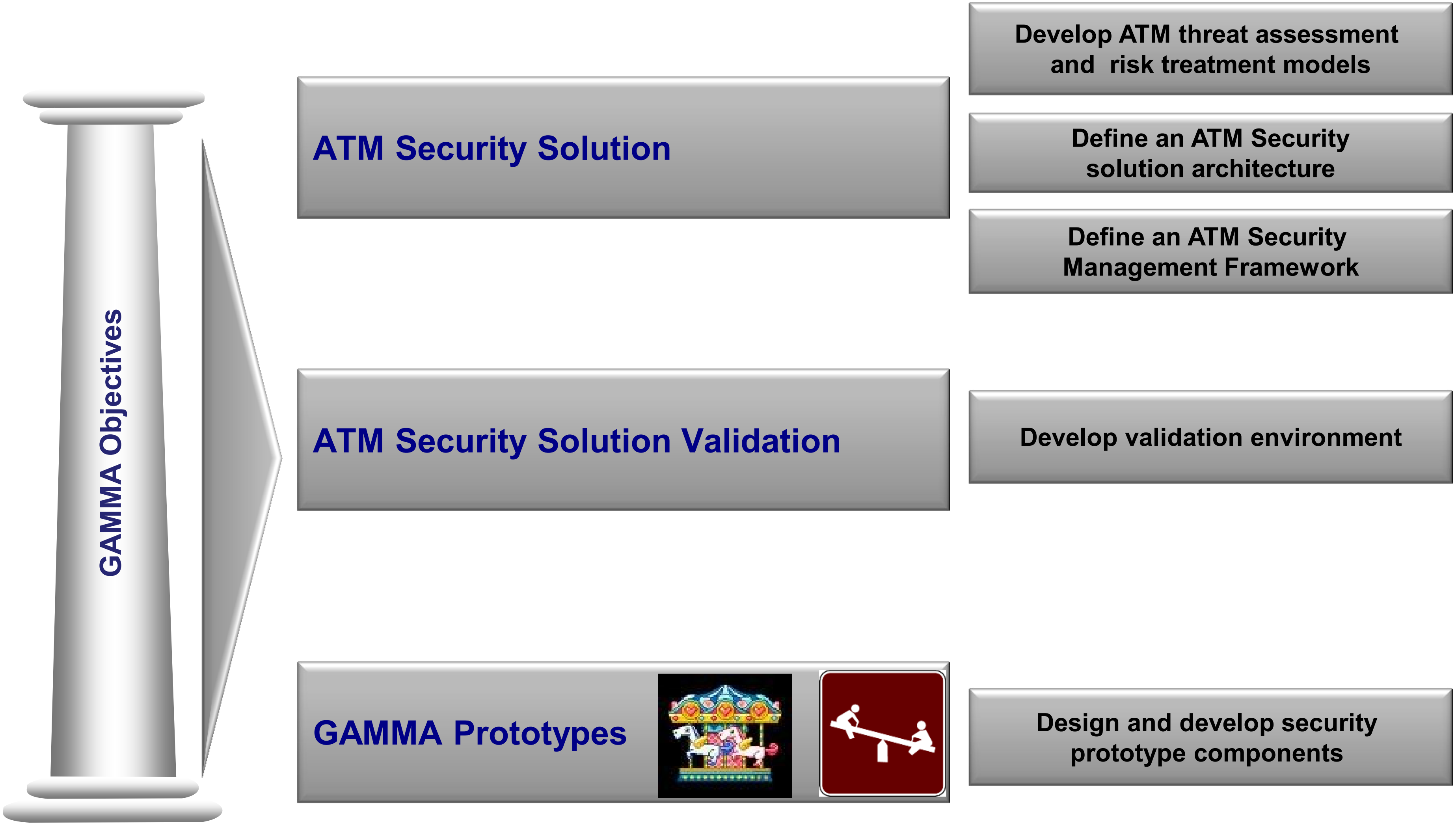
romatsa · ENAV · SEA

- User Group



THALES

GAMMA: Objectives



GAMMA Objectives

ATM Security Solution

- Develop ATM threat assessment and risk treatment models
- Define an ATM Security solution architecture
- Define an ATM Security Management Framework

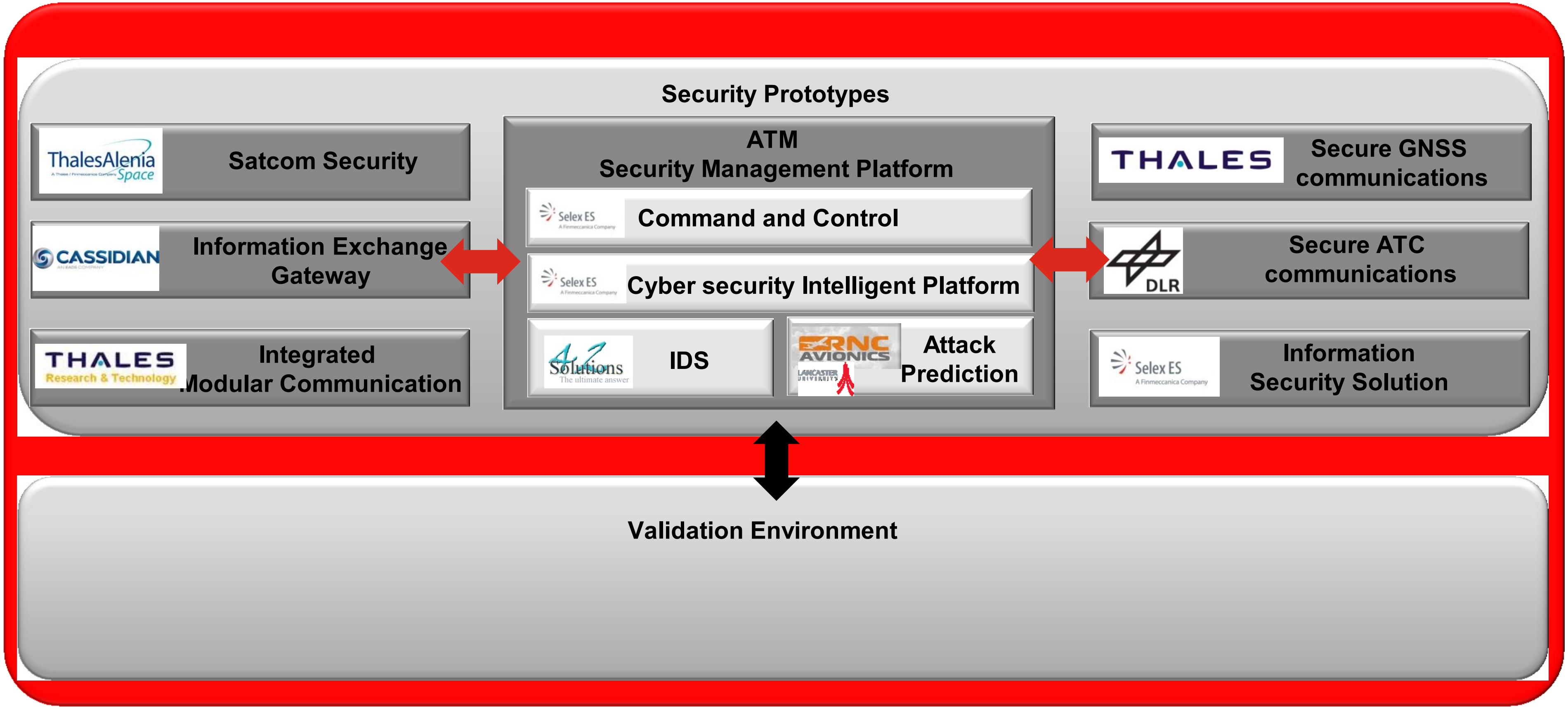
ATM Security Solution Validation

- Develop validation environment

GAMMA Prototypes

- Design and develop security prototype components

GAMMA Security Prototypes



Security Prototypes

Satcom Security

Information Exchange Gateway

Integrated Modular Communication

ATM Security Management Platform

Command and Control

Cyber security Intelligent Platform

IDS

Attack Prediction

Secure GNSS communications

Secure ATC communications

Information Security Solution

Validation Environment

SESAR and GAMMA Link

- GAMMA make use of the methodologies developed by SESAR in WP16
  - SECRAM (Security Risk Assessment Methodology)
  - MSSC (Minimum Set of Security Controls)
    - *An initial set of security controls to ensure a baseline for security measures across the SESAR solutions; Reduce risk level "medium" to "low"*
  - GAMMA additional Security Controls
    - *Counteract specific threats with risk level of "high".*

- GAMMA used the same modelling tool (MEGA) as SESAR, allowing for GAMMA outputs to be reused in SESAR.

- GAMMA Operational and System security Architectures are described using the Enterprise Architecture views of the NATO Architecture Framework (NAF).

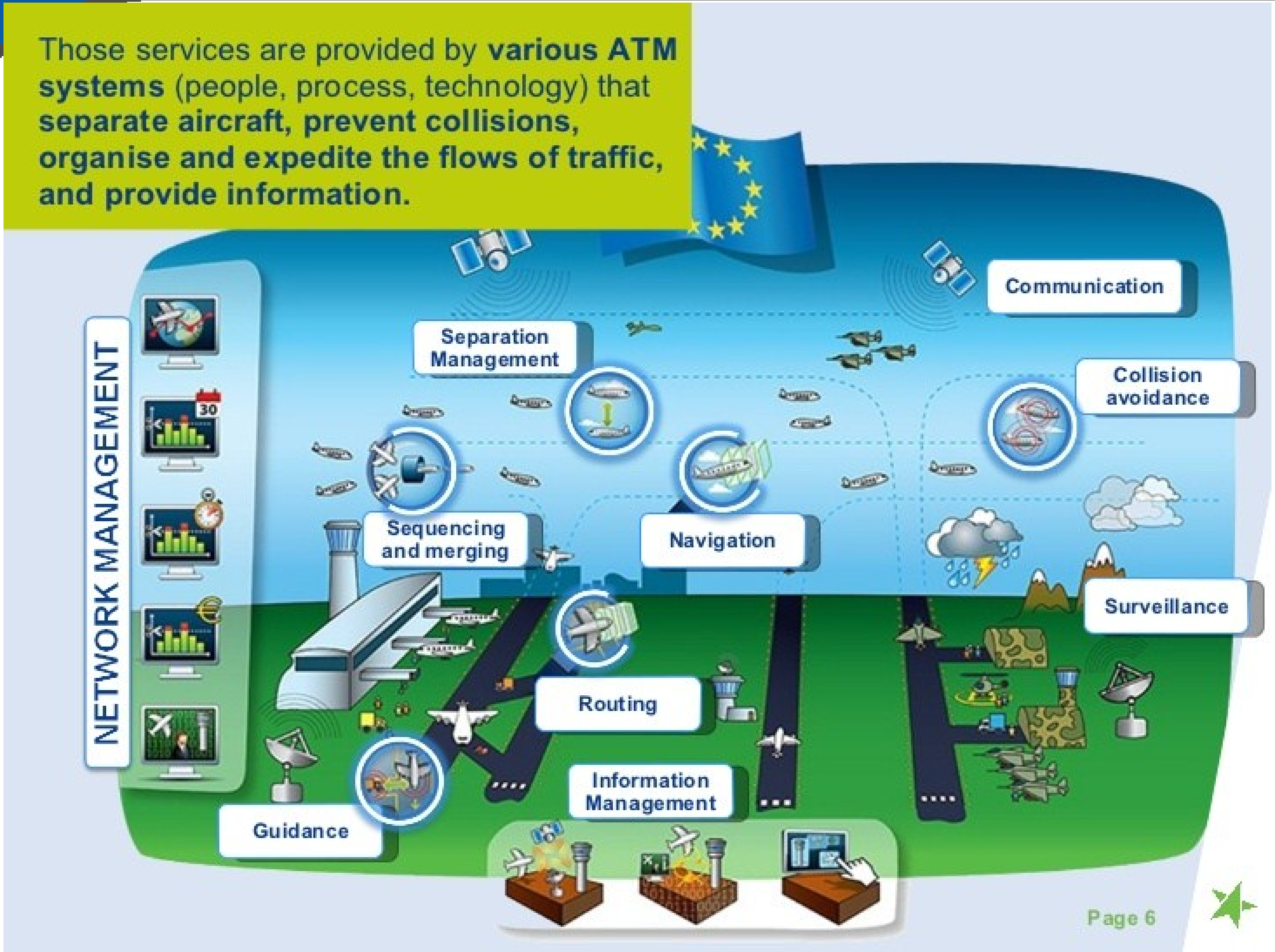
MEGA for NAF is repository-based tool for describing and documenting NAF architectural views, ensuring coherence within and between different views.

GAMMA

GLOBAL ATM SECURITY MANAGEMENT

ATM Context and Integrated Modular Communication

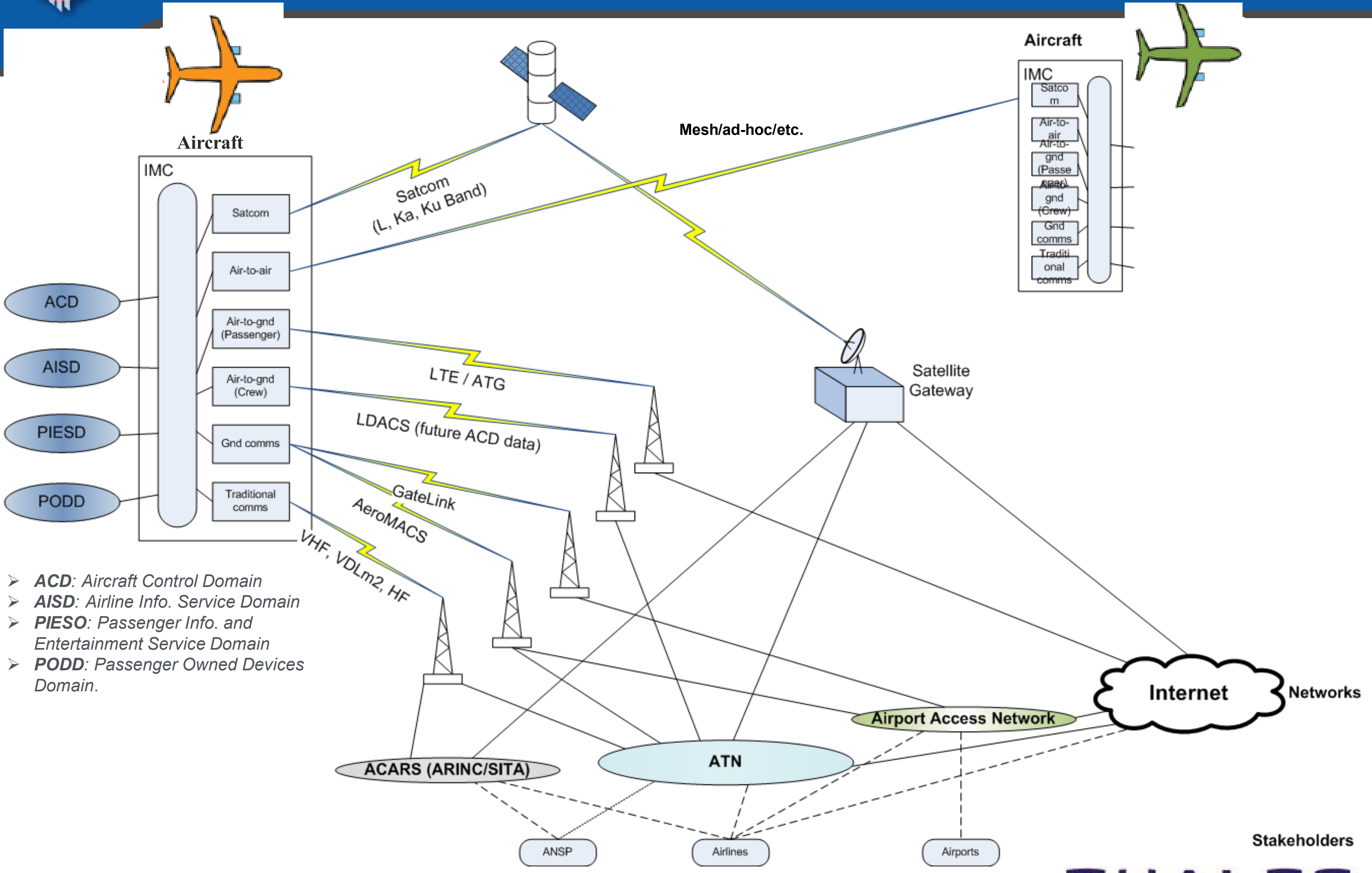
Context - Air Traffic Management (ATM)



Those services are provided by **various ATM systems** (people, process, technology) that **separate aircraft, prevent collisions, organise and expedite the flows of traffic, and provide information.**

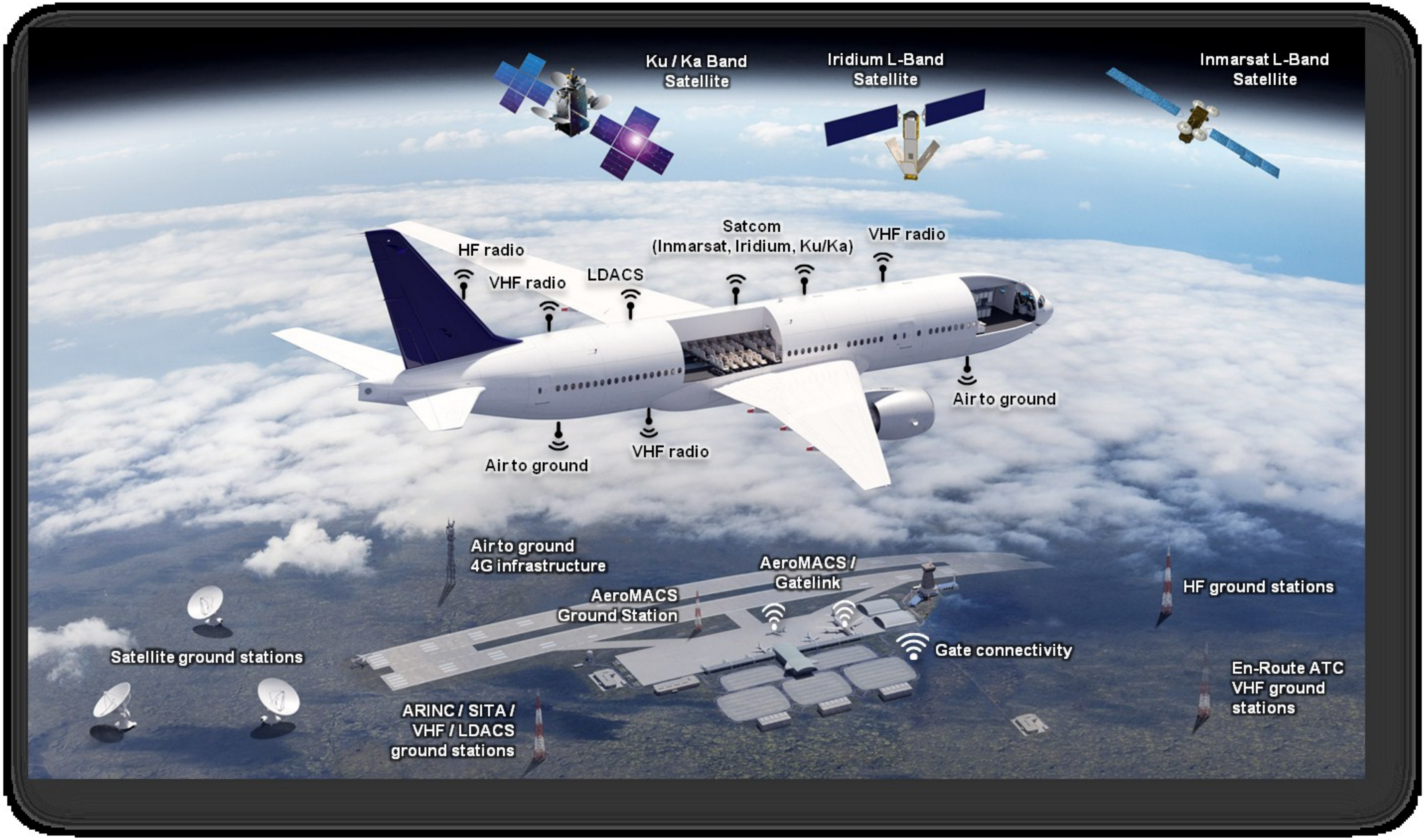
From SESAR general presentation

Context - The Networking



- ***ACD**: Aircraft Control Domain*
- ***AISD**: Airline Info. Service Domain*
- ***PIESO**: Passenger Info. and Entertainment Service Domain*
- ***PODD**: Passenger Owned Devices Domain.*

Context - Communication Means to/from a Commercial Aircraft

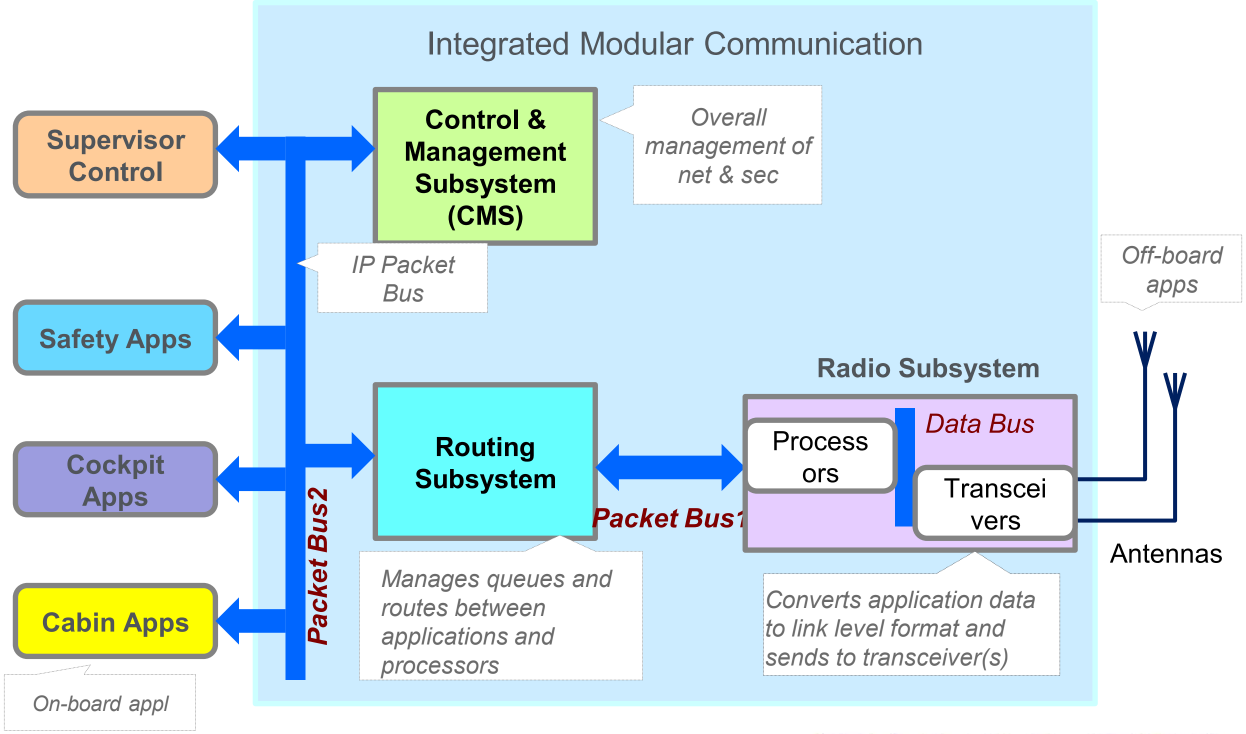


Context – High Level IMC View

- Currently, commercial airliners comprise a *federated* com architecture of diverse radios, routers, switches and associated control equipment – with a separate radio for each service.
- **IMC is a cost effective approach to provide aircraft Communications, Navigation and Surveillance systems by integrating many individual radio systems into a processing platform, offering off-board communication and on-board network connectivity.**

ARINC-664 defined 4 different traffic domains:

- ***ACD****: Aircraft Control Domain -* Supporting the safe operation of aircraft and providing env. functions for cabin operations.
- ***AISD****: Airline Info. Service Domain -* Airplane (maintenance, perf. data, etc.) Airline operational and Admin Support.
- ***PIESO****: Passenger Info. and Entertainment Service Domain*
- ***PODD****: Passenger Owned Devices Domain*.


Integrated Modular Communication
Supervisor Control
Control & Management Subsystem (CMS)
Overall management of net & sec
IP Packet Bus
Off-board apps
Safety Apps
Radio Subsystem
Cockpit Apps
Routing Subsystem
Process ors
Data Bus
Transcei vers
Packet Bus2
Packet Bus1
Antennas
Cabin Apps
Manages queues and routes between applications and processors
Converts application data to link level format and sends to transceiver(s)
On-board appl

IMC Security Requirements

- **Robustness & System Integrity**
  - *To offer the communication services as expected as well as achieving integrity of system and its components*
- **Availability**
  - *To ensure accessibility of services and information*
- **Data Confidentiality**
  - *To provide confidentiality for stored and communicated data*
- **Data Integrity**
  - *To guarantee no improper modification of data*
- **Access Control**
  - *To regulate and control data access and data flow*
- **Compliance to Regulatory Framework**
  - *To guarantee compliance to the relevant regulations*.

IMC Security Threats (1)

- **Jamming of the channel**
  - *To hamper or obstruct all communications in a spectrum band; disrupt the management channels used for distributing C&M messages.*
- **Unauthorised Access through RF Interfaces**
  - *Unauthorised access through the RF interfaces (such as the VHF links) to the aircraft.*
- **Access to Disrupt Services**
  - *Unauthorised access between different segments on the aircraft. For example, access to cockpit services through cabin services.*
- **Insertion of Malicious Software**
  - *Malware, software bugs,* or deliberate covert channels for unauthorised access.
- **Alteration of Messages**
  - *To disrupt the IMC operation by altering messages exchanged across the ground-to-air network, the internal IMC network, and the cabin network.*

IMC Security Threats (2)

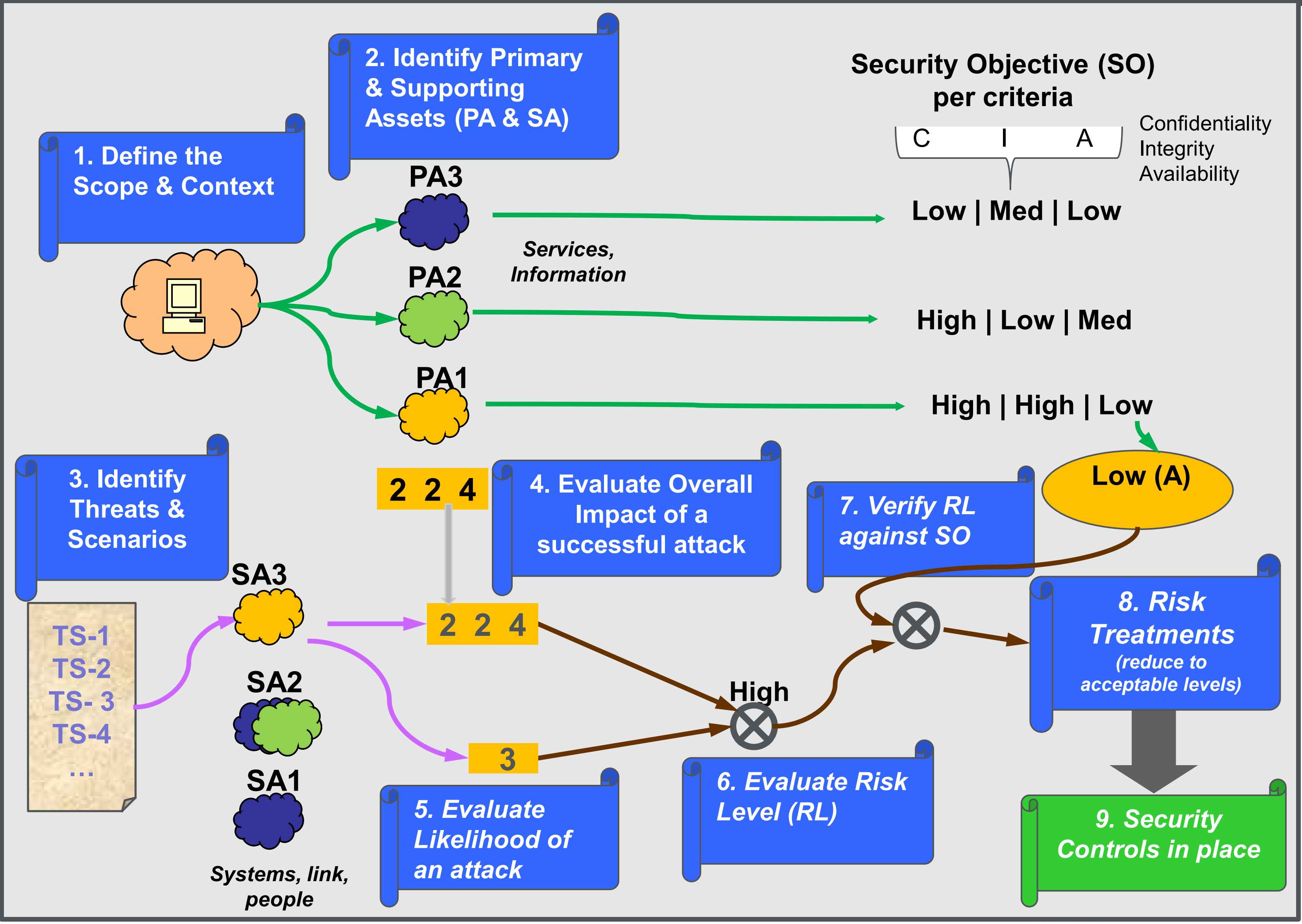
- **Alteration, Destruction or Extraction of Configuration Data**
  - *To prevent IMC performing its normal functions; with the extraction, attacker collects configuration data that can be used in subsequent attacks.*
- **Alteration or Destruction of User Data**
  - *Improper manipulation of user data*
- **Alteration or Destruction of Software**
  - *To create malfunctioning of middleware, generic SW/HW, OS, and the waveform code that is needed to support a radio access technology or air interface.*
- **Excessive Resource Consumption**
  - *To cause unavailability of services/information due to e.g. DoS attacks*
- **Software/Hardware Failures**
  - *Malfunctioning of middleware, generic SW/HW, etc. More emphasis should be put on critical components.*

GAMMA

GLOBAL ATM SECURITY MANAGEMENT

RISK Assessment

Risk Assessment Methodology - SecRAM



1. Define the Scope & Context

2. Identify Primary & Supporting Assets (PA & SA)

Security Objective (SO) per criteria

C I A

Confidentiality
Integrity
Availability

PA3 — Low | Med | Low

PA2 — High | Low | Med

PA1 — High | High | Low

Services, Information

Low (A)

3. Identify Threats & Scenarios

TS-1
TS-2
TS- 3
TS-4
…

SA3

SA2

SA1

Systems, link, people

2 2 4

4. Evaluate Overall Impact of a successful attack

2 2 4

3

5. Evaluate Likelihood of an attack

High

6. Evaluate Risk Level (RL)

7. Verify RL against SO

8. Risk Treatments (reduce to acceptable levels)

9. Security Controls in place

Primary Assets

Primary Asset	Type	Description
Air Traffic Communication Service	Service	The service that allows the transfer of essential data between ATM systems and an IMC for safety-related purposes, requiring high integrity and rapid response; flight control information, alerting, collision avoidance, etc. The service is used by **Safety Critical** applications.
Aeronautical Control & Operational communications	Service	The data service for use by aircraft operators requiring high integrity for handling the operation and efficiency of flights, and support of passengers; The service is used by **Cockpit** applications.
Computing resources	Service	This refers to the IMC system’s internal resources, configurations, and operations, e.g. processes, functions, and data-bases.
Control and Management data	Information	Any data that is exchanged concerning the operation and management of the IMC system or its connected networks; Exchanged with the Supervisor Control processes and the external GAMMA Security Management Platform.
Airline data	Information	Any data that is exchanged to or from airliner’s domain i.e., the operational and airline administrative information to both **Cockpit and Cabin** applications.
User data	Information	Any data that is transferred to or from a **Cabin** application process. This is done by a passenger device, accessing the aircraft network (e.g., WiFi or telecom services).

Supporting Assets

Supporting Asset	Description	Primary Asset
IMC system	IMC as a complete system in the ATM environment	Com. Service, Computing resources, Airline data, User data, C&M data
IMC's Routing Sub-system	Routes data traffic from on-board applications/processes to radio sub-system and vice versa.	Computing resources, Airline data, User data, C&M data
IMC's Radio Sub-system	Converting data into a link level format, passing data to one or more transceivers	Computing resources, Airline data, User data, C&M data
IMC's CMS	The entity performing the overall management of IMC functions and security	C&M data
IMC's Internal BUS	IMC internal packet bus as the data link between RoS, RaS, and CMS	Airline data, User data, C&M data
Satellite link	Satellite link to provide worldwide reliable communication channels	Com. Service, Airline data, User data, C&M data
HF/UHF/VHF links	Different radio Data links	Com. Service, Airline data, User data, C&M data,
Wireless access inks	Broadband wireless access systems for on-the-ground communication.	Airline data, User data, C&M data
Cellular link	Provides cellular connectivity such as 3G	User data

Category of Identified Risk Sources/Threats

IMC Threat	Description
T-IMC1	**On-board application attack**: An application on board the aircraft uses its data connection to the IMC to attack an ATM primary asset (e.g. flight/airline information managed by another application).
T-IMC2	**Off-board application attack**: An off-board application uses its data connection to the IMC to attack an ATM primary asset. This could be a ground segment application, or something external to the ATM system (e.g., Internet traffic destined for the cabin).
T-IMC3	**Subverted software or hardware**: Corrupted software or hardware in the IMC attacks an ATM primary asset (e.g., denying communication to ATC).
T-IMC4	**Abuse of management interface**: An administrator of the IMC (e.g. someone setting configuration parameters) abuses his/her privileges, or someone impersonates the administrator, and uses this to attack an ATM primary asset.
T-IMC5	**Jamming of data links**: A jamming device is used in proximity to ATM channels to perform this attack. These devices prevent IMC from communicating application data.

1. ADS-B: Automated Dependant Surveillance-Broadcast

Risk assessment example

Supporting Asset	Related to Primary Asset	Impact on PA #x		
		C	I	A
IMC CMS	Com. Service		5	5

Threat	Impacted Criteria			Impact	Likelihood	Risk level
	C	I	A			
IMC-3		X	X	5	3	High

Risk treatment example

Threat	Impacted Criteria			Impact	Likelihood	Risk level	Security Objectives
	C	I	A				
IMC-3		X	X	5	3	High	Low

Supporting Asset	Threat	Impact	Likelihood	Risk	S.O.	CIA	Option	MSSC id	Description	Strategy	Security Controls
IMC	IMC-3	5	3	High	Low	I+A	Reduce	MSSC_32	Configuration Information shall be appropriately protected.	Combined SC-Defense in depth	MSSC_32_IMC_03

Accept, Reduce, Avoid, Transfer

SC implements actions: Deter, Avoid, Prevent, Detect, React.

Security Controls	Description
MSSC_32_IMC_03	Integrity of IMC information shall be appropriately protected.

SESAR defined 56 MSSCs.
GAMMA defined a large set of SCs based on the MSSCs.

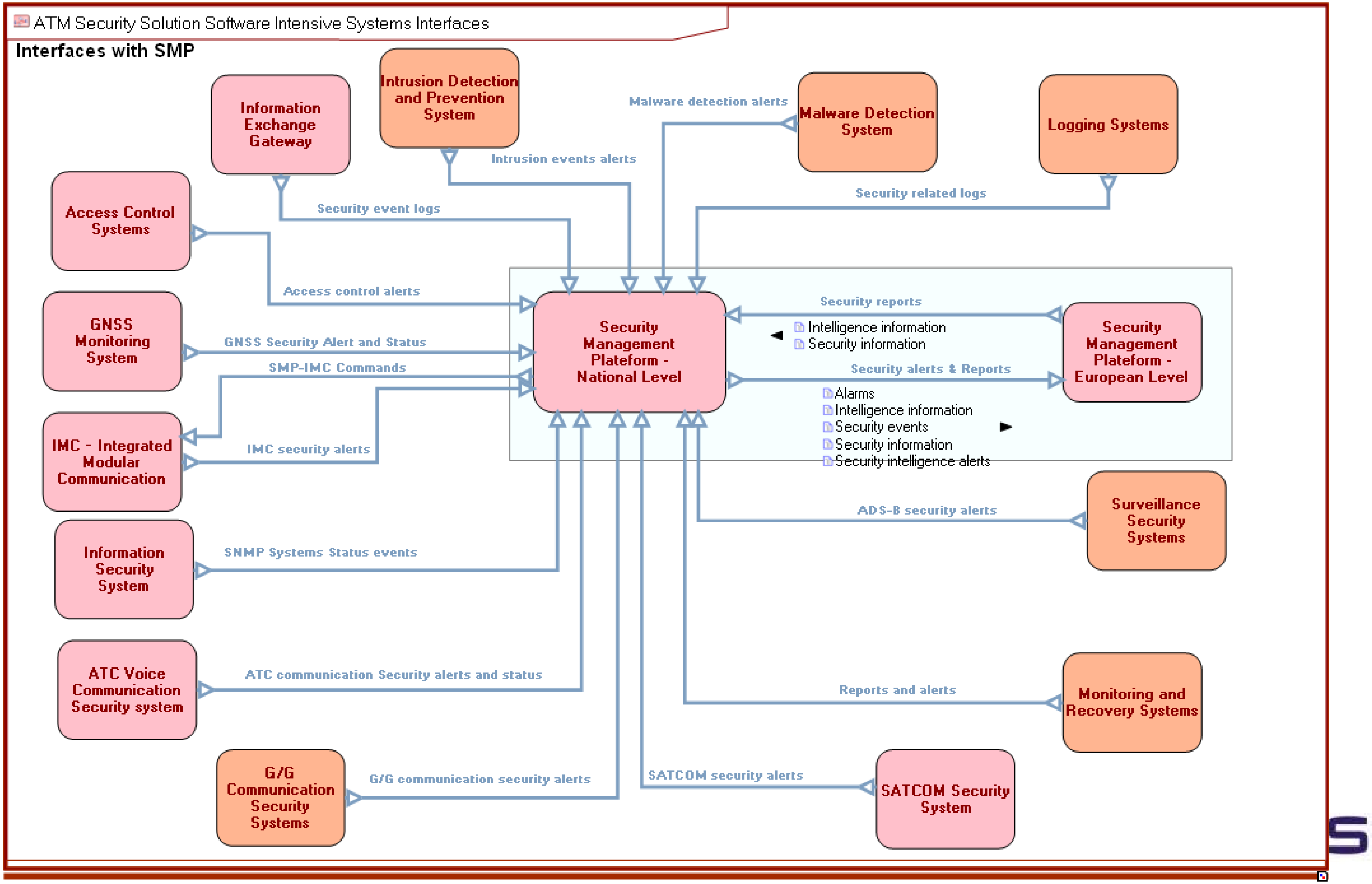
GAMMA

GLOBAL ATM SECURITY MANAGEMENT

Modelling the Attacks & Solution Architecture

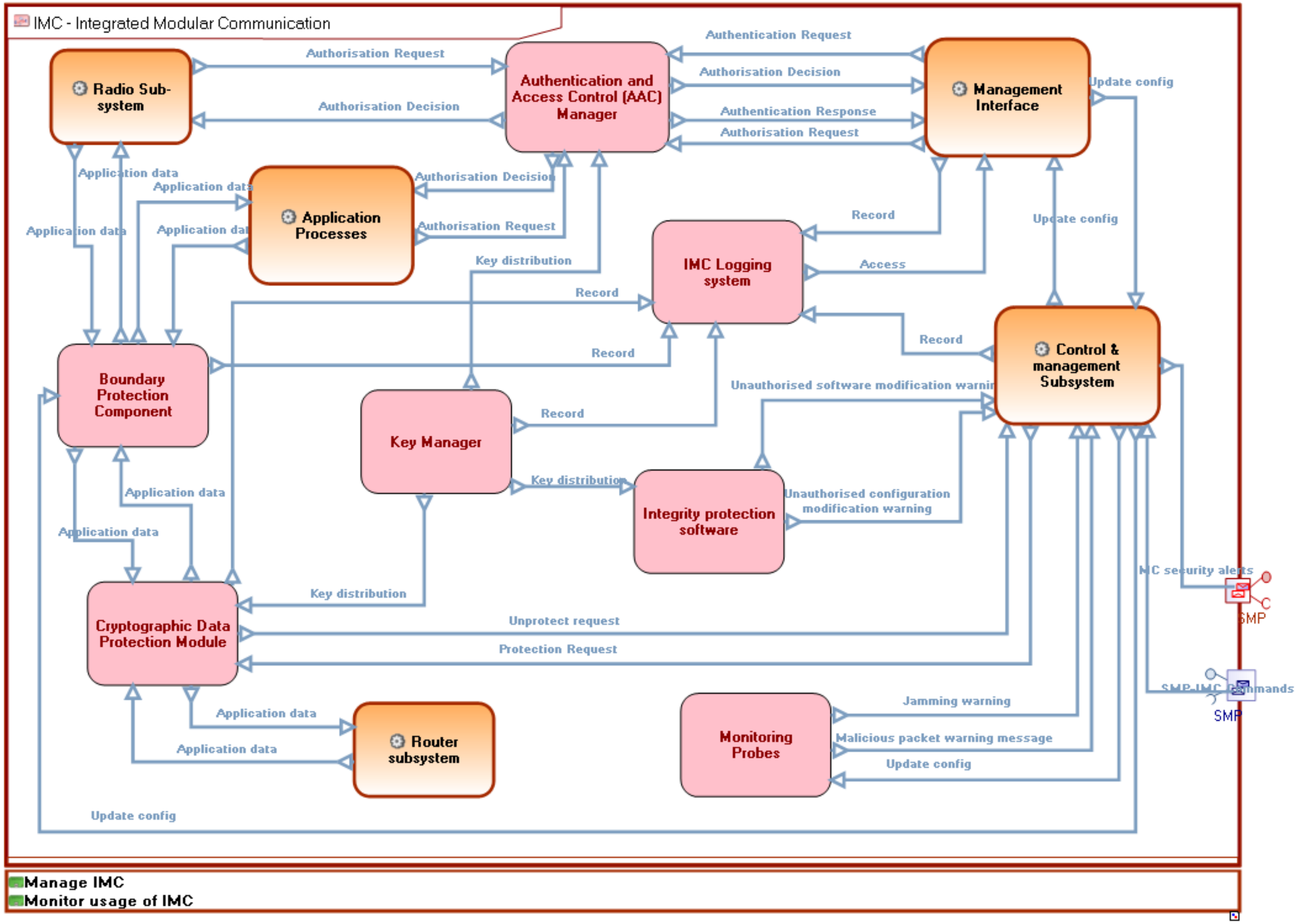
System View - Systems Internal Interfaces – NSV1

System's view includes system functions, focuses on WHAT the system must do to produce the required operational behaviour, inter-function relationships, and the required inputs, outputs, states, and rules.


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
Access Control Systems
Security event logs
Security related logs
Access control alerts
GNSS Monitoring System
Security reports
Intelligence information
Security information
Security Management Plateform - National Level
Security Management Plateform - European Level
GNSS Security Alert and Status
SMP-IMC Commands
Security alerts & Reports
Alarms
Intelligence information
Security events
Security information
Security intelligence alerts
IMC - Integrated Modular Communication
IMC security alerts
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

Security System Architecture of IMC – NSV1

- Authenticating users of the IMC.
- Controlling access to the resources via access control mechanisms.
- Using cryptographic protection to protect the confidentiality and integrity of assets.
- Monitor, control and program the relevant processes in the IMC.



THALES

Concluding Remarks

Conclusions

- There is a much growing need to interconnect devices, sensors, and the users that consume data/content.
- ATM systems themselves are growing and becoming more complex.
- We no longer face with isolated systems but increasingly interconnected, shared and dynamic.
- We have not been great at dealing with security in the networks, the ATM systems bring criticality, more complexity and dynamics.
- Our technical solutions must incorporate security functions as integral part of the system.
- ATM systems must be programmable/flexible to be secure and resilient against persistent and new/sophisticated attacks, to allow *running different functions at different times.*

THALES

Thanks for your attention

Hamid Asgari

Email: Hamid.Asgari@uk.thalesgroup.com

SecATM - 2nd Sept. 2016