Addressing Security in the ATM Environment

From identification to validation of security counter-measures with introduction of new Security Capabilities in the ATM System context.

Addressing Security in the ATM Environment

ARES 2016 – SecATM Workshop

Salzburg, 2. September 2016

Contributors

- Patrizia Montefusco, Leonardo
- Rosa Ana Casar Rodriguez, Isdefe
- Tim Stelkens-Kobsch, DLR
- Rainer Koelle, Lancaster University

Summary

- ✓ Introduction
- ✓ Security Function
- ✓ Security Risk Assessment and Treatment
- ✓ Security Requirement and Solution
- ✓ Validation
- ✓ Next Steps

The Overlooked Security Function

SESAR Definition Phase

- Budget cuts → redefinition of security working packages

SESAR Development Phase

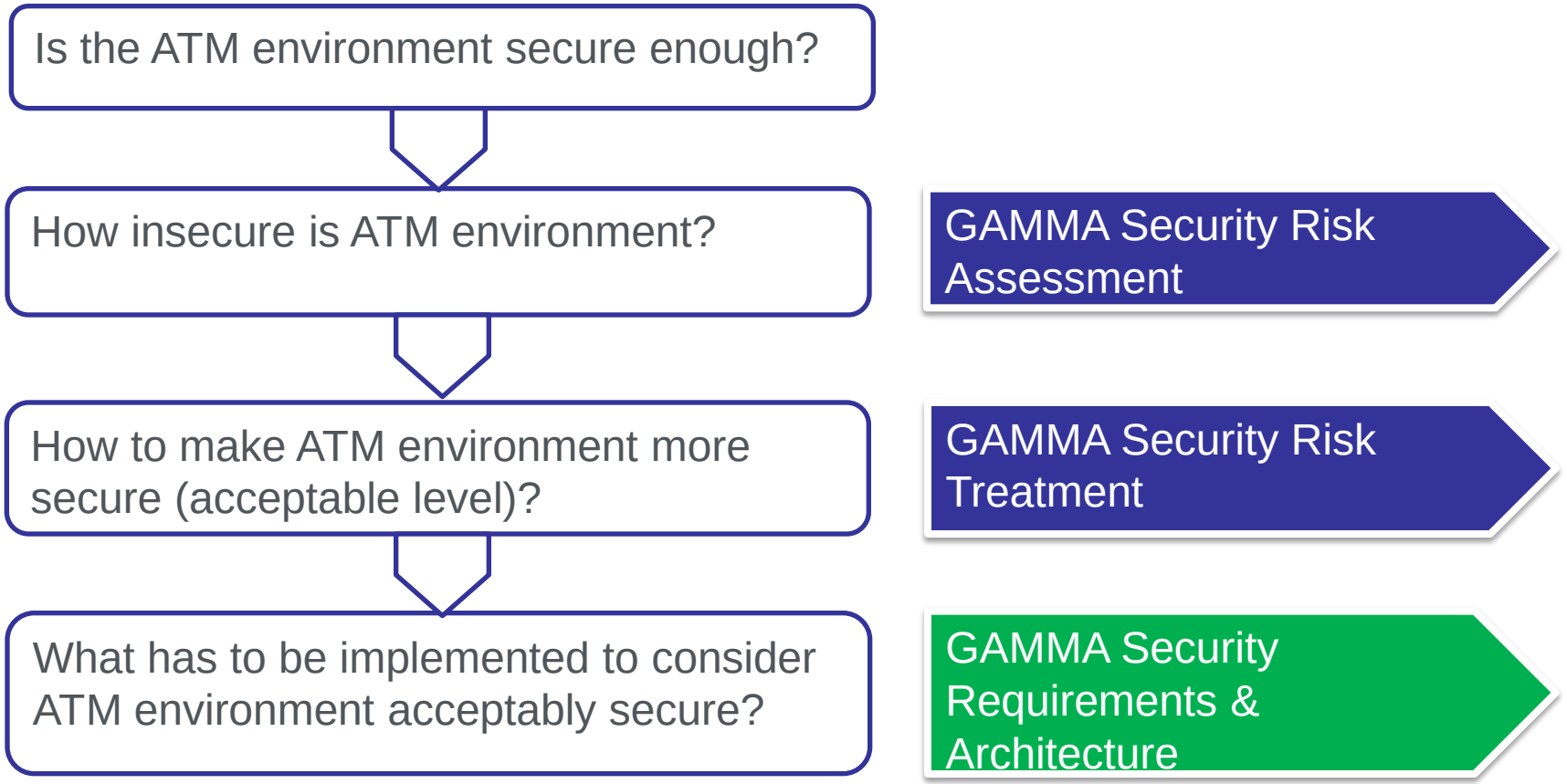
- Security “transversal activity”
- Security Risk Assessment
- Limited security engineering

SESAR Deployment Phase

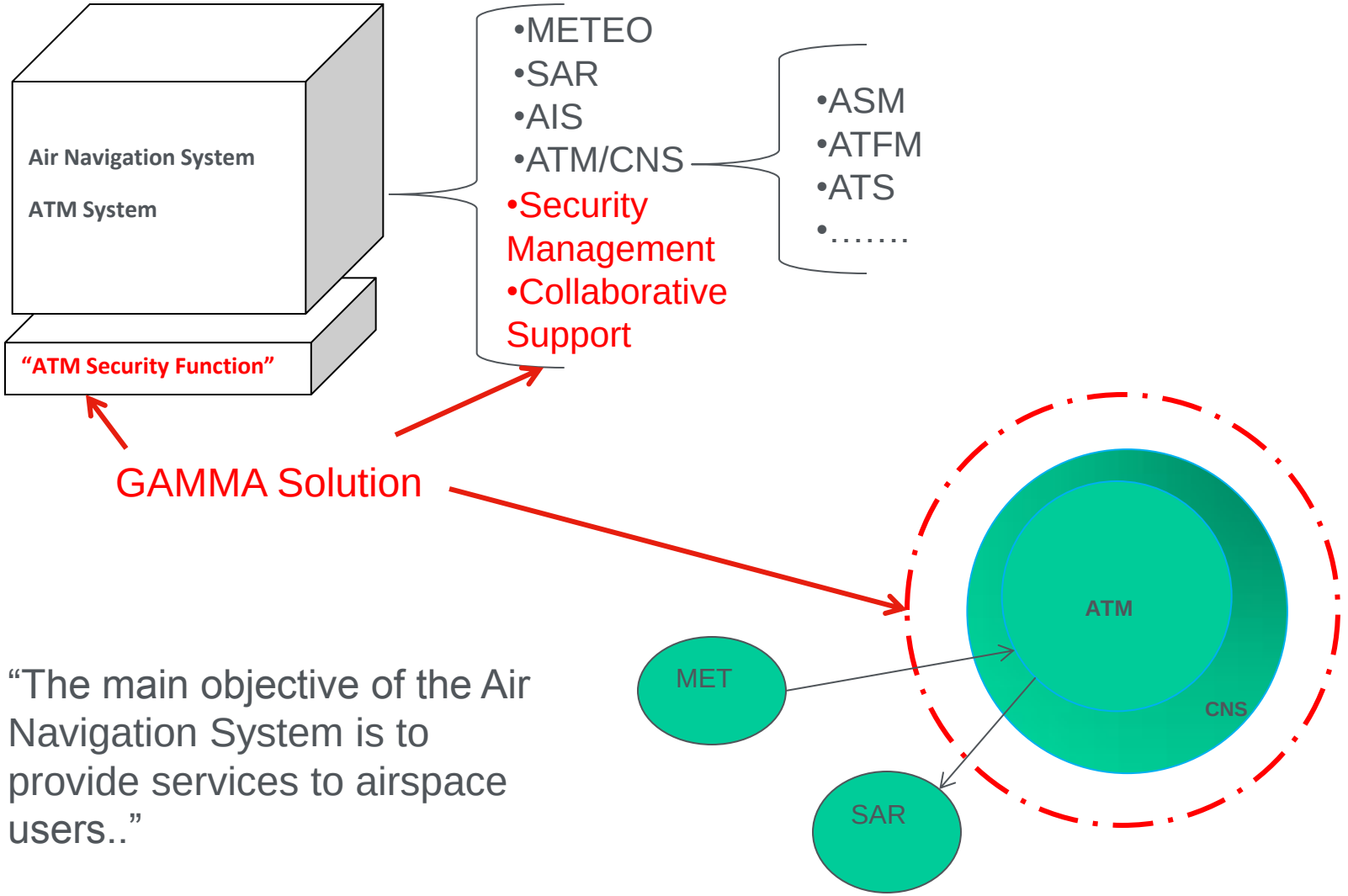
- “pilot” projects to deliver operational benefits
- Deployment Plan “recognises” “cyber security”

WP4 Objective and Scope

- **Objective**: To define the GAMMA solution that once implemented, the ATM environment can be considered as «Secure».
- **Scope**: Global approach for ATM environment focusing on Security Risk Assessment («most feared threat scenarios»)

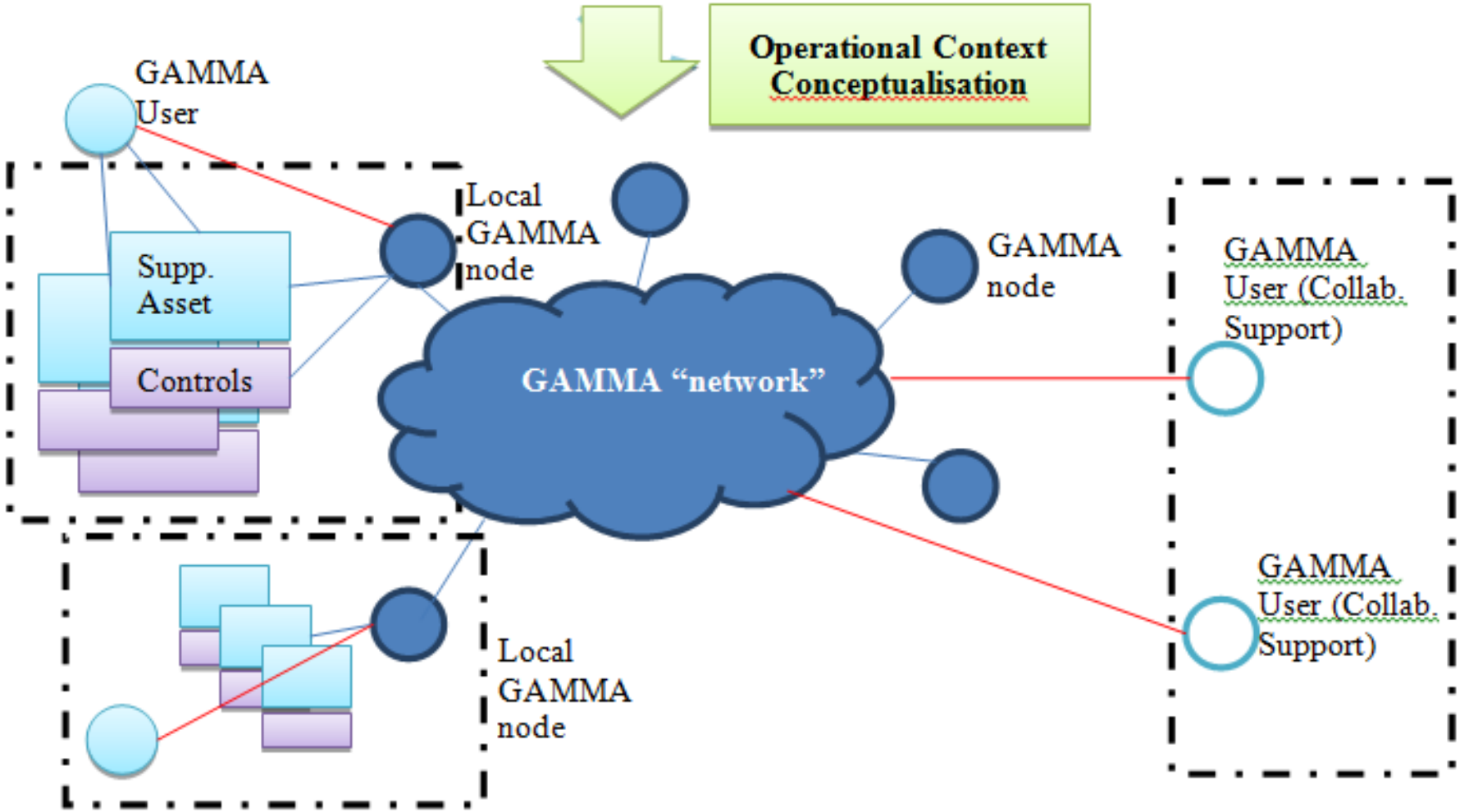


Third Input: ATM context for GAMMA scope establishment



"The main objective of the Air Navigation System is to provide services to airspace users.."

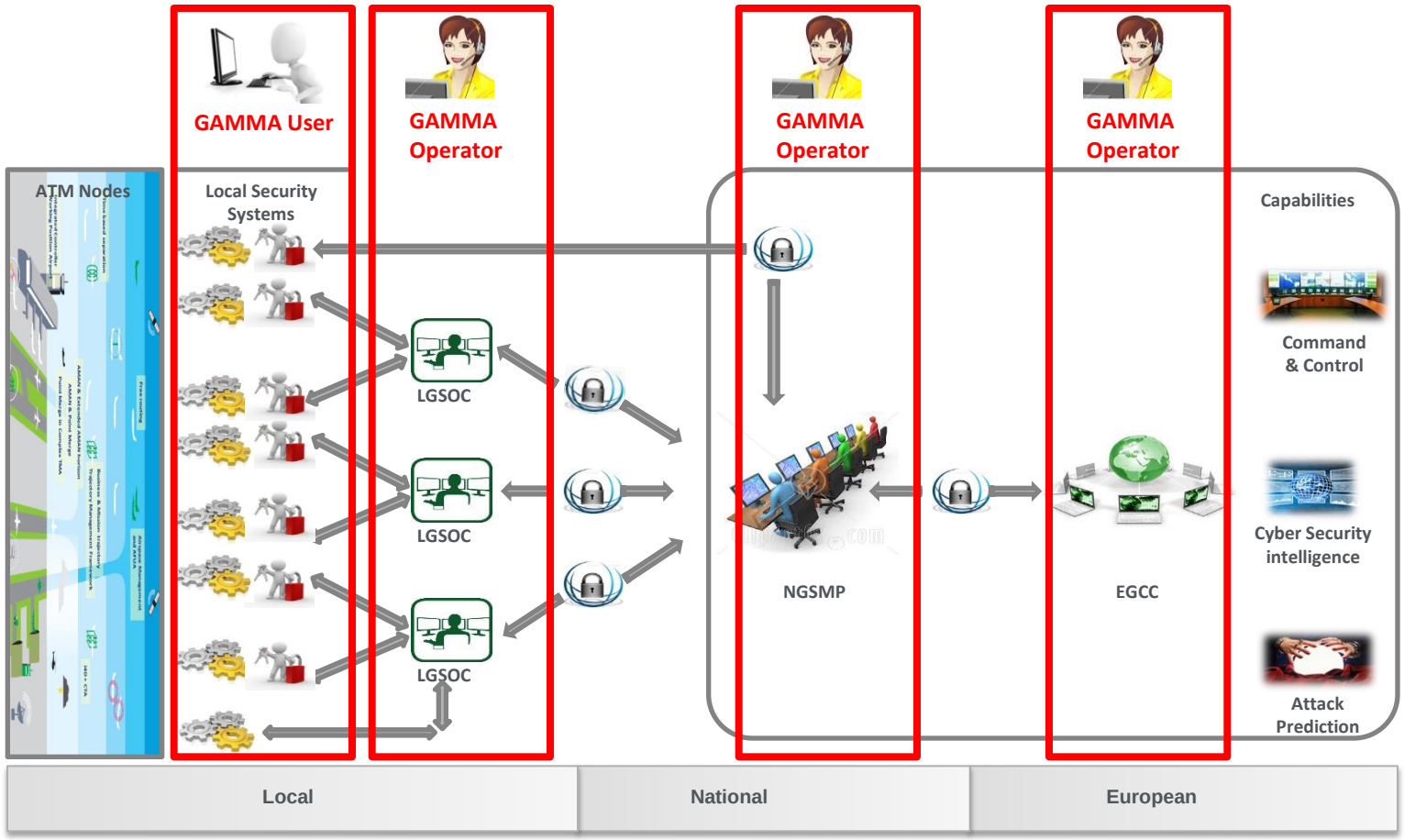
Operational Context



The GAMMA Concept 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.



Security Risk Assessment and Treatment in GAMMA

ATM Core Functions (Primary Assets) → Security Objectives

Supporting Assets

Threat Scenarios

Risks

To be treated to meet Sec Objectives !

Security Controls = MSSC + Additional SC

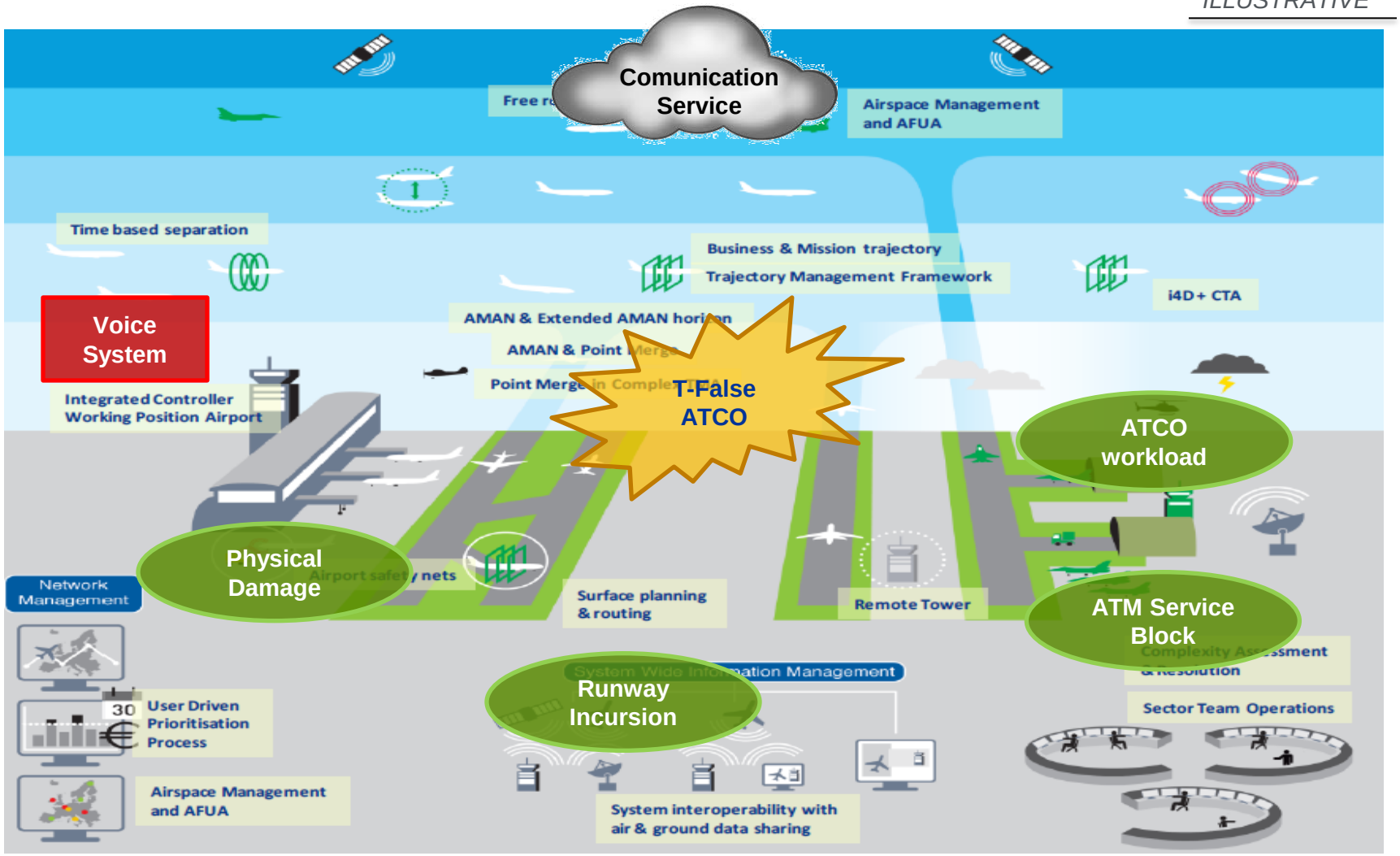
Security KPIs

To measure SCs effectiveness !!

Security Threats in the ATM world

Primary asset | Supporting Assets | Threats | Impacts

ILLUSTRATIVE



Security Objectives

Threat scenario	Description	Security KPI
False ATCO	Intrude unauthorized messages into the voice system	No. of unauthorized speakers detected in a defined time frame
		No. of detected dangerous/undesired aircraft behavior events in a defined time frame
Frequency Blocking	Make frequency useless for communication for the time the attack takes	No. of Denial of Service detected in a defined time frame.
Generation of attack impact prediction report	Perform DDoS attack against AeroMACS network.	False alarm rate
		Recorded time until detection
		Detection rate

Security Objective : The risk for the loss of integrity for Comunication service should be at minimum low.

Supporting Asset	Threat	Primary Asset	Reviewed Impact	Likelihood	Risk Level
Voice System	T - False ATCO	ATM information	5	4	High

Security Control ID	Supporting Asset affected	Security Control Description
ASC_TFA_05	Voice System	Air-Ground voice system in order to be protected from False ATCO shall be supported by means to detect voice pattern anomaly
ASC_TFA_06	Voice System	Each ACC/TWR shall operate and control speaker verification.
MSSC_TFA_01	Voice system	Each ACC/TWR shall have procedures in place that specify when and by whom external authorities (e.g. law enforcement, fire department, supervisory authorities) shall be contacted in the event of a false ATCO

From Security Controls to Security Requirements definition….

Requirement description	KPI (ID)	Source
REQ - ATC – 1: Formal exchange policies, procedures, and controls shall be in place to protect the voice system through the use of all types of communication facilities.	Sec_KPI_03 Sec_KPI_07 Sec_KPI_17 Sec_KPI_21	**MSSC_TFA_01**
REQ - ATC – 9: Voice pattern anomaly in air-ground voice communications shall be detected by technical means.	Sec_KPI_17 Sec_KPI_21	**ASC_TFA_05**
REQ - ATC – 10: Each ACC/TWR shall operate and control speaker verification.	Sec_KPI_17 Sec_KPI_21	**ASC_TFA_06**

Security KPI in GAMMA was defined by considering all the threat scenarios impacting on ATM system in order to measure the effectiveness of security controls…

In the example of the paper, these are the security KPIs traced to the security controls then developed in requirements:

Sec_KPI_03: Number of denial of service attacks detected in a defined time frame.
Sec_KPI_07: Number of disrupted data detected in a defined time frame.
Sec_KPI_17: Number of detected dangerous/undesired aircraft behaviour events in a defined time frame
Sec_KPI_21: Number of unauthorized speakers detected in a defined time frame.

To describe all the fields of the requirement card…

REQ - ATC Voice		
Identifier	REQ - ATC - 9	
Requirement Description	Voice pattern anomaly in air-ground voice communications shall be detected by technical means.	
Phase	Detection	
Type	System	
Validation Method	Simulation / Experts judgment	
Success Criteria	Earlier detection of voice pattern anomaly than with current system.	
REQ Trace		
Source	ASC_TFA_05	
Threat scenarios	T - False ATCO	
Supporting assets	Voice System	
Prototype	Secure ATC Communication (SACom)	
KPI	Sec_KPI_17	Number of detected dangerous/undesired aircraft behavior events in a defined time frame.
	Sec_KPI_21	Number of unauthorized speakers detected in a defined time frame.

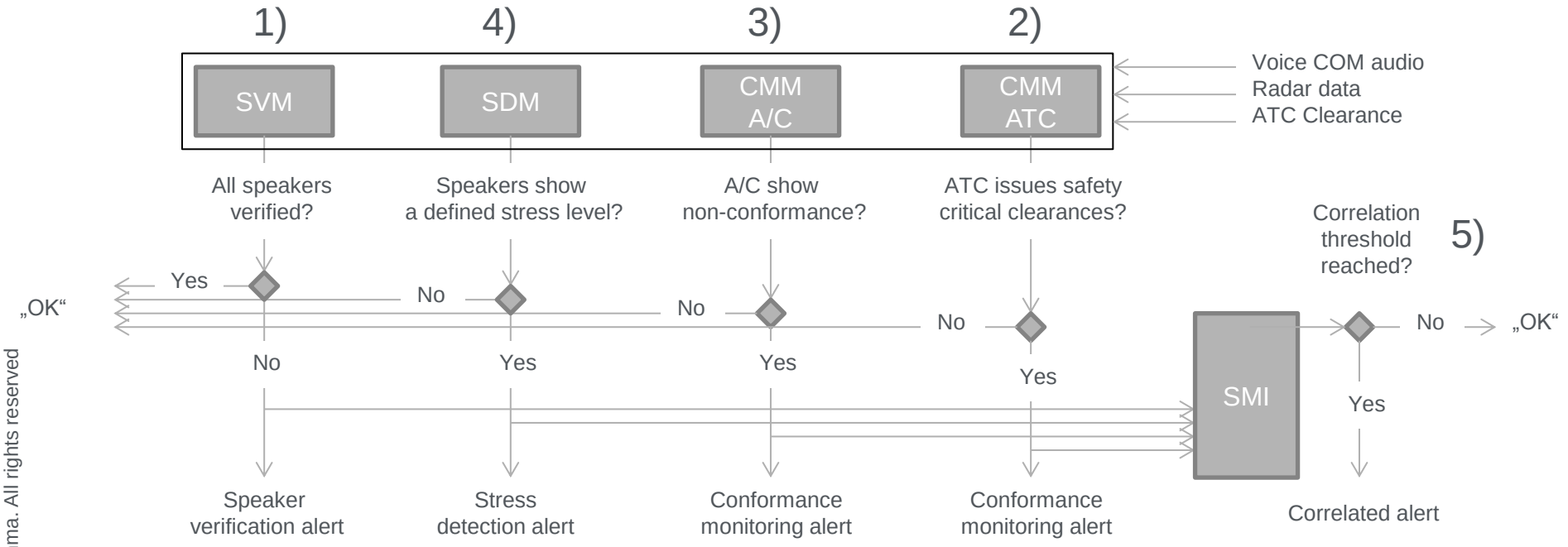
Added value of the prototype to the GAMMA solution

SACom

The prototype Secure ATC communication (SACom) shall

1) detect non-authorized communication (speaker recognition and verification)

2) identify abnormal behaviour of ground side (monitoring current traffic and comparison to normative behavior)



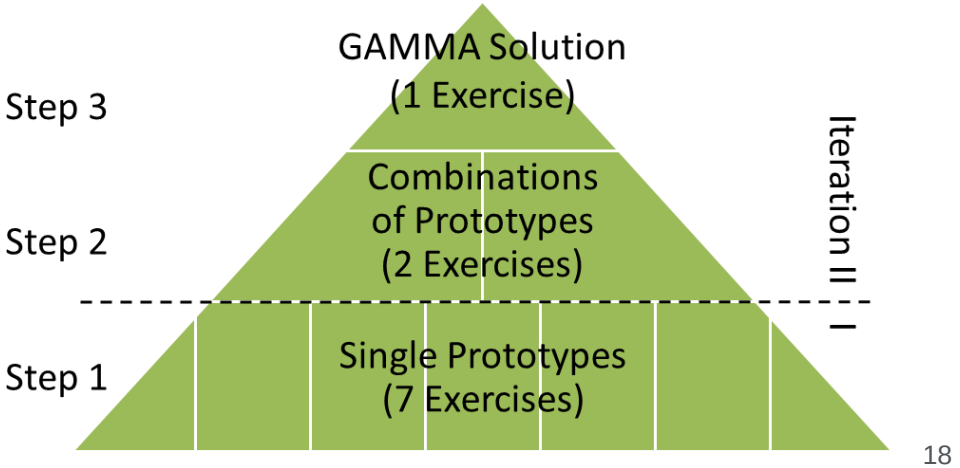
3) identify non-compliant action of onboard side including means of conformance monitoring

4) identify mental pressure of ATC and pilot by evaluating speech characteristics

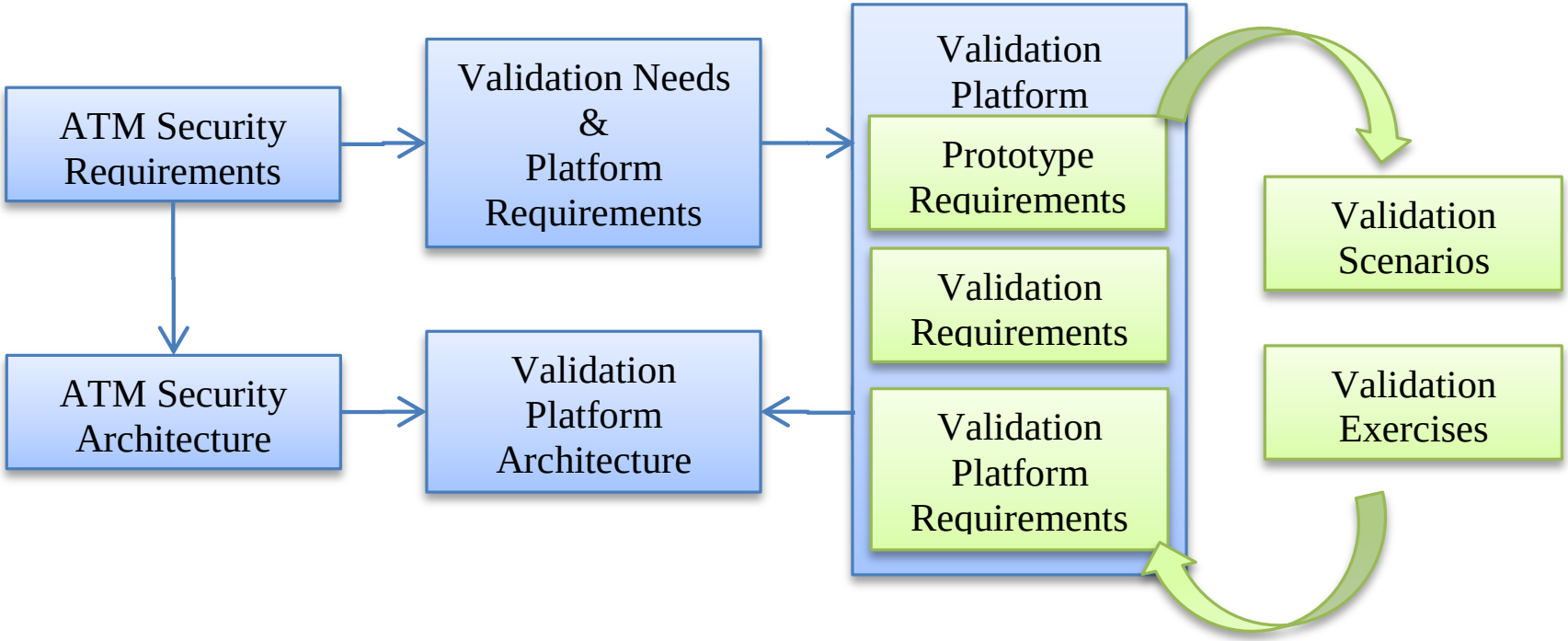
5) correlate different indications to provide information to GAMMA Security Management platform

Achievement for Validation Strategy Task 5.1

- **Validation** follows **ATM-security-incidents-centered approach** (not prototype-driven approach)
  → validation scenarios are specified for the selected threats identified in WP2
- **Most important objective** of validation exercises:
  demonstrate improvement in security management when security incidents occur
- **Information regarding GAMMA operational concepts' feasibility and benefits** of GAMMA will be **obtained on threat scenario level and for collective validation** (summed over all validation exercises).
- **Validations will be conducted in three steps:**
  - **Single prototype validation**
  - **Validation of combination of prototypes** (partially integrated GAMMA architecture)
  - **GAMMA concept validation** (fully integrated GAMMA architecture)



Iterative Validation



General Validation Goals

The general validation goals found in the project at hand are:

1. GAMMA-VALG-GEN-1: the ATM environment including GAMMA solution improves security management at local, national and European level compared to the defined baseline situation (without GAMMA solution).

2. GAMMA-VALG-GEN-2: the information can be accessed by the proper roles at the right time.

3. GAMMA-VALG-GEN-3: the sensible information is available only to the authorized roles.

Validation Goals for SACom prototype

Strategy-related Validation Goal ref.	Description	GAMMA Global Validation Goal ref.
GAMMA-VALG-STR-1	The information about security generated at local level is considered usable by all the roles when a threat is detected.	GAMMA-VALG-GEN-1
…	…	…
GAMMA-VALG-STR-4	The information about security generated at local level is considered beneficial by all the roles when a threat is detected.	GAMMA-VALG-GEN-1
…	…	…
GAMMA-VALG-STR-10	The GAMMA operator can access the information needed to perform its activities (prevention, detection and mitigation).	GAMMA-VALG-GEN-2
…	…	…
GAMMA-VALG-STR-14	Exchanged information and new procedures performed are in line with the current regulations.	GAMMA-VALG-GEN-1 GAMMA-VALG-GEN-2 GAMMA-VALG-GEN-3

Objective ID	Objective Description	Validation Strategy Goal
Obj.-5_1:	To validate that the detection of a False ATCO is optimized by using the prototype	GAMMA-VALG-STR-1 GAMMA-VALG-STR-4 GAMMA-VALG-STR-10 GAMMA-VALG-STR-14
Obj.-5_2:	To validate that the performance of the prototype is acceptable (regarding false alarms, correct detection, usefulness and trust)	GAMMA-VALG-STR-1 GAMMA-VALG-STR-4 GAMMA-VALG-STR-10 GAMMA-VALG-STR-14
Obj.-5_3:	To compare the impact of individual prototype subsystems (speaker verification module (SVM), stress detection module (SDM) and conformance monitoring module (CMM)) on threat management	N/A
Obj.-5_4:	To validate that the solution leads to a better situational awareness of ATCO regarding appearance of False ATCO	GAMMA-VALG-STR-1 GAMMA-VALG-STR-4

Obj 5.1 «To validate that the detection of a False ATCO is optimized by using the prototype»

Acceptance criteria

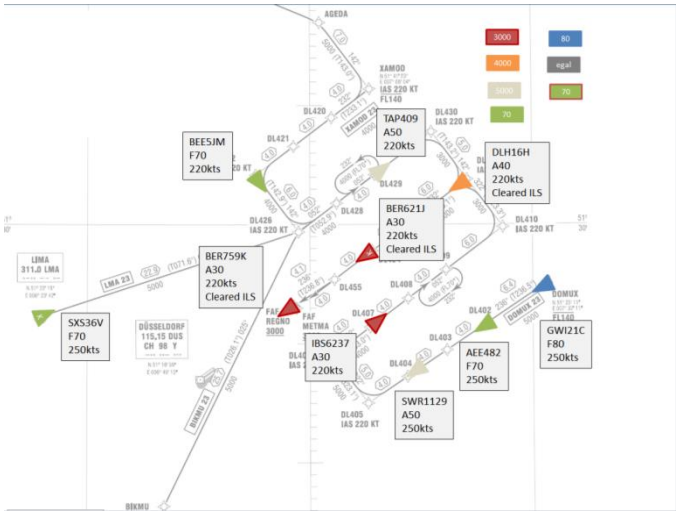
VAC-ID	Req-ID	Objective	Acceptance Criteria
...	...	...	...
AC_SACom_6	REQ - ATC - 9	Obj.-5_2	Stress detection module assistance will be accepted by ATCOs
AC_SACom_7	REQ - ATC - 9	Obj.-5_1	With the SACom prototype stress detection module the detection rate of False ATCOs is improved compared to the baseline
AC_SACom_8	REQ - ATC - 9	Obj.-5_1	With the SACom prototype stress detection module the false alarm rate of identifying False ATCOs is not degraded compared to the baseline
AC_SACom_9	REQ - ATC - 9	Obj.-5_1	With the SACom prototype stress detection module False ATCOs are detected earlier compared to the baseline
AC_SACom_10	REQ - ATC - 9	Obj.-5_2	With the SACom prototype stress detection module ATCOs situation awareness ratings are improved compared to the baseline
AC_SACom_11	REQ - ATC - 10	Obj.-5_2	Speaker verification module assistance will be accepted by ATCOs
AC_SACom_12	REQ - ATC - 10	Obj.-5_1	With the SACom prototype speaker verification module the detection rate of False ATCOs is improved compared to the baseline
AC_SACom_13	REQ - ATC - 10	Obj.-5_1	With the SACom prototype speaker verification module the false alarm rate of identifying False ATCOs is not degraded compared to the baseline
AC_SACom_14	REQ - ATC - 10	Obj.-5_1	With the SACom prototype speaker verification module False ATCOs are detected earlier compared to the baseline
AC_SACom_15	REQ - ATC - 10	Obj.-5_4	With the SACom prototype speaker verification module ATCOs situation awareness ratings are improved compared to the baseline
AC_SACom_16	... REQ - ATC – 9 REQ - ATC – 10	Obj.-5_2	SACom prototype assistance will be accepted by ATCOs
AC_SACom_17	... REQ - ATC – 9 REQ - ATC - 10	Obj.-5_1	With the SACom prototype the detection rate of False ATCOs is improved compared to the baseline
AC_SACom_18	... REQ - ATC – 9 REQ - ATC - 10	Obj.-5_1	With the SACom prototype the false alarm rate of identifying False ATCOs is not degraded compared to the baseline
AC_SACom_19	... REQ - ATC – 9 REQ - ATC - 10	Obj.-5_1	With the SACom prototype False ATCOs are detected earlier compared to the baseline
AC_SACom_20	... REQ - ATC – 9 REQ - ATC - 10	Obj.-5_4	With the SACom prototype ATCOs situation awareness ratings are improved compared to the baseline

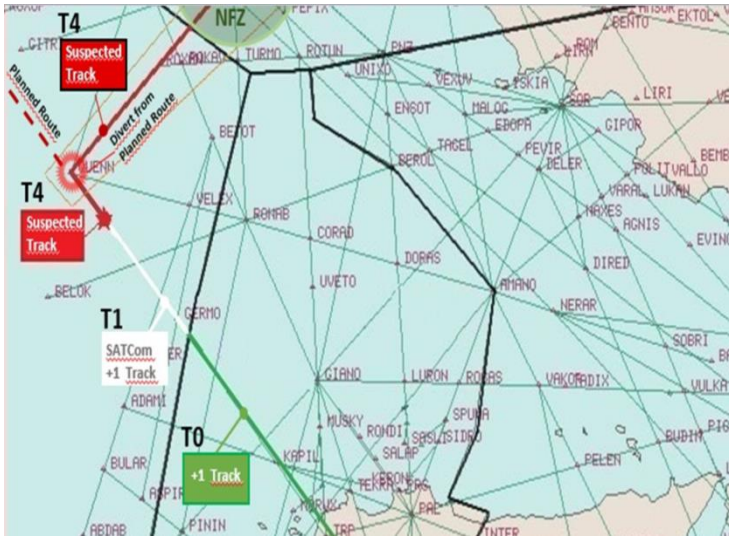
AC_SACom_9	**REQ - ATC - 9**	**Obj.-5_1**	**With the SACom prototype stress detection module False ATCOs are detected earlier compared to the baseline**

Sec_KPI_17: Number of detected dangerous/undesired aircraft behaviour events in a defined time frame

Next Steps

- Validations of individual prototypes take place at the moment
- SACom Validations are Human-In-the-Loop Simulations
  - Validation data will be collected as well prior as occasionally and also after the exercises of the validation campaigns
  - Validation data consists of
    - Recorded speech samples,
    - Recorded flight paths of aircraft,
    - Recorded single and correlated indicator values
    - questionnaires provided before, inbetween and after the exercises
- Validations of the partial and fully integrated GAMMA concept will take place in spring 2017





Summary and Conclusions

Paper "*Addressing Security in the ATM Environment*"

"The proposed solution goes beyond the theoretical approach. The validation of the solution will assess the feasibility of the concept through the development of prototypes which will be examined in the validation exercises. The implementation furthermore benefits from automation while providing a complete picture of the ATM Security and the establishment of a reliable collaborative framework."

Summary and Conclusions

- NextGen and SESAR offer an unique (“technological”) opportunity
- The approach to security and a security capability is not addressed due to political and operational priorities
- GAMMA addresses this void offering “dual use” / complementary solutions to SESAR
- GAMMA developed a Security Situation Management Concept of Operations that allows for
  - a modular / iterative implementation and build up of a “security function” in ATM/Air Navigation
  - distributed situation management and decision-making recognising “classical” ATM actors and security actors (i.e. GAMMA organisation)
  - Hierarchical national implementation and wider regional collaboration
- Filling the void of “security validation” in ATM
- Validation of security solutions (“prototypes” → nodes), human-in-the-loop

Thanks for your attention!

Questions ?

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