Validating an ATM Security Prototype – First Results

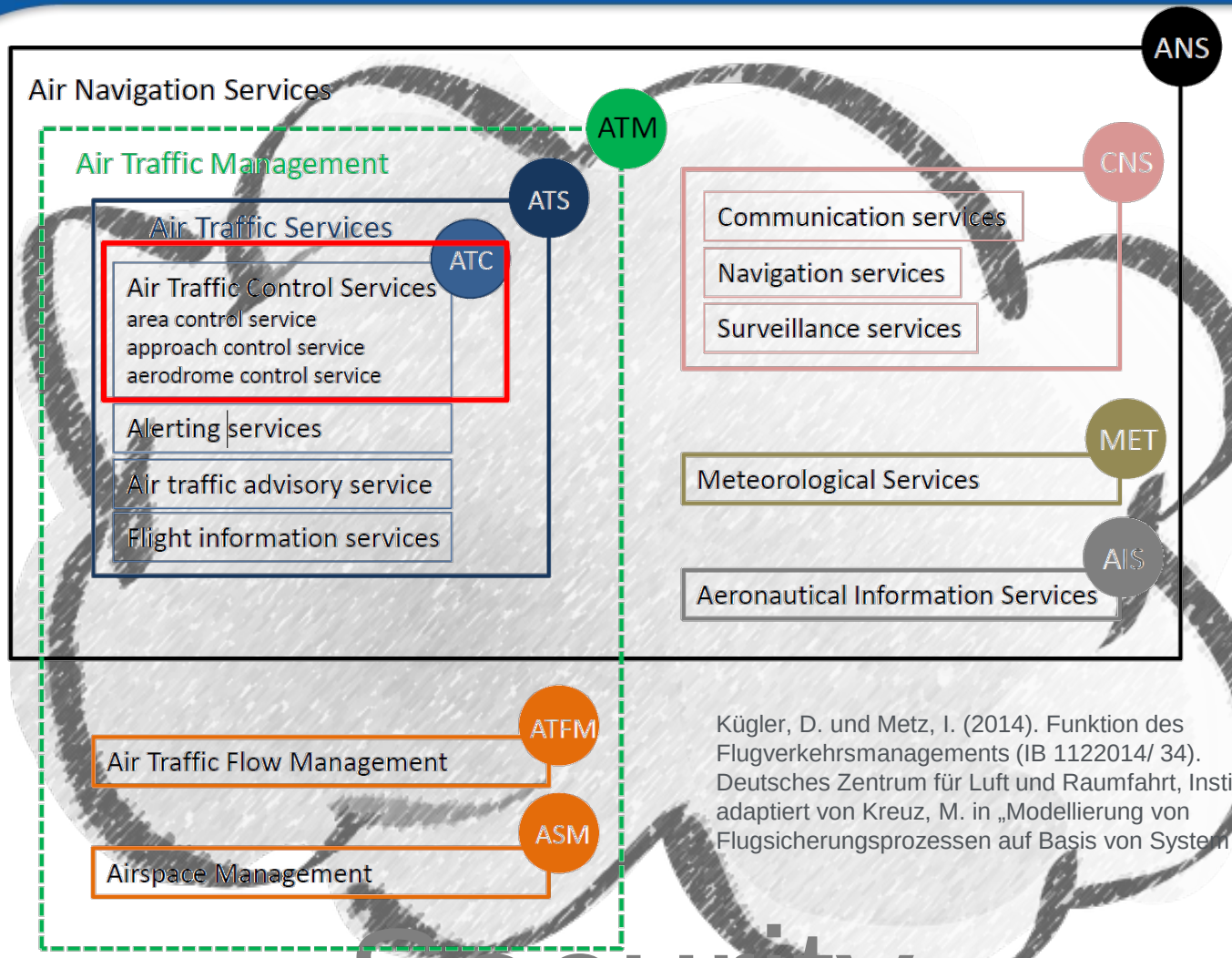
35th DASC, Tim H. Stelkens-Kobsch, Michael Finke

Sacramento, 29 September 2016

Overview

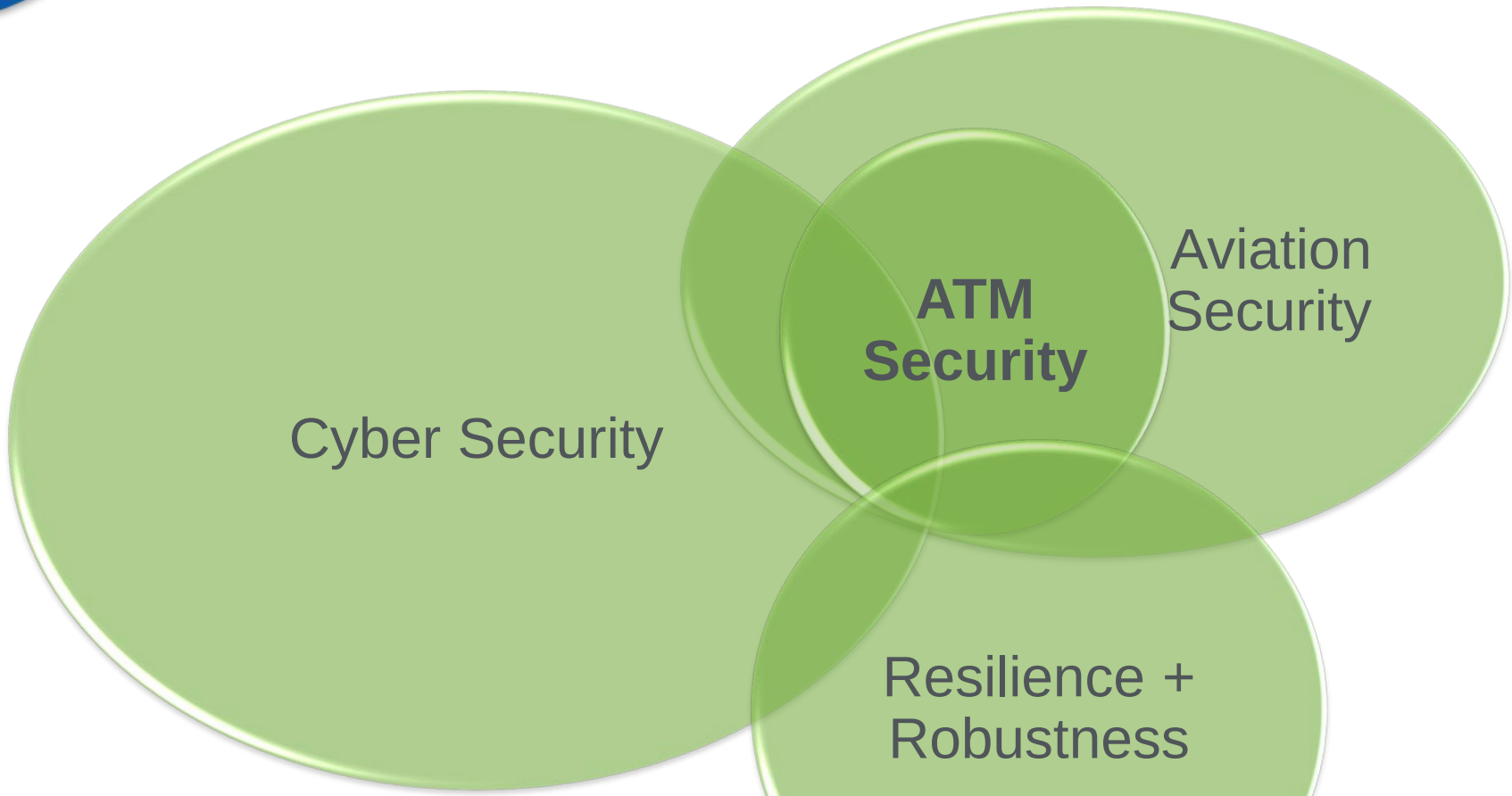
- Context Establishment
- Security Risk Assessment and Treatment
- Validation Methodology
- Validation Approach for SACom
- First Results
- Conclusions
- Outlook

Context – ATM Security



Kügler, D. und Metz, I. (2014). Funktion des Flugverkehrsmanagements (IB 1122014/ 34). Deutsches Zentrum für Luft und Raumfahrt, Institut für Flugführung; adaptiert von Kreuz, M. in „Modellierung von Flugsicherungsprozessen auf Basis von System Dynamics“, 2015

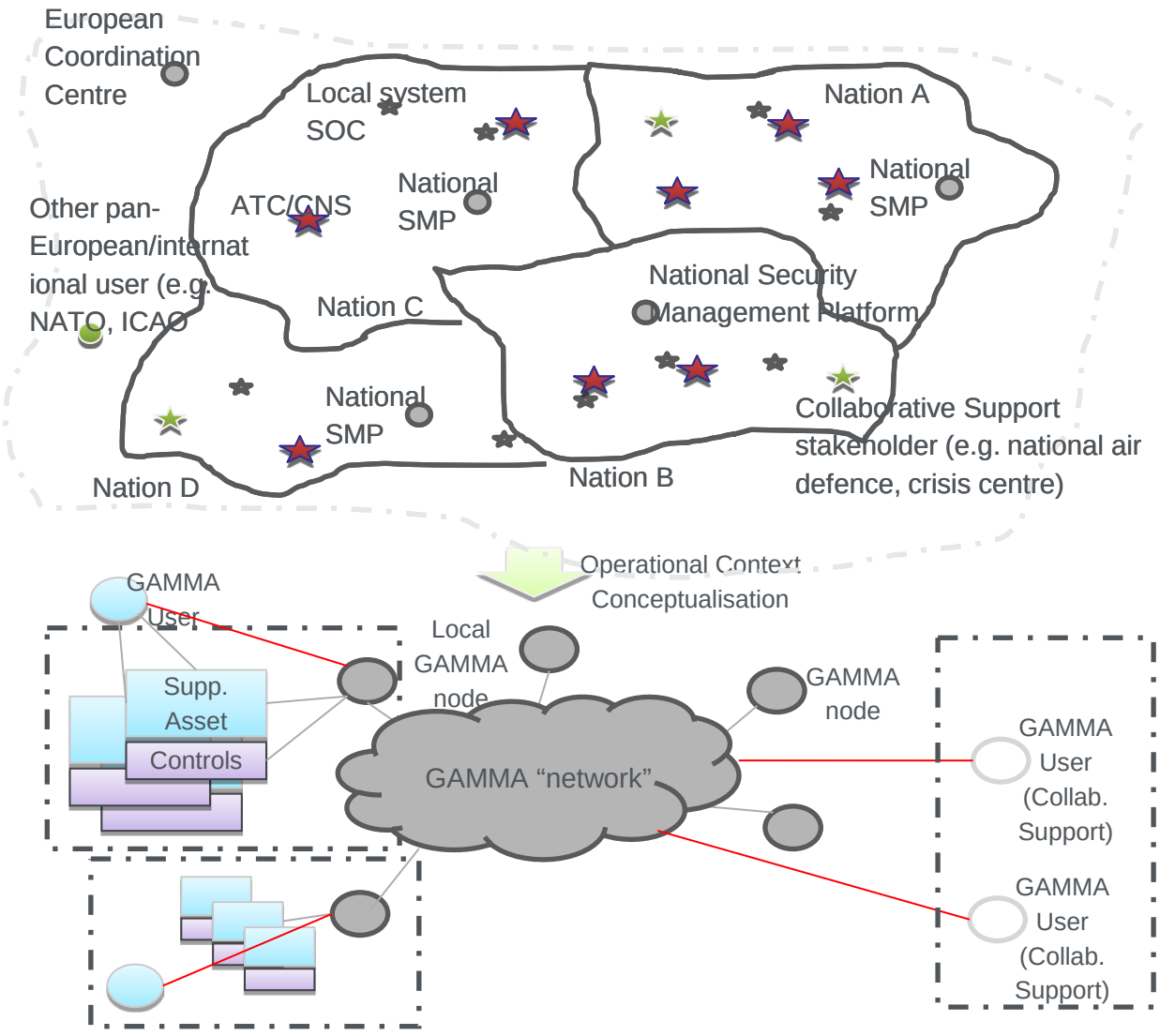
Context – ATM Security



SESAR addresses emerging operational concepts and technical enablers.
But the security validation of these novel SESAR solutions is none to limited.

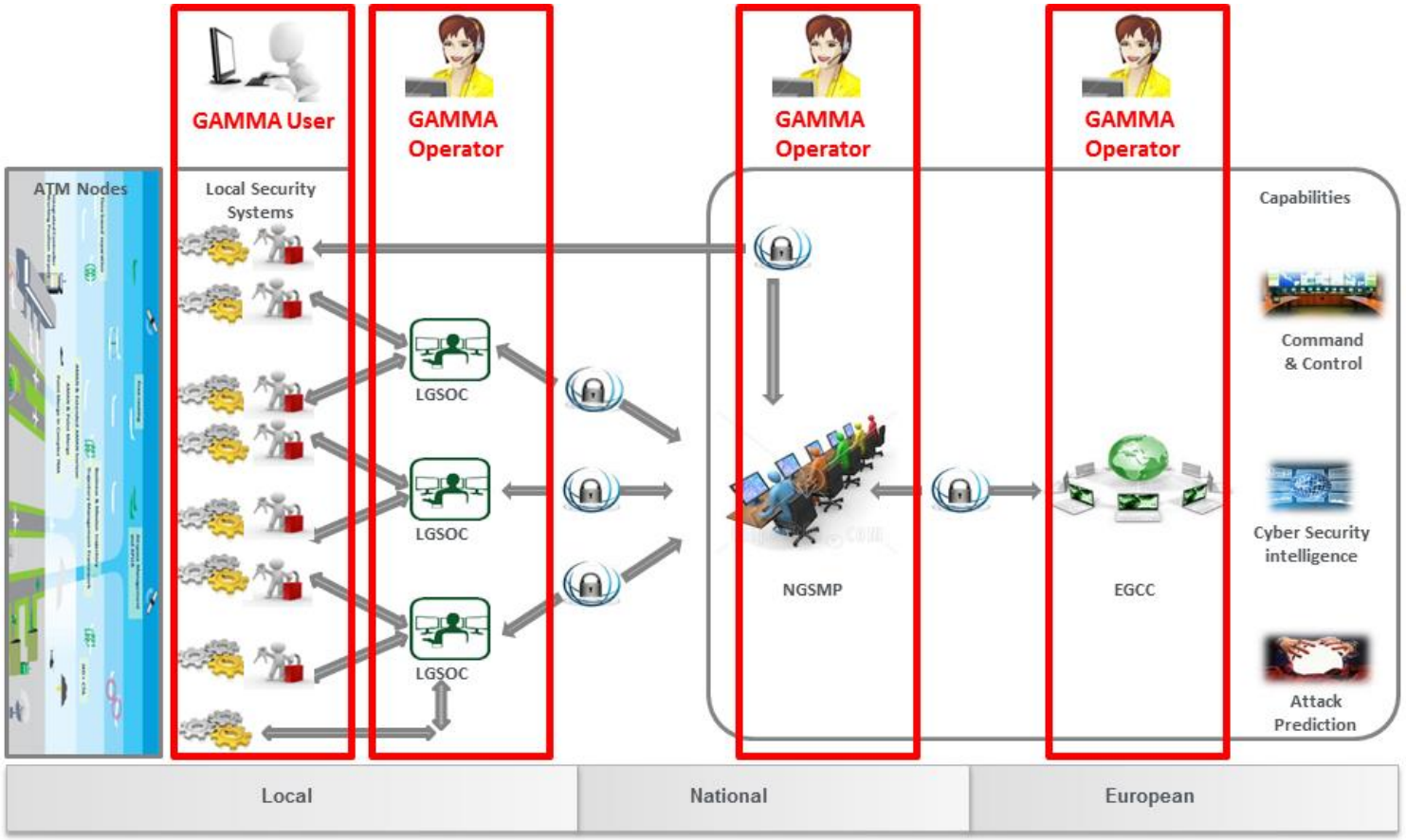
FP7 Project: Global ATM Security Management (GAMMA)

Context Conceptualisation



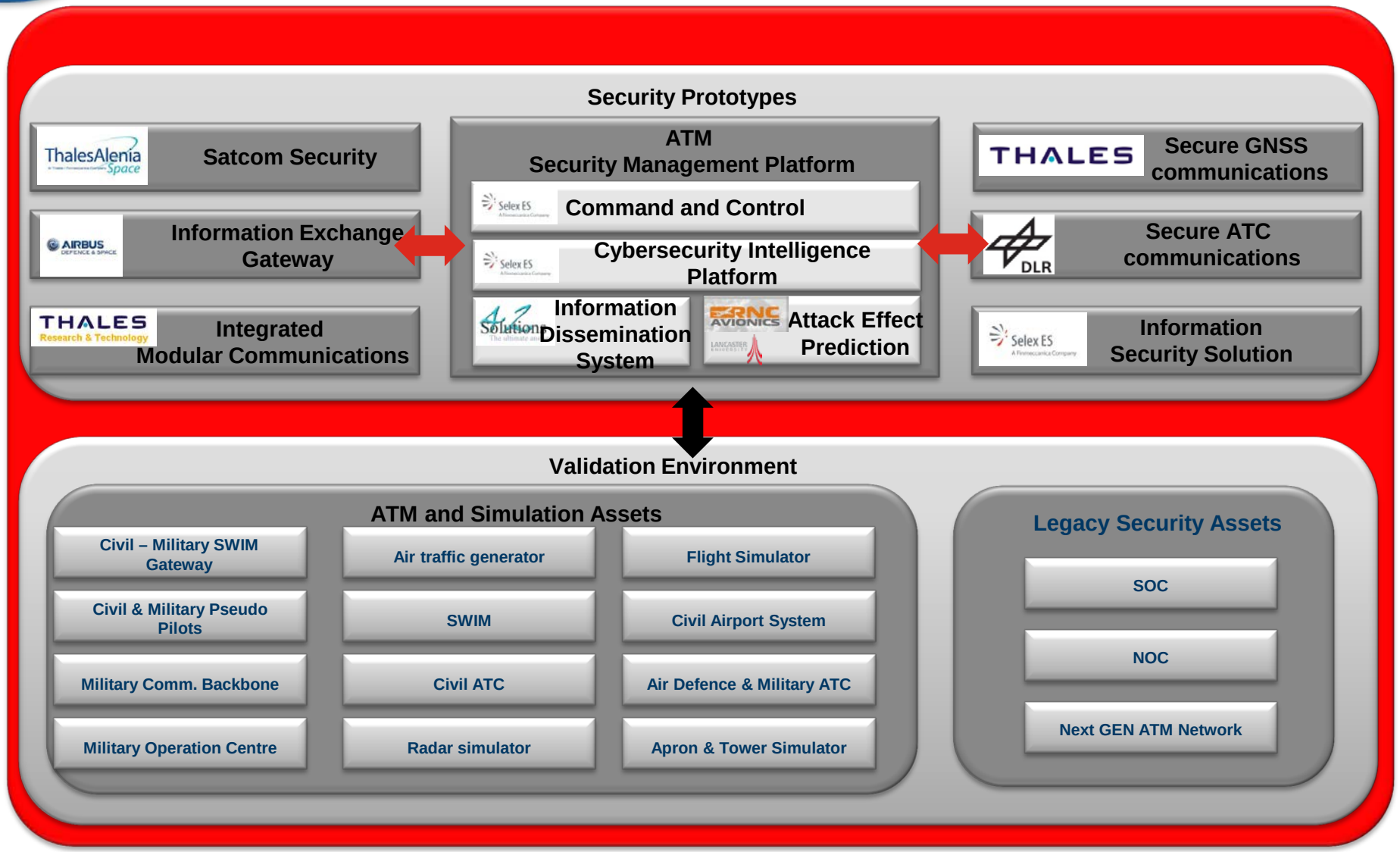
Two different human roles considered within GAMMA concept:

- GAMMA Operators performing functions within the LGSOC, NGSMP and EGCC;
- GAMMA Users using local security systems.



FP7 Project: Global ATM Security Management (GAMMA)

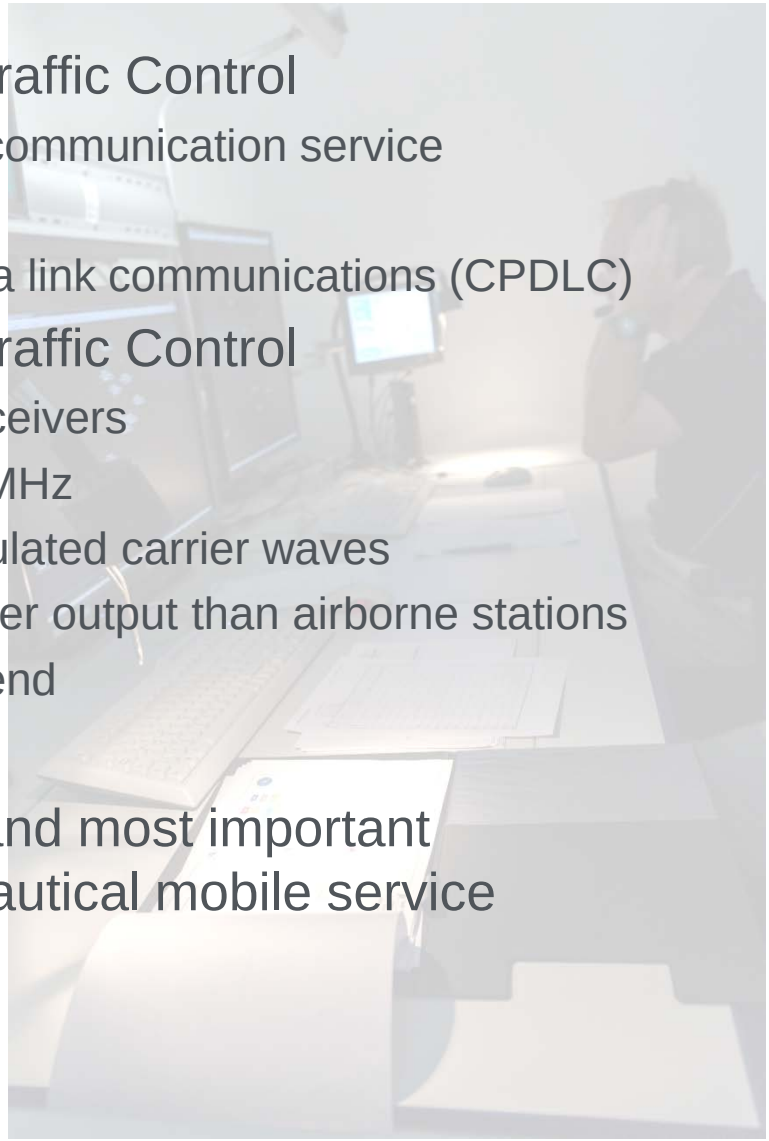
GAMMA Prototypes and Validation Environment



What are we treating here?

ATC Voice Communication

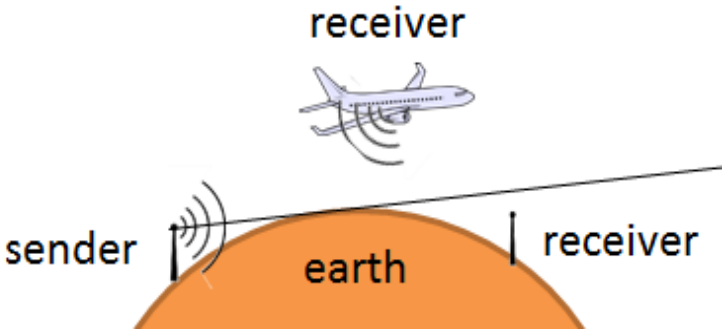
- Air Ground Communication in Air Traffic Control
  - Part of international aeronautical telecommunication service
  - Aeronautical mobile service
  - Differentiation between voice and data link communications (CPDLC)
- Air Ground Communication in Air Traffic Control
  - Omnidirectional analogue radio transceivers
  - VHF band within 117.975 – 137.000 MHz
  - Double-sideband and amplitude modulated carrier waves
  - Ground stations work with higher power output than airborne stations
  - Requires line-of-sight to a certain extend



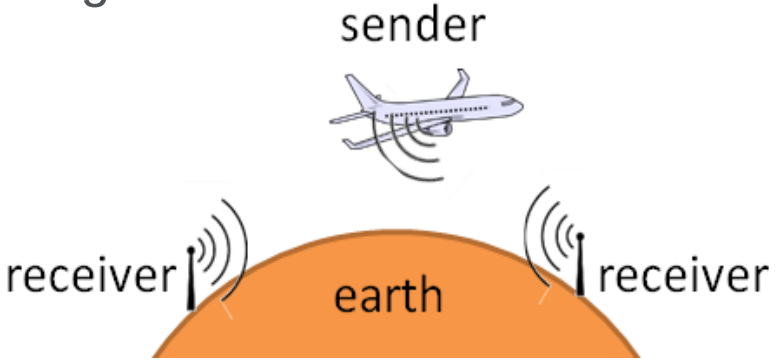
Voice communication still the basic and most important communication method within aeronautical mobile service

Security Risk in Voice Communication

- Radio transmitter equipment generally available
- Line-of-sight dependency
- Signal power decreases with distance
  (nearby stations may block out stations far away)
- Analogue distribution of communication
- Limited number of frequency bands
- Open to masquerading intruders
- No protection against frequency blocking
- Significant number of attacks
- Attacks pose real danger of confusing air traffic controllers



Ground Receiver Does Not Track Sender

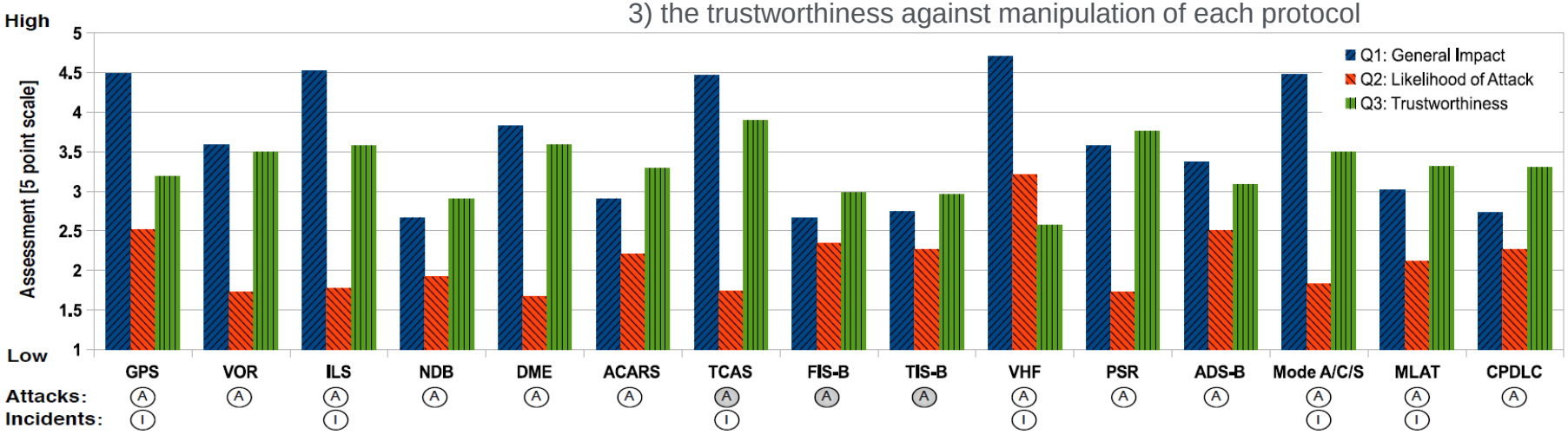


Both Receivers Track Sender

Security Risk in Voice Communication

- Analogue voice communication between air traffic control and aircraft pilots is one of the major security risks identified.
- Radio transmissions in civil ATC neither encrypted nor verified by signature or otherwise protected → can easily be intruded by unauthorized persons.
- Reported increase in non-legitimate use of frequency in recent years.
- Pirate radio stations

Assessment of
1) the flight safety impact,
2) the likelihood of being attack targets and
3) the trustworthiness against manipulation of each protocol

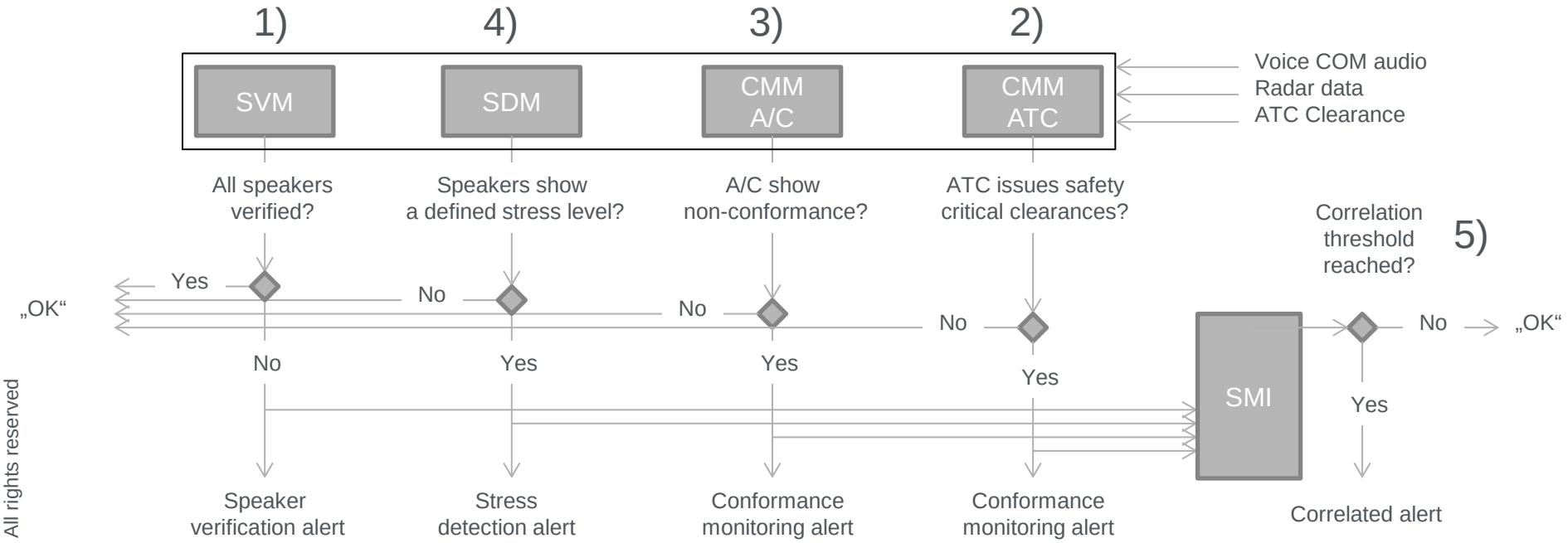


"On Perception and Reality in Wireless Air Traffic Communications Security", Strohmeier et al., 2016

Proposed Prototype to Secure ATC Communications

SACom prototype (developed by DLR and SAV*)

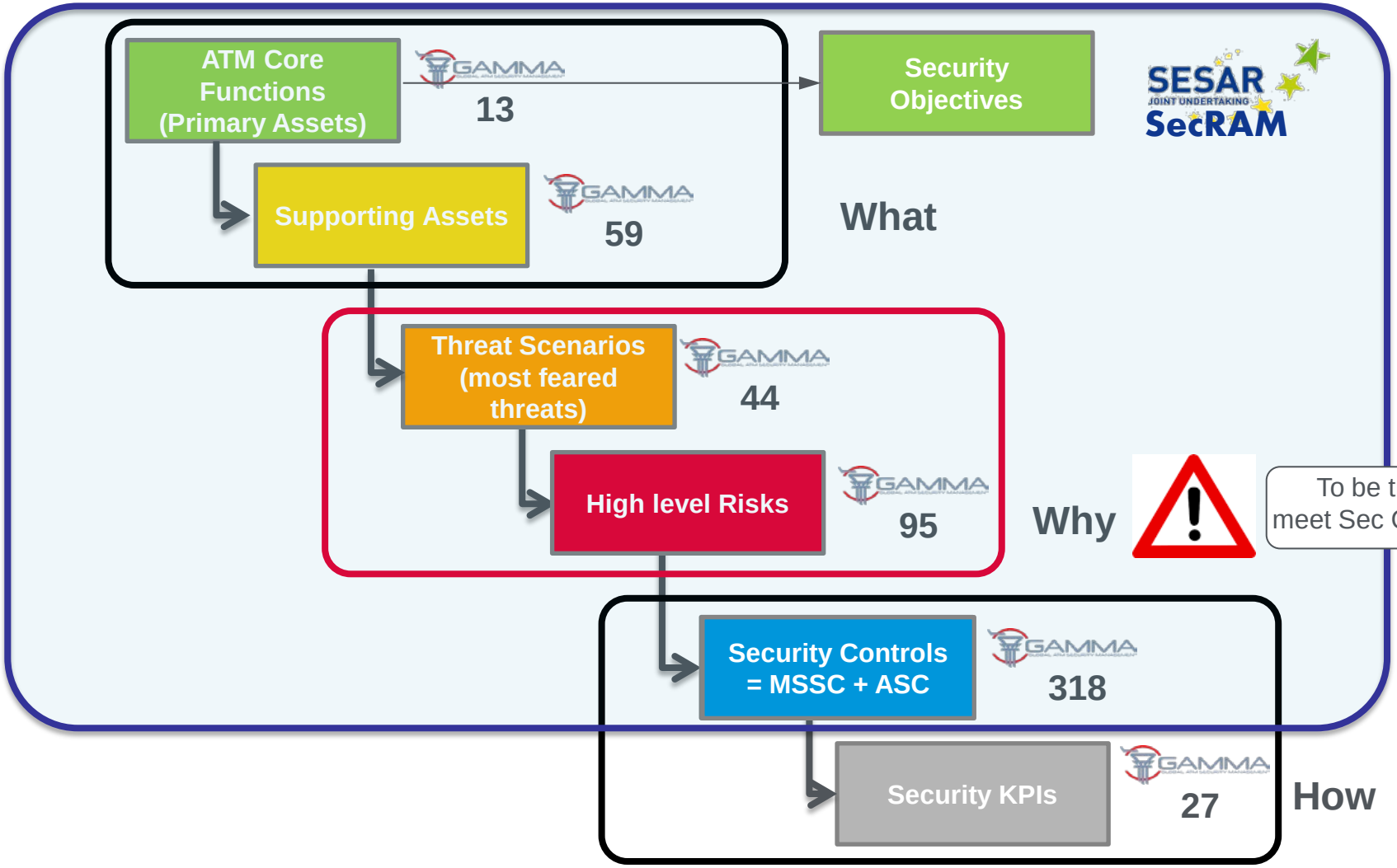
1) detect non-authorized communication (using speaker recognition and verification)
2) identify abnormal behaviour of ground side (monitoring current traffic and comparison to normative behavior)



3) identify non-compliant action of onboard side (including means of conformance monitoring)
4) identify mental pressure of ATC and pilot (evaluating speech characteristics)
5) correlate different indications (provide information to GAMMA SMP)

* Slovak Academy of Science

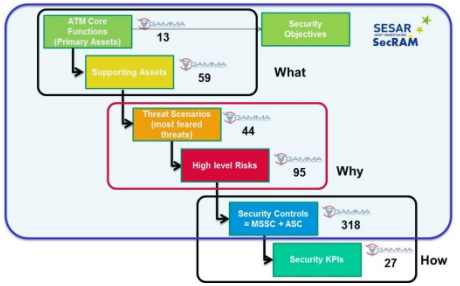
Security Risk Assessment and Treatment in GAMMA



Security Risk Assessment and Treatment in GAMMA

Projected to SACom

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



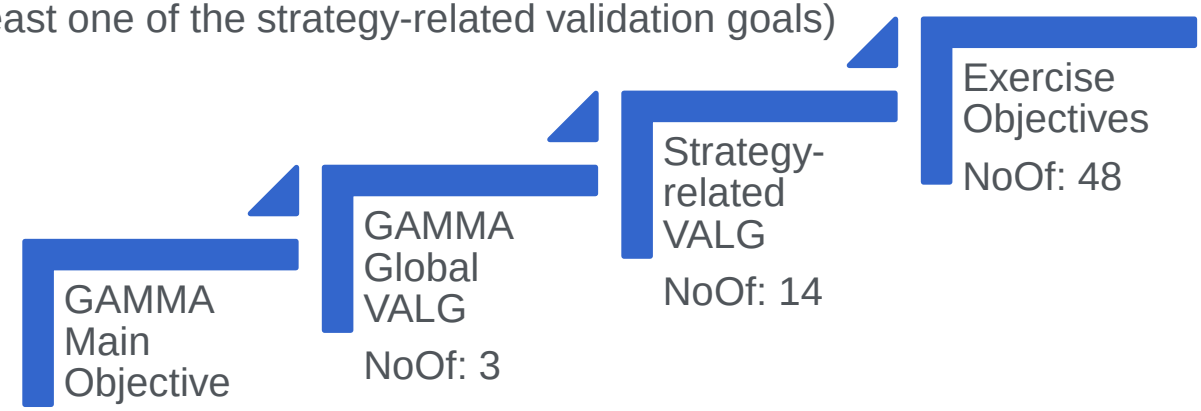
Security Control ID	Supporting Asset affected	Security Control Description
ASC_TFA_05	Voice System	Air-Ground voice system in order to be protected from False ATCO shall be supported by means to detect voice pattern anomaly
ASC_TFA_06	Voice System	Each ACC/TWR shall operate and control speaker verification.
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

Security Objective : Risk for loss of integrity of communication service should be low.

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**

Validation Methodology for ATM Security Prototypes

- In order to achieve the main GAMMA objectives and to comply with specific needs identified, **different levels of validation goals are proposed**:
  - **General GAMMA validation goals** applying to all type of validation exercises and linked to these.
  - **Strategy-related validation goals**, applicable to each types of validation exercises (linked to global validation goals), dependent on validation approach chosen.
    → there are three types of strategy-related validation goals:
    - focused on validation of individual prototypes
    - focused on partial integration of prototypes (event detector prototypes + national level of SMP) and
    - focused on a full integration of GAMMA solution (event detector prototype + National level of SMP + European level of SMP)
- Each validation exercise defines **specific exercises objectives** (linked to at least one of the strategy-related validation goals)



Needed steps to validate SACom

- Briefing of test person,
- Speaker verification enrollment,

- Simulator training,
- 20 Short simulations,

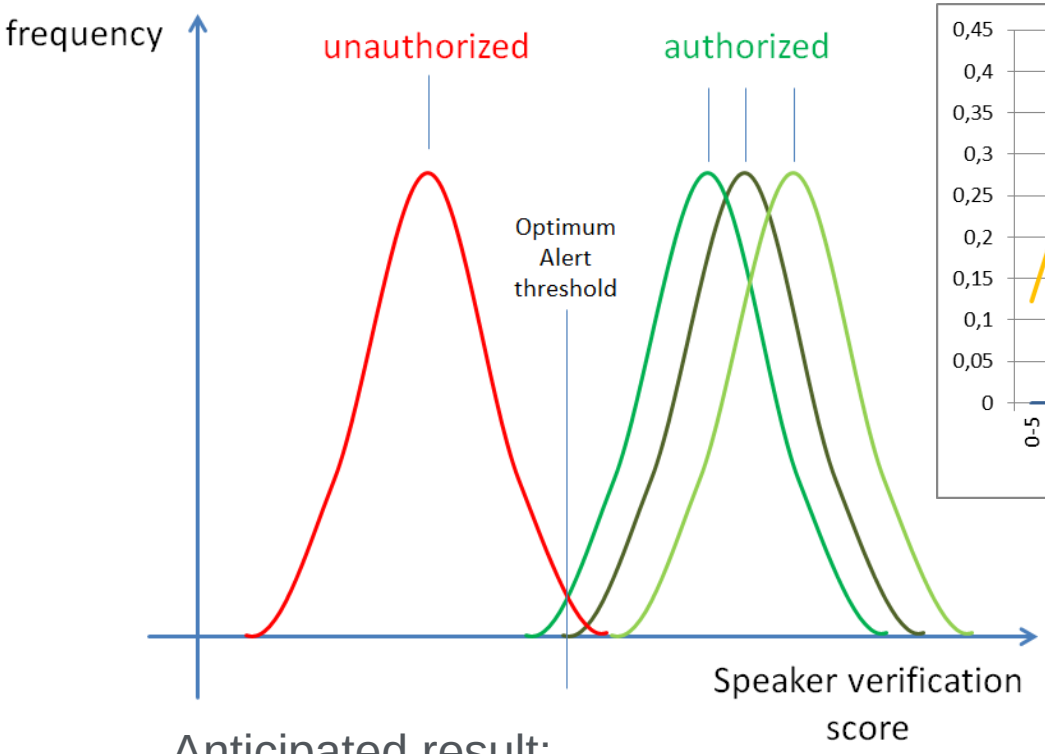
- SACom briefing,

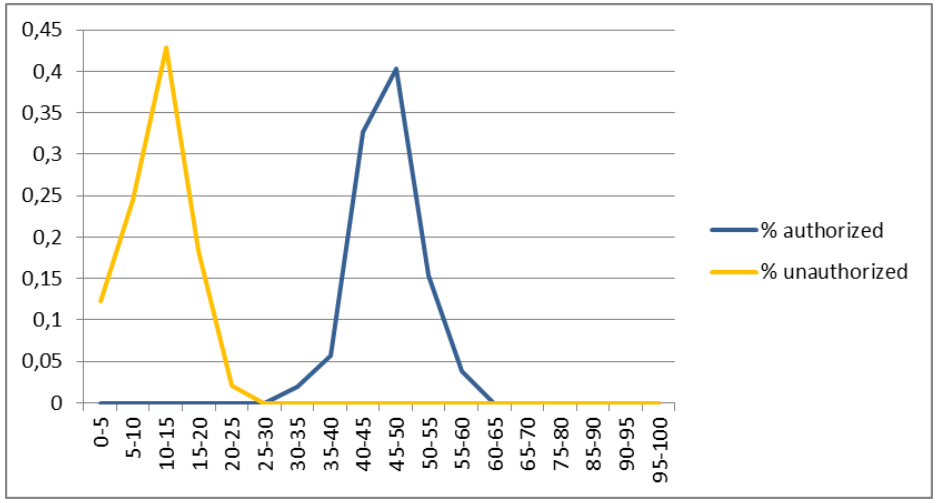
- SACom training

- One long simulation

- De-briefing and questionnaires

First Validation Results – Speaker Verification





results from a validation trial
03/08/2016, Braunschweig

Anticipated result:
each speaker´s utterances distributed around a distinct value.
all authorized speakers show higher x-value
unauthorized speaker show lower x-value

First Validation Results – Stress Detection

- situation to cause stress and stress scores just associated by chance because of:
  → sophisticated training
  → balanced nature
  → what about aggressors?

- Challenge: distinguish between different stress typologies (e.g. excitement, high workload, other “normal” reasons) and stress resulting from precarious and unlawful intervention.

Figure 3.1: A two-dimensional representation of emotion terms (vertical dimension: active/passive; horizontal dimension: positive/negative) after [Sche 01a]

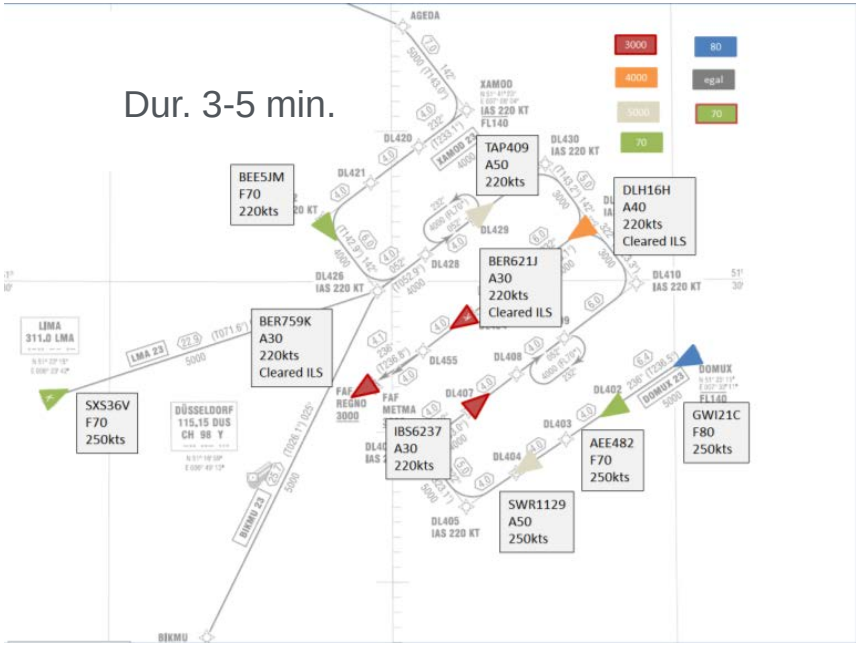
First Validation Results – Conformance Monitoring

$$DR_{CM} = \frac{\sum \text{Correctly Detected Deviations}}{\sum \text{All Deviations}}$$

$$FAR_{CM} = \frac{\sum \text{Incorrect Deviation Alerts}}{\sum \text{All Deviation Alerts}}$$

$$DS_{CM} = T_{Detection} - T_{Initial\ Occurence}$$

- 20 short validation exercise scenarios used.
- Time of first occurrence of a conflict stored in database.
- Results show False Alarm Rates (FAR) of SACom of around 7%.
- Results show average $DS_{CM,\ ATCo}$ of 40.6 seconds and $DS_{CM,\ SACom}$ of 18.9 seconds.



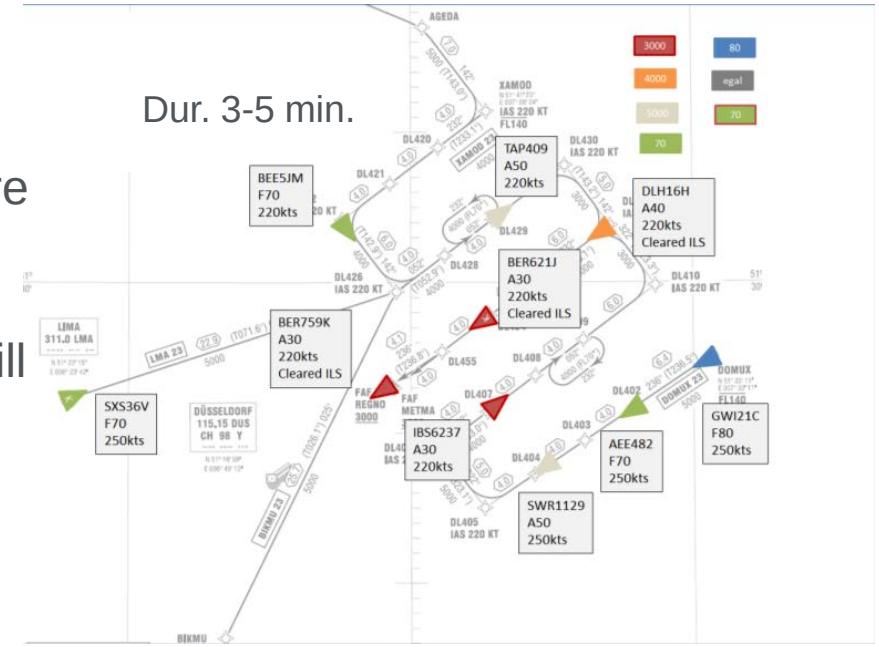
First Validation Results – Conflict Detection

$$FAR_{CD} = \frac{\sum \text{All Conflict Alerts} - \sum \text{Correct Alerts}}{\sum \text{All Conflict Alerts}}$$

$$DR_{CD} = \frac{\sum \text{Correct Conflict Alerts}}{\sum \text{Real Conflicts}}$$

- 20 short validation exercise scenarios are used.
- Module not yet validated.
- Validation of conflict detection module will be done in the near future

Dur. 3-5 min.



Conclusions

- Adherence to the developed validation methodology appears to be straightforward for ATM security prototype SACom.
- Achieved values and insights are still subject for further improvement.
- Presented first results encourage developing SACom further.
- Speech data analysing tools (speaker verification, speech recognition) need higher voice quality for evaluation of real air traffic voice communication.
- Female voices seem much more difficult to identify than male voices. Seems to be much more difficult to distinguish between stressful and non-stressful utterances.
- Focus also on integrated validations with other GAMMA prototypes.
- Security validation approach developed in GAMMA has potential to be adopted to be the sought-after construction kit for ATM security validation.

Outlook

- Validate SACom integrated with other prototypes/systems in partial integrated validations.
- Necessary research needed:
  - In stress detection area regarding voice patterns and its validation
  - In analyzing low quality voice signals similar to current ATC-pilot radio communication
  - In fostering the voice analysis while transmission is ongoing
  - In facing the big data issue
    → creating, managing, updating as well as continuously activating and deactivating a large number of speaker enrollments

www.gamma-project.eu

The research leading to this paper has received funding from the European Community‘s Seventh Framework Programme under grant agreement nr. 312382