DLRK
DEUTSCHER LUFT- UND RAUMFAHRTKONGRESS
2016

Security in ATM – A Validation Methodology for Security Prototypes

Tim H. Stelkens-Kobsch

DLRK, September 14, 2016

GAMMA
GLOBAL ATM SECURITY MANAGEMENT

SEVENTH FRAMEWORK PROGRAMME

DLR

Member of AT-One

PARTNER OF SESAR JOINT UNDERTAKING

Context – Security und Safety

Luftsicherheit
== Security („Angriffssicherheit“, Schutz des Objektes vor der Umgebung, d. h. Immunität, z.B. Vermeidung einer unberechtigten Nutzung)

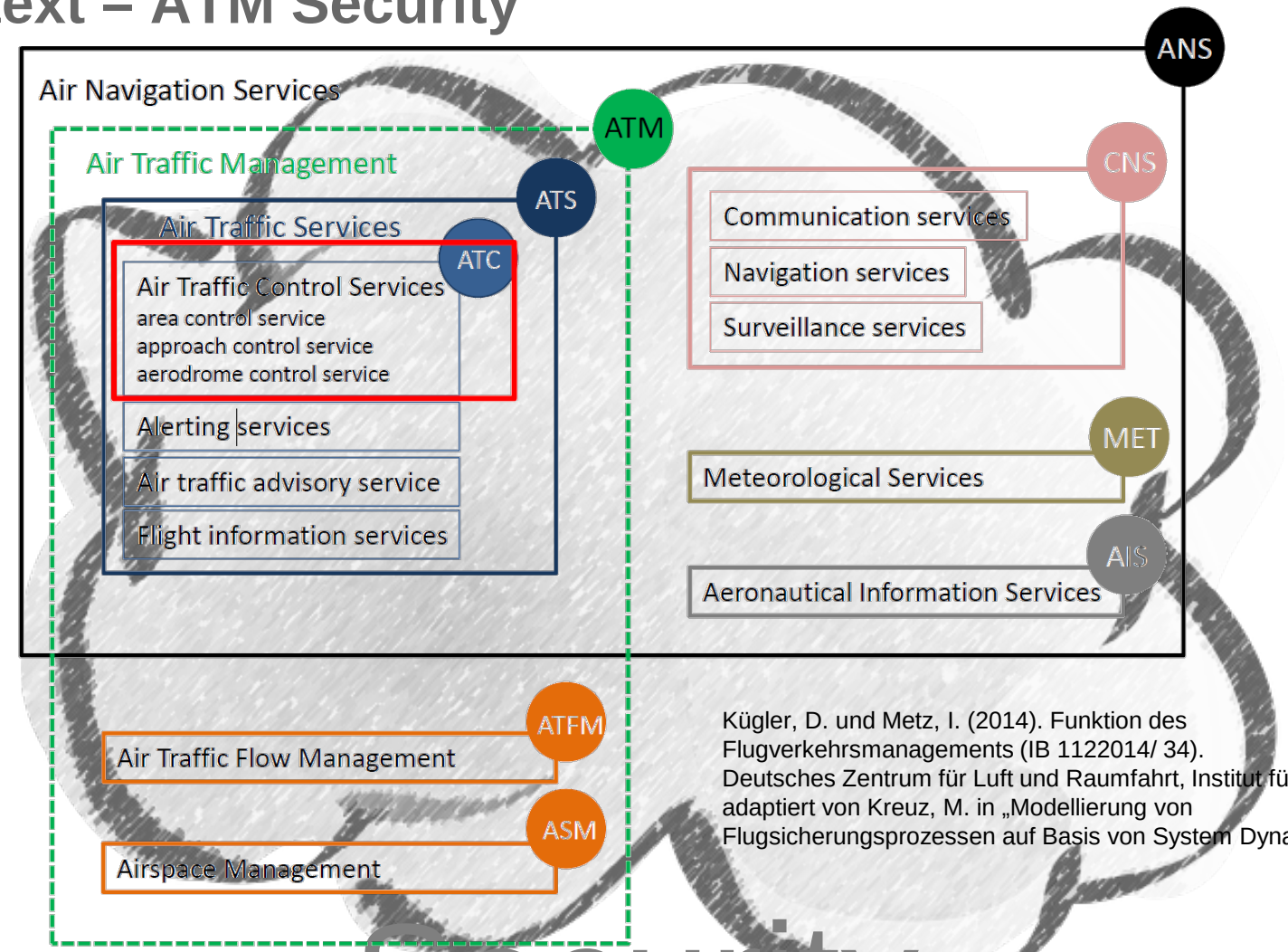
- ICAO: Safeguarding civil aviation against acts of unlawful interference (ICAO, 2011 , Annex 17, S. 1-2)

Funktionale Sicherheit, Luftverkehrssicherheit
== Safety („Betriebssicherheit“)

- ICAO: Safety is the state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management (ICAO 2013, Safety Management Manual (SMM), S.2-1)
- EUROCONTROL: Freedom from unacceptable risk (EUROCONTROL, 2001 , ESARR 4, S. 21)
- DFS: Die Erwartung, dass ein System - unter definierten Voraussetzungen - nicht in einen Zustand gelangt, in dem Menschenleben, menschliche Gesundheit, Umwelt oder Sachwerte gefährdet werden. Man nennt ein System sicher, wenn alle Risiken, die aufgrund von Bedrohungen vorhanden sind, durch geeignete Maßnahmen auf ein akzeptables Maß reduziert sind.

Abgrenzung gegenüber Katastrophenmanagement und Surveillance!
Abgrenzung gegenüber Safety!

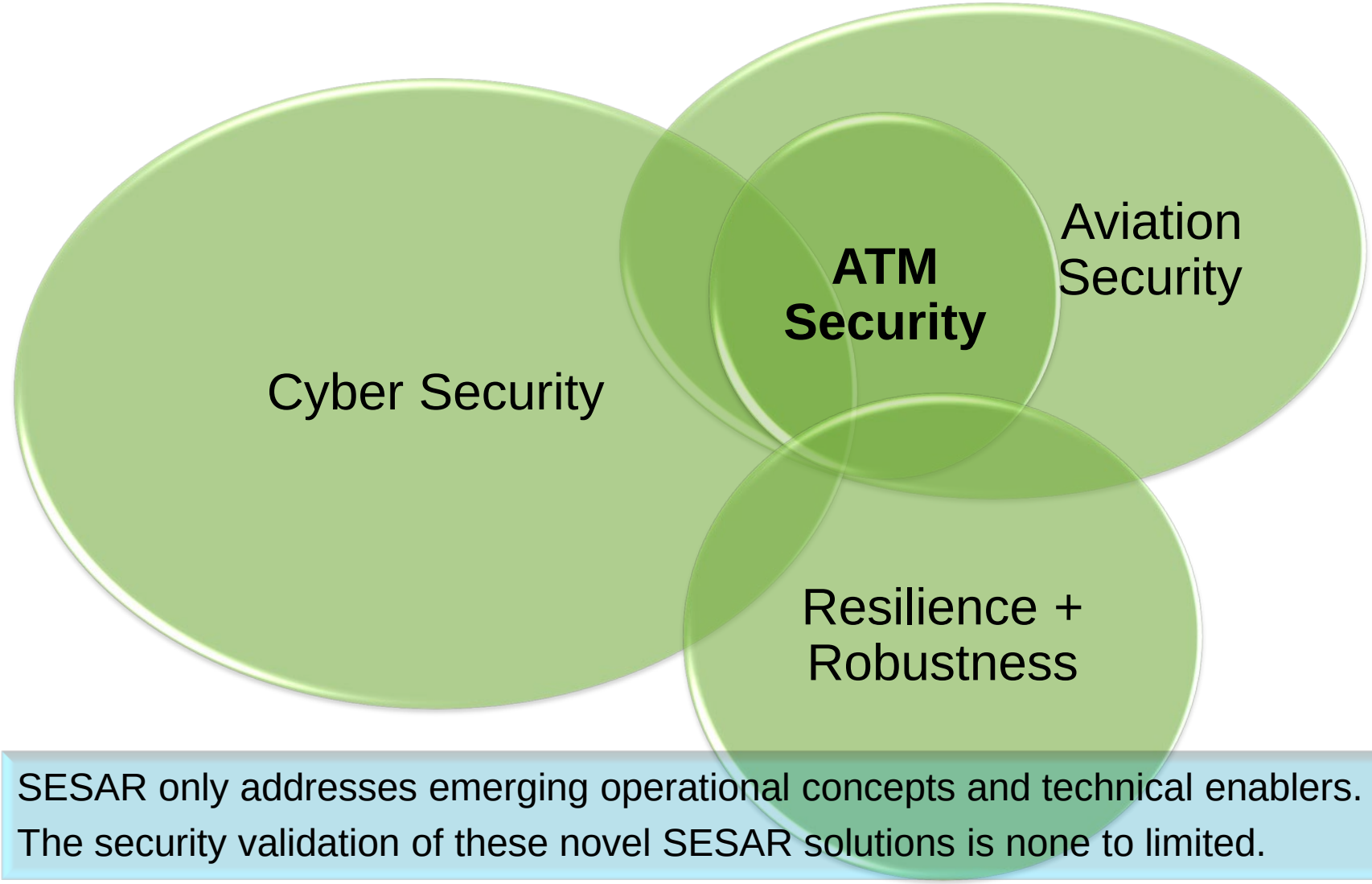
Context – ATM Security



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

Security

Context – ATM Security



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

FP7 Project: Global ATM Security Management (GAMMA)

Addresses the full set of security threats and vulnerabilities affecting the ATM system.

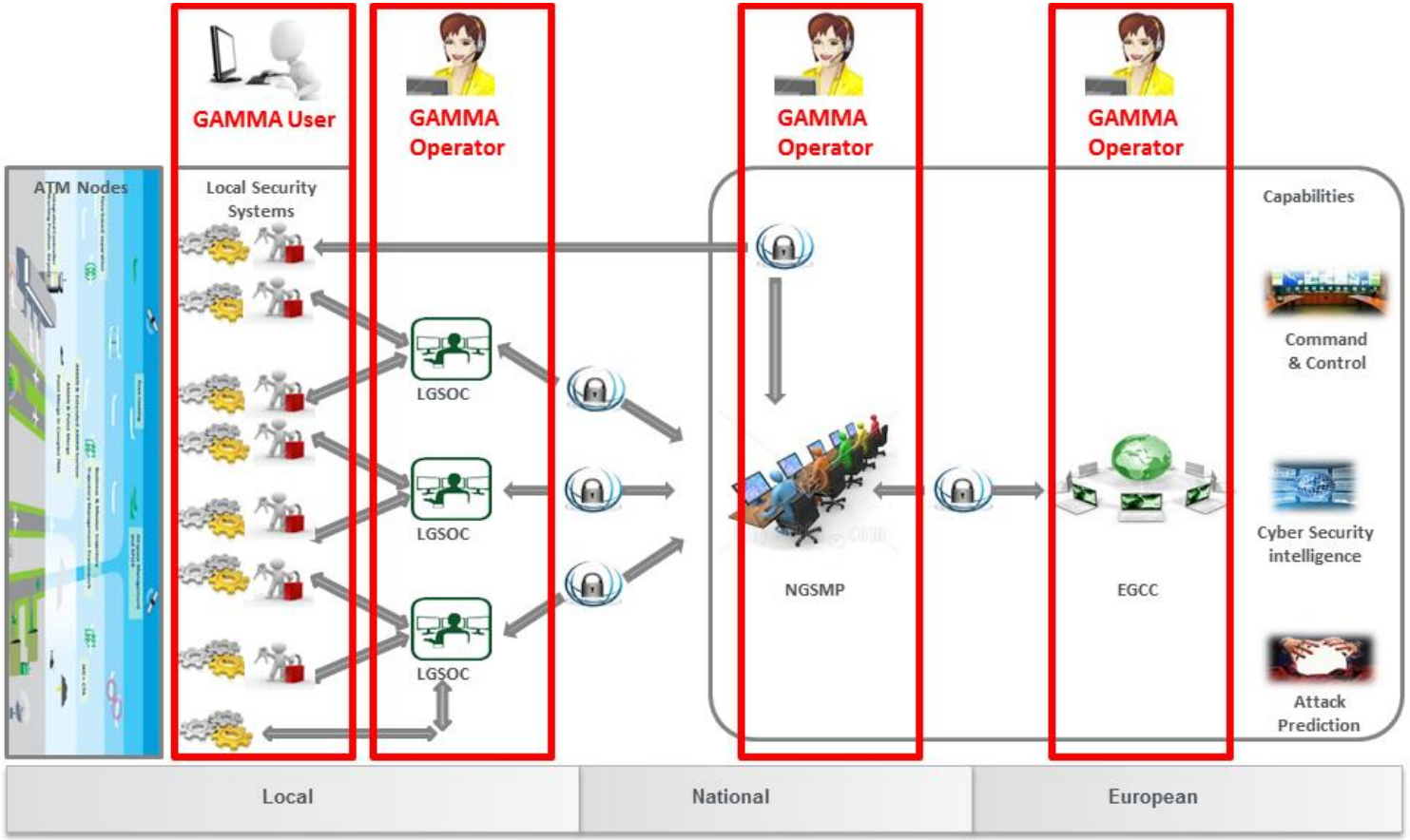
Identification of ATM Security Objectives:

- manage airspace security incidents
- detect illicit use of airspace
- detect abnormal situations of identified flights (deviation of flight trajectory, renegade aircraft, hijacking, etc.)
- etc...

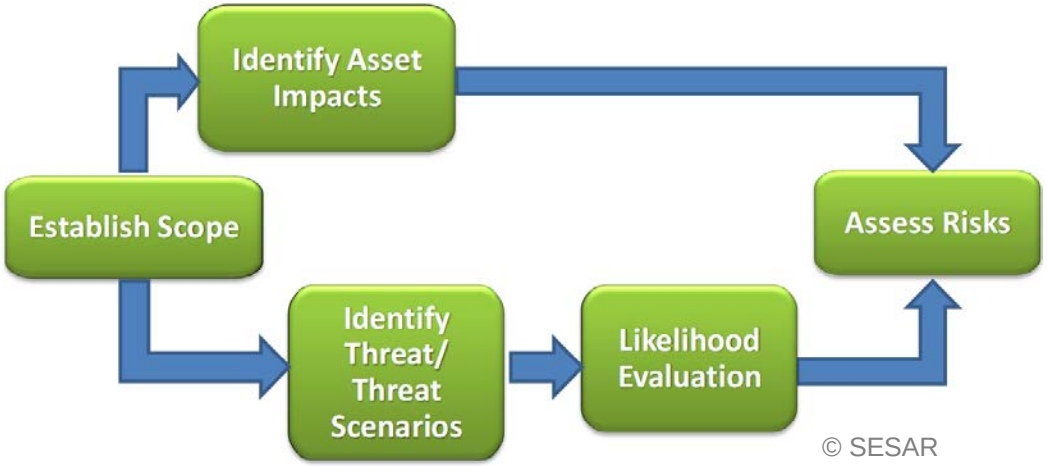
FP7 Project: Global ATM Security Management (GAMMA)

Two different human roles considered within GAMMA concept:

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



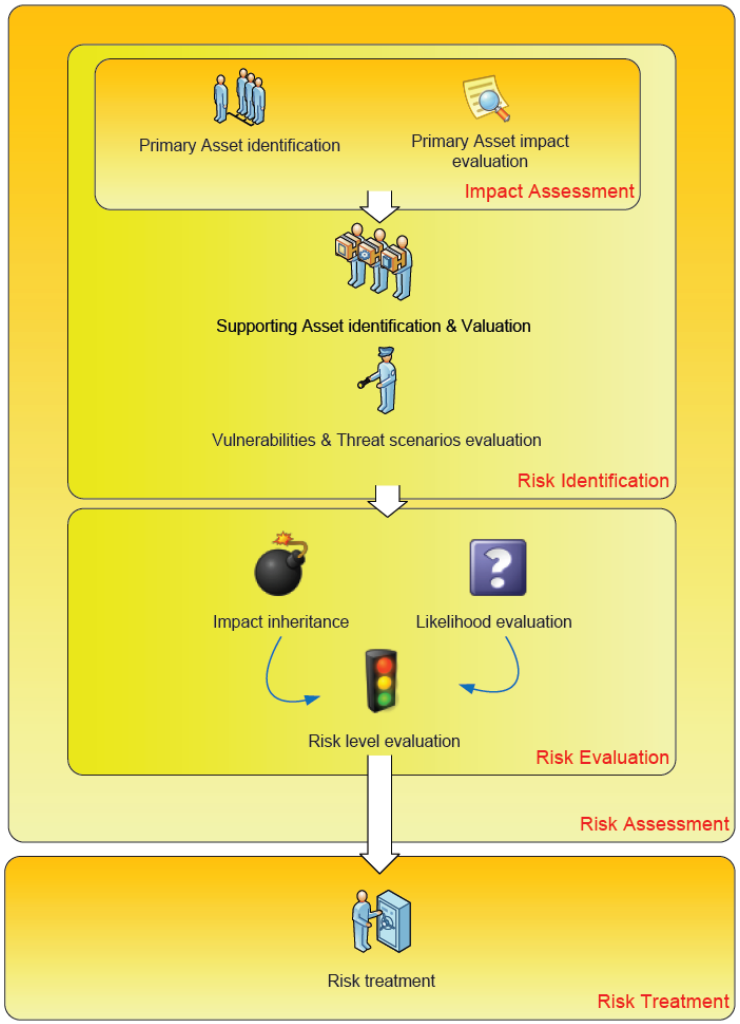
Security Risk Assessment Process (SESAR)



Further insight into the process:

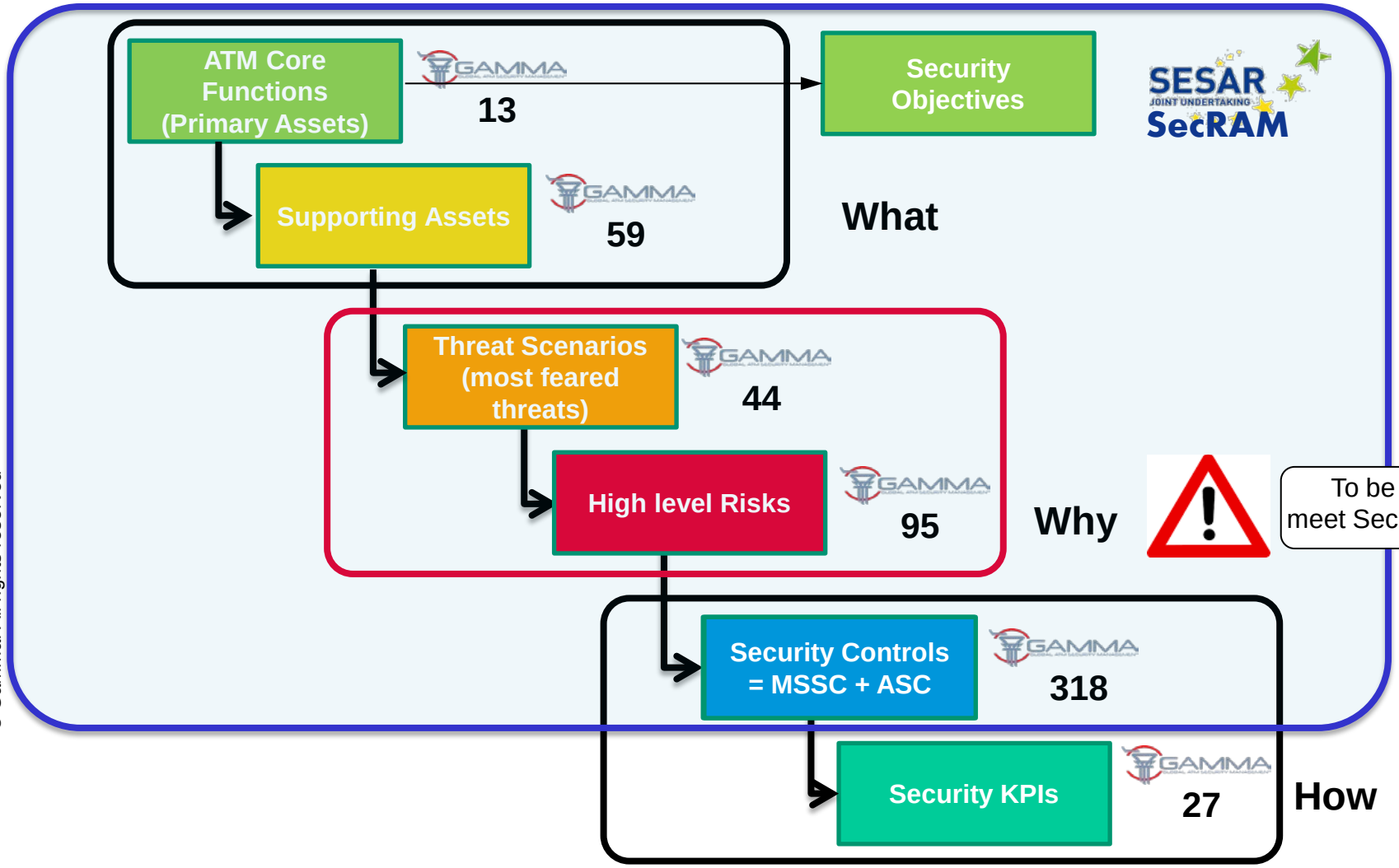
- Overall process of risk identification and evaluation
- After risk is assessed, it is possible to identify a set of security requirements
- Security requirements ensure that consequences of an attack are known and managed
- Allow targeted asset to recover to normal operation in reasonable time

Methodology: SecRAM (SESAR)



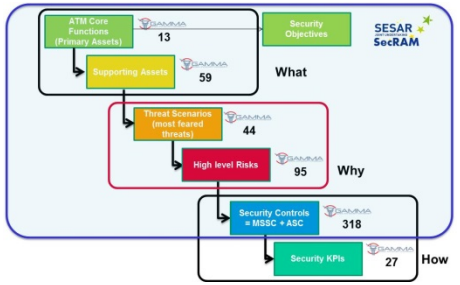
© SESAR

Security Risk Assessment and Treatment in GAMMA



Security Risk Assessment and Treatment in GAMMA

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



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

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

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**

What are we trying to protect?

Air Ground Communication in Air Traffic Control

- Part of international aeronautical telecommunication service
- Aeronautical mobile service
- Differentiation between voice and data link communications (CPDLC)

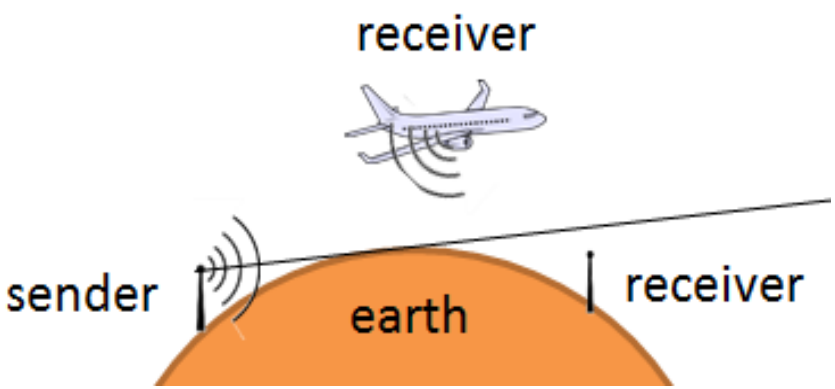
Air Ground Communication from technical point of view

- 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

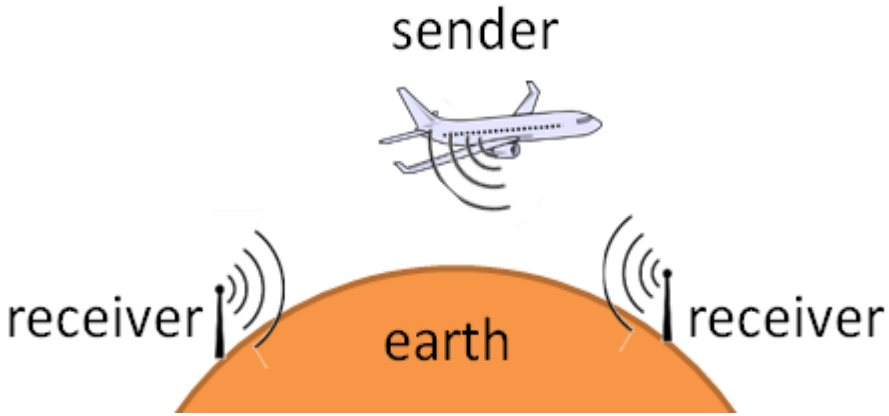
Voice communication is still the basic and most important communication method within aeronautical mobile service

Vulnerabilities of ATC Voice Communications

- Radio transmitter equipment generally available
- Line-of-sight dependency



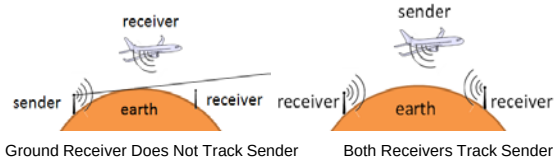
Ground Receiver Does Not Track Sender



Both Receivers Track Sender

© Gamma. All rights reserved

Vulnerabilities of ATC Voice Communications

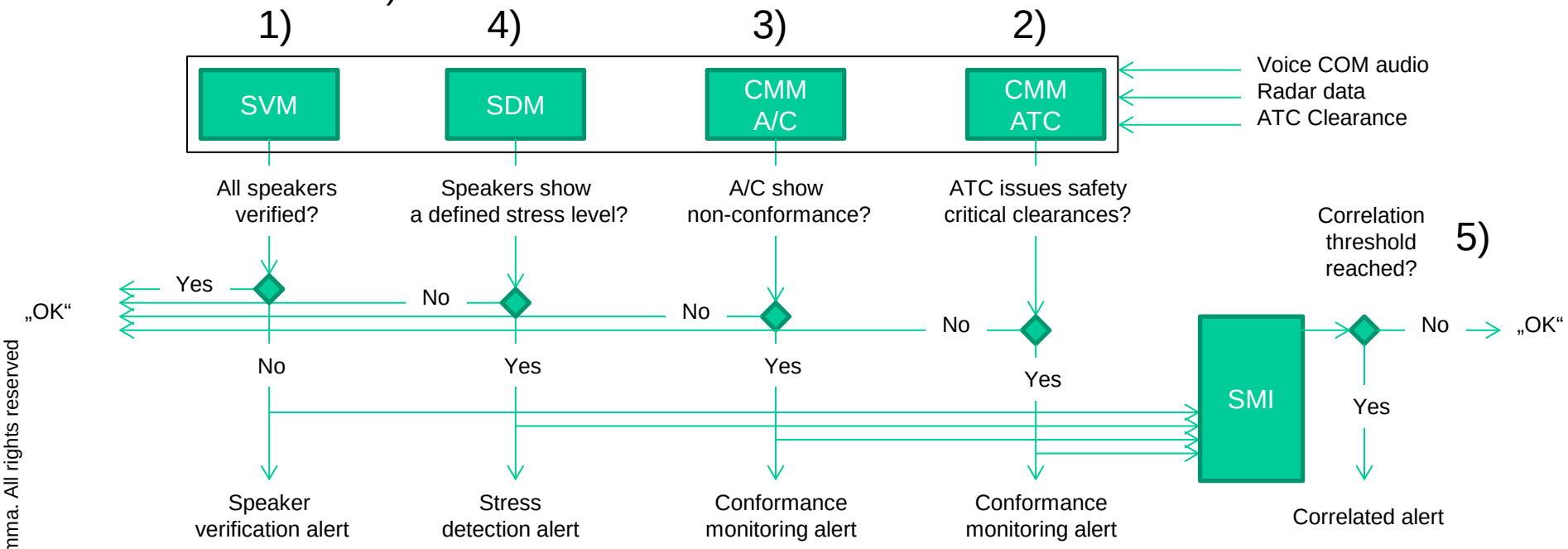


- Radio transmitter equipment generally available
- Line-of-sight dependency
- Signal power decreases with distance
  (nearby stations may block out stations far away)
- Analogue distribution of communication
- Limited number of frequency bands
- Open to masquerading intruders
- No protection against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

Proposed Prototype to Secure ATC Communications

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)

Setup of the Validation Exercises

Needed steps to validate SACom

- Briefing of test person,

- Speaker verification enrollment,

- Simulator training,

- Short simulations,

Simulation

- SACom briefing,

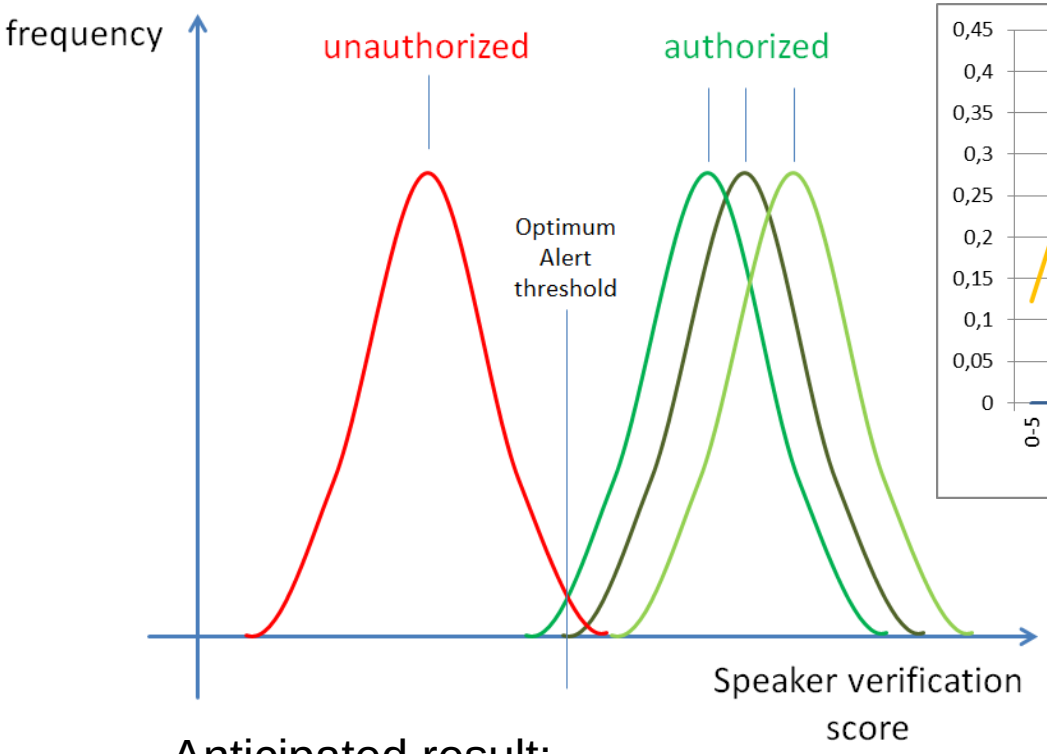
- SACom training

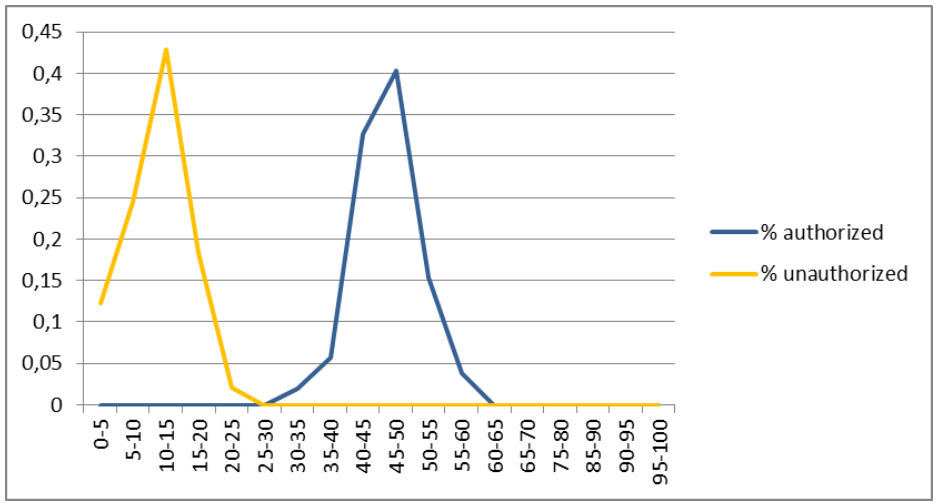
- Long simulation

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]

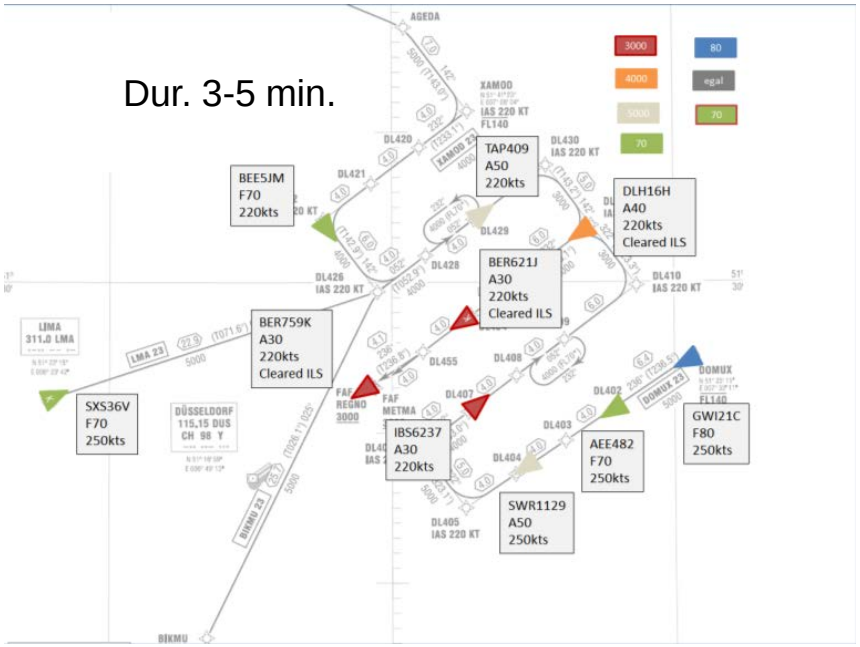
First Validation Results – Conformance Monitoring

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

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

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

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



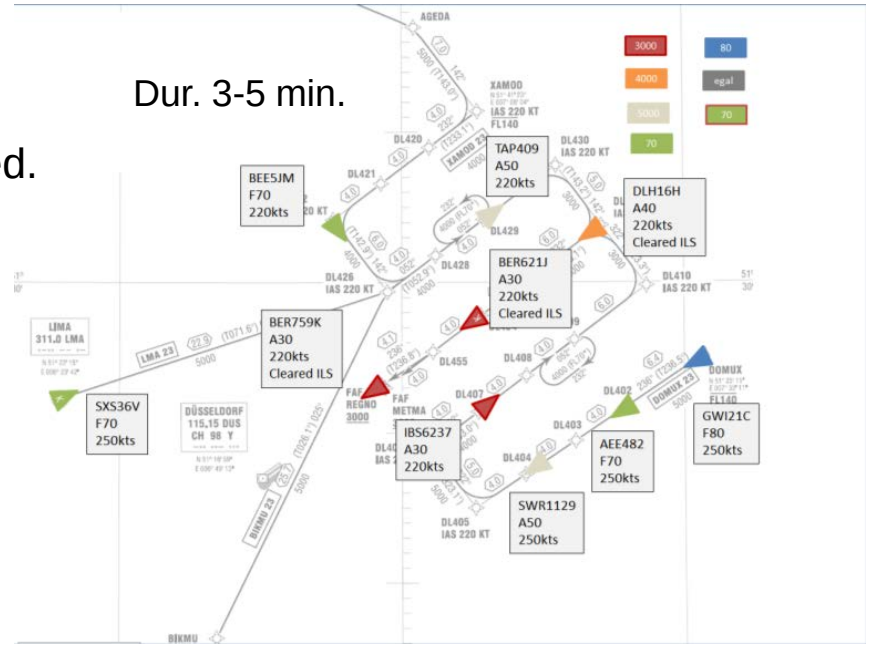
First Validation Results – Conflict Detection

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

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

- 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 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.

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