NEWSLETTER | Issue n°4 | May 2017

CONTENTS

EDITORIAL

In this edition of the GAMMA Newsletter we continue our review of the seven prototypes developed within the project with an article focusing specifically on the Information Security System (ISS) realized by Leonardo.

ISS adds a security layer and mechanism to protect data exchange using new airport data link services such as AeroMACS and ground VoIP ATN communications to guarantee the required level of data confidentiality, integrity and availability. The ISS prototype therefore includes security solutions for service authentication, allowing the monitoring and identification of suspicious activities and possible countermeasure proposals for security threats mitigation.

The development of prototypes within GAMMA is part of a broader cycle which started with the analysis and assessment of ATM vulnerabilities and continued with the development of a new vision for managing ATM security in Europe, including a description of the associated architectural framework. This process has now led to the final stage which involves the validation of the developments realized in GAMMA. In this phase of the project separate GAMMA prototypes have been validated in a stand-alone configuration in preparation for the validation of the entire GAMMA concept, performed through geo-distributed validation exercises involving several prototypes.

This edition of the Newsletter includes an article providing a comprehensive view of the separate validation activities performed on each of the seven prototypes. The results of these activities represent an important baseline pointing towards the final goal of validating the GAMMA concept through integrated scenarios involving combinations of prototypes. These integrated geo-distributed exercises represent the final stage of the project and will be associated with a range of workshops with the external community of experts and stakeholders.

Stay tuned for this final and most exciting lap of the GAMMA project!

by Giuliano D' Auria,
GAMMA Project Coordinator

GAMMA IN BRIEF

GRANT NUMBER:	312382
PROJECT COORDINATOR:	LEONARDO SpA
CONTACT PERSON:	Giuliano D'Auria
	giuliano.dauria@leonardocompany.com
PROJECT WEBSITE:	www. gamma-project.eu
DURATION:	48 months
BUDGET:	14.8 € Million

PAPERS

The following papers have been prepared by GAMMA partners and presented in conferences. Title and authors of these papers are reported below, while the complete documents are available for download at: www.gamma-project.eu

Title: The Social Acceptance of the Passivation of Misused Aircraft
Author: Ana P. G. Martins Institute of Flight Guidance Deutsches Zentrum für Luft- und Raumfahrt e.V. Braunschweig, Germany

Title: Towards a More Secure ATC Voice Communications System
Authors: Tim H. Stelkens-Kobsch, Dr. Andreas Hasselberg, Dr. Thorsten ühlhausen, Dr. Nils Carstengerdes, Michael Finke and Constantijn Neeteson, German Aerospace Center (DLR), Braunschweig, Germany

Title: Security Situation Management – Developing a concept of operations and threat prediction capability
Authors: Denis Kolev, Rinicom, Lancaster (UK), Rainer Koelle, Lancaster University, Lancaster (UK), Rosa Ana Casar Rodriguez, Isdefe, Madrid (ES), Patrizia Montefusco, Leonardo, Napels (IT)

ARTICLES

GAMMA Information Security System

Author: Leonardo

Prototype description and capabilities

The Information Security System (ISS) provides a solution to protect data communication at the Airport and for PENS in ATN communication systems that are using new datalink communication services with 4D capabilities (CPDLC and ADS-C) such as AeroMACS and VoIP ATN communication services for the Ground -Ground PENS segment.
The ISS prototype is the Leonardo response to the security assessment carried out at the start of the GAMMA project which highlighted the need to introduce a range of additional security controls:
- The uses of AeroMACS Network End point Authentication/Authorization/Accounting mechanisms to increase the network security of End point systems and applications in the Airport site;
- Increase the security for A/G DL communications for the operation on the Airport site;
- Security mechanisms to detect and to mitigate security threats.
The ISS prototype therefore includes solutions for communication and service authentication that demonstrate the capability of threat mitigation for the vulnerabilities identified during the assessment phase of GAMMA, guaranteeing the required level of confidentiality, integrity and availability.

ISS prototype System components

The ISS prototype includes the following system components:
- The AeroMACS Networks in the Airport site;
- A/G DL applications for A/C management of ATS procedures;
- EUROCAE Ground VoIP communication;
- ISS Local Network Management System (NMS);
- ISS IPS (Intrusion Prevention System).

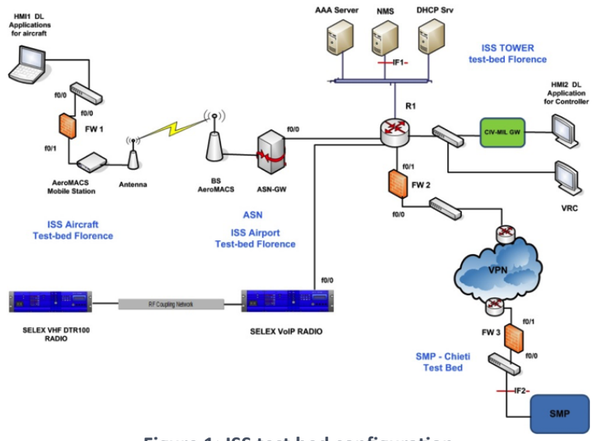

Figure 1: ISS test bed configuration

More specifically the AeroMACS Networks in the Airport site includes the following elements:

AeroMACS Base Station (BS)
The AeroMACS Base Station (BS) is a logical entity complying with the AeroMACS specifications that host one or more access functions. The BS AeroMACS is responsible to receive, amplify and retransmit signals from the airborne mobile station (MS). The main task of a Base Station is to provide radio coverage over the airport area to the airborne subscriber.

AeroMACS Mobile Station (MS)
The AeroMACS Mobile Station (MS) provides connectivity between the aircraft and a base station (BS).

AeroMACS Access Service Network GW
The AeroMACS ASN-GW assists mobility, security data control and handles the IP forwarding. The GW data plane feature includes the mapping of the radio bearer to the IP network, packet inspection, tunneling, admission control, policing, QoS and data forwarding capability.

AAA Server/Proxy
The AAA proxy or server provides policy and Admission Control based on user subscription profiles. The AAA server functionalities set include authorization, authentication, accounting (AAA), context management, profile management and service flow authorization.

ISS – Nework Management System (NMS)
The ISS Network Management System (NMS) oversees AeroMACS networking environments to guarantee high availability of monitoring ISS network elements to avoid degraded service.
The NMS functionalities include network configuration and monitoring, fault management, communication management and reporting problems.

AeroMACS Air interface encryption functionalities

The Air interface encryption functionalities provided by the ISS AeroMACS prototype guarantee the adequate level of confidentiality and integrity of A/G communications. These AeroMACS functions involve the BS, MS and AAA AeroMACS network components. The messages between these components are exchanged to enable the End to End encrypted communications:

- The Authenticator (in ASN/ASN GW) initiates EAP authentication procedure with MS.
- The BS relays the EAP Request/ Identity to the MS and the MS responds with an EAP Response/ Identity message providing Identity.
- The Authenticator (AAA server) analyses the Identity provided by the MS (Mobile Station). Depending on the domain the MS could be locally authenticated in cases where the MS is in its Home Network.

These main process and protocols between the AeroMACS components are exchanged to enable the End to End encrypted communications:

- The EAP authentication process (tunnelling EAP authentication method) is performed between the MS and the Authentication server via the Authenticator in ASN/ASN-GW. BS provides “relay” of EAP payload from PKMv2 EAP-Transfer messages to Authentication Relay EAP Transfer and vice versa. The Authenticator in ASN/ASN-GW acts in pass through mode and forwards the EAP messages received as a payload from the BS in EAP Authentication request messages to the AAA server using RADIUS Access-Request messages and vice versa.
- PKMv2 3-way handshake (SA-TEK-Challenge/Request/Response exchange) is conducted between BS and MS to verify the Authorization Key (AK) to be used and to establish the Security Association(s) pre-provisioned for the MS.

ISS A/G CPDLC and ADS-C communications over AeroMACS datalink at the airport site

The A/G CPDLC and ADS-C communications on the ISS prototype includes these main elements that allow aircraft traffic management in the airport for aircraft take-off procedures.

ISS HMI application for Aircraft
HMI Client Application for i4D A/G Data link communication (CPDLC and ADS-C) is an application that simulates pseudo cockpit messages and services over AeroMACS channel communication.

ISS HMI application for Controller
HMI Client Application for i4D A/G Datalink communication (CPDLC and ADS-C) is an application that simulates pseudo working position messages and services over the AeroMACS channel communication.

I4D messages for A/G datalink communications
This paragraph includes a list of CPDLC and ADS-C messages that are exchanged between the pilot HMI and the controller HMI. The ISS prototype includes the following Air Traffic Services (ATS) at the airport’s surface:
- DLIC (DataLink Initiation);
- ACM (ATC Communication Management)
- CRD (Clearance Request and Delivery)
- AMC (ATC Microphone Check)
- 4D-TRAD (4-Dimensional Trajectory Data Link)

The ATS messages are exchanged over the AeroMACS communication channel that includes E2E air encryption mechanisms that guarantee authentication, integrity and data confidentiality.

ISS Security mechanisms to detect and to mitigate security threats

The ISS probe module unit examines network traffic and performs traffic analysis. The DoS policies use

traffic analysis by keeping track of the type and quantity of packets, as well as their source and destination addresses. This information offers suggestions on how the Security Network Manager secures the ISS network against specific threat contents.
The IPS functionalities allow executing these main activities:

- Threats monitoring
- Policy configurations
- Security event reporting

During the network security attacks, the network manager receives data and events related to the security events detected. The ISS sends the security messages to the ISS NMS (Network Management System) and the ISS IPS (Intrusion Prevention System).

The ISS NMS HMI captures and shows the security events “IPS anomaly” detected” (see Figure 2 and Figure 3).

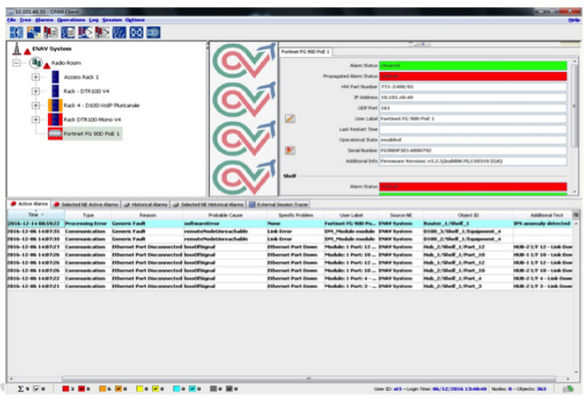

Figure 2: ISS NMS threats event

The Local Network Manager receives the alert of “Anomaly event” and is able to verify the active threats in collaboration with the Security Network Manager.

Figure 3: ISS NMS anomaly event detail

The ISS security events are visible by the Security Network Manager on the ISS IPS HMI (Figure 4) and ISS IPS report (Figure 5).

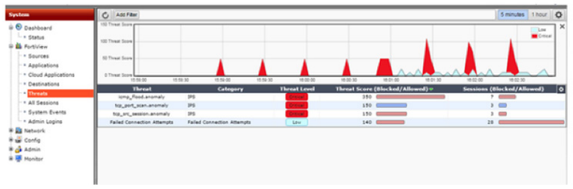

Figure 4: IPS Security events monitoring

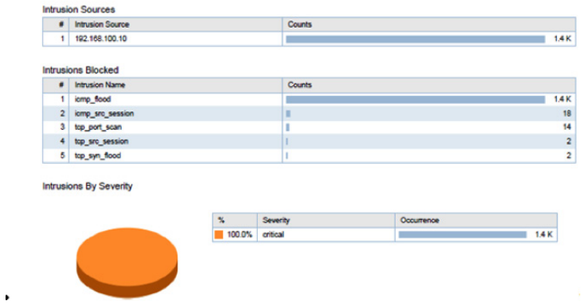

Figure 5 - ISS IPS report

The ISS IPS has the capability to configure an appropriate policy to manage by default the threat scenarios; these policies stored on the IPS can be changed or selected at run time by the Local ISS network Manager to face specific threats or to apply a specify security policy. The figure below provides a screenshot of the ISS policy configuration.

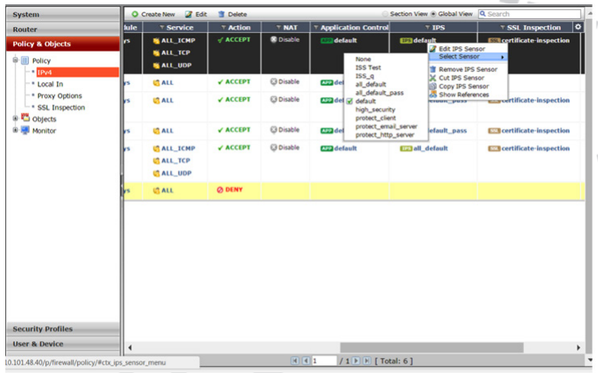

Figure 6 - ISS IPS policy configuration

The ISS IPS allows also to configure new policies with predefined “threshold values” that are used by the “Network Security Manager” to mitigate and prevent possible attacks.

The ISS solution includes the appropriate integration with the Security Management Platform (SMP) prototype to identify and monitor suspect activities and activates the required countermeasures to minimize or avoid the side attack effect on the communication and ATN service.

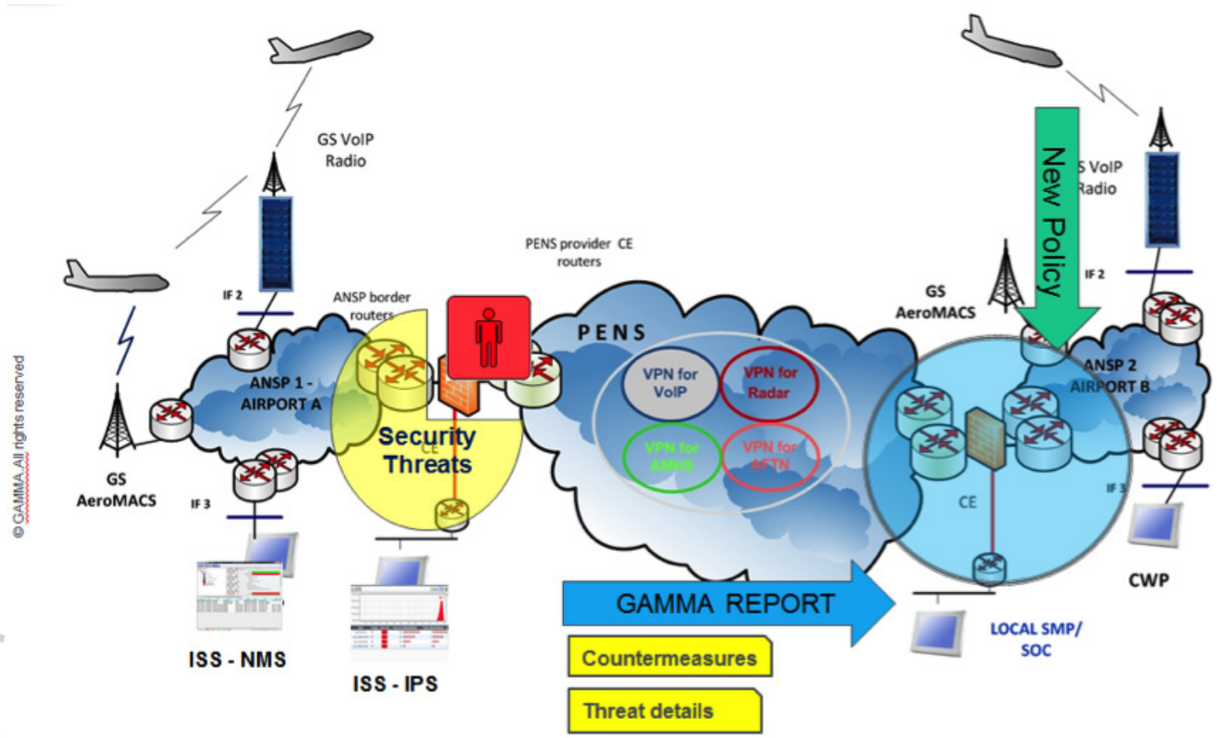

Figure 7 – Security countermeasures and Policy update

The ISS prototype should be seen as part of a broader vision for enlarging the scope for cooperative management by providing situational awareness over the diverse systems which form the ATM system of system.

For this purpose the ISS prototype is able to configure and update security policy configuration, shared with the SMP at National and European level (i.e. security threats details and countermeasures), which enables prevention and mitigates distributed security attacks that could impact on the ATM system and operation.

ISS Prototype and Standard References

- ICAO ATN-OSI 9880 and ATN-IPS 9896 standards;
- EUROCAE ED AeroMACS communication;
- EUROCAE VoIP Standards - ED-136, ED-137 and ED 138 normative;
- PKI recommendation from ICAO WG-I and WG-S.

ARTICLES

GAMMA Prototypes and Validations

Author: DLR

The GAMMA project was started with the ambitious goals

- to deliver and to validate a concept for a holistic and comprehensive ATM security management system and
- to develop and validate seven different ATM security prototypes on their own and interconnected with the others.

GAMMA is now drawing to a close and it is time to culminate the work in the final validations. These validation exercises are two fold, starting with a first series of validations focused on the prototypes in standalone mode followed by several partially and fully integrated exercises. This article gives an introduction to the seven prototypes designed and developed within GAMMA and describes the first series of validations.
The different prototypes designed and developed during the project duration are introduced hereafter.

Information Exchange Gateway (IEG)

The IEG enhances the traditional approach with a very strong mechanism of protection against most sophisticated attacks. IEG is capable of detecting new kinds of offensive contents and intercepting them by deciphering, analysing and confronting the messages with access control and filtering policies. Thus, it will serve to protect web services from XML-based threats. The IEG will be placed in a Demilitarized Zone (DMZ), facing the web service provider. It scans ingoing-outgoing XML traffic. All requests coming from the consumer addressing the provider will be inspected by the IEG before they reach the provider. In case the requested content is not considered as malicious, it will reach the target. Otherwise, the IEG will drop the request.

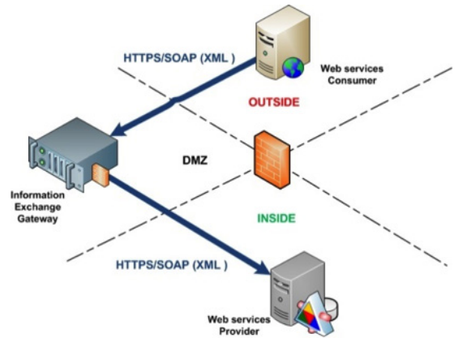

Figure 1: Information Exchange Gateway Positioning

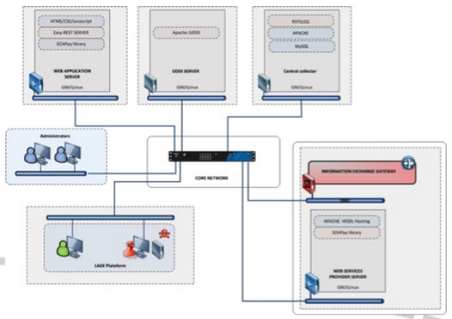

Figure 2: IEG validation platform

SATCOM Security (SATCOM)

The goal of the SATCOM security prototype is to detect and to offer countermeasures as fast as possible when a threat is targeting assets under concern. This holds true from the technical and/or operational point of view. The SATCOM security prototype is a client-server software solution designed to secure the management and control the communication in satellite networks. The impact of the threats targeting SATCOM assets is reduced by the coordinated functions of a set of modules integrated in the software of the prototype.

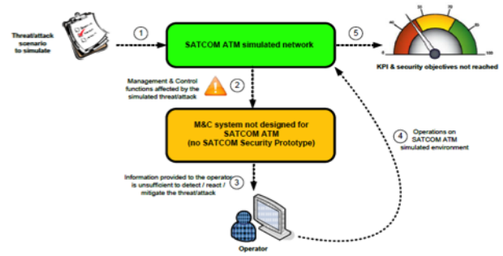

Figure 3: Without SATCOM security prototype

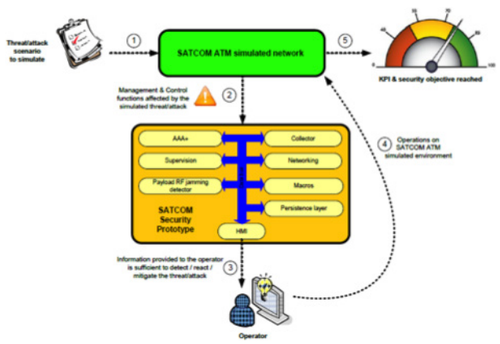

Figure 4: With SATCOM security prototype

Information Security System (ISS)

The ISS is composed of multiple systems integrated in the operational environment for Air-Ground Voice over IP (VoIP) ATC communications and data communication carried by the AeroMACS system. The ISS provides protected data communication on the airport side and for the Air-Ground (CPDLC and ADS-C) as well as Ground-Ground communications (PENS). The ISS also includes capabilities for communication and service authentication which enhances the required level of confidentiality, integrity and availability by mitigation of the threats. The ISS assists in identifying and monitoring suspicious activities and activates required countermeasures to minimize or avoid side effects on the communication and the air traffic network service.

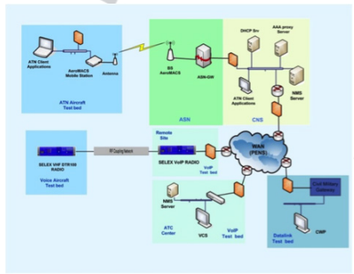

Figure 5: Information Security System

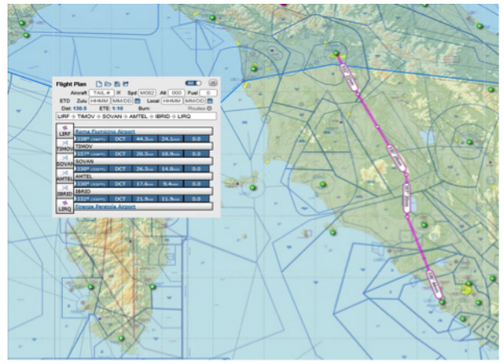

Figure 6: Aircraft in Florence Airport with a scheduled flight Plan to Rome

Integrated Modular Communication (IMC)

The IMC disseminates security alerts and may receive instructions for switching to different configuration depending on the security situation. These may be instructions to reduce functionality in response to an attack.

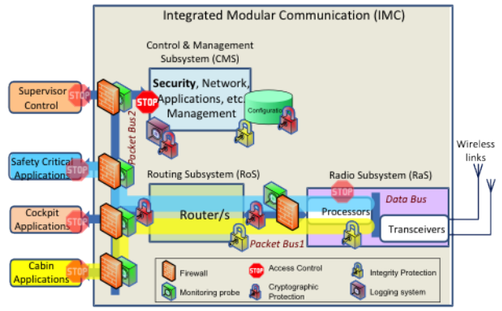

Figure 7: The IMC architecture with security controls

Secure ATC Communication (SACom)

The SACom Prototype in consists of three detector modules which perform speaker verification, stress detection and conformance monitoring. The different indicators are correlated and disseminated. The speaker verification module screens the voice communication and confirms authorization of speakers. The stress detection module also screens the voice communication and identifies abnormal voice patterns (e.g. induced by stress), which can be an indicator for unlawful actions. The conformance monitoring module uses electronically available clearances and surveillance data as input and checks if the aircraft flight trajectories correspond to given ATC

instructions. Finally the correlation indicator module correlates all indications and forwards an overall threat indicator to the dedicated receiver.

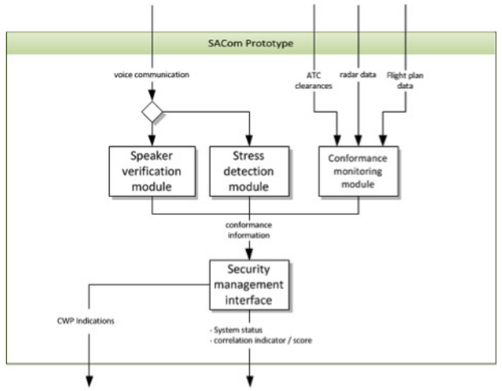

Figure 8: SACom Prototype architecture

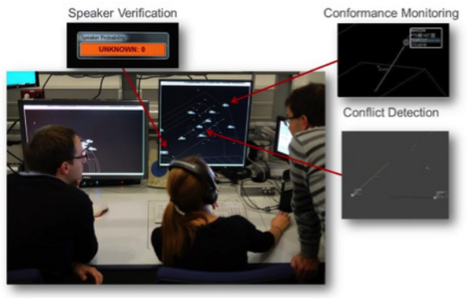

Figure 9: SACom Prototype

Secure GNSS Communication

The Secure GNSS prototype is able to detect GNSS jamming and spoofing. The system is composed of several sensors deployed on an airport and linked with a server easy to reach for ATC operators. Secure GNSS prototype provides an alert in case of interference detection with the GNSS signal to support an overall security threat evaluation. After receiving the alert about a threat from the system, ATC shall inform aircraft in approach to cancel GNSS procedures and information shall be send to national and European authorities.

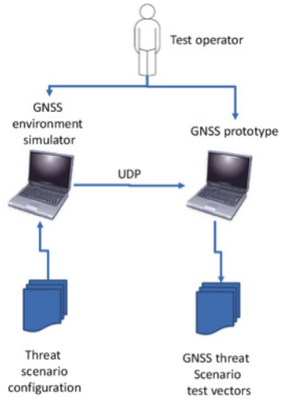

Figure 10: GNSS prototype overview

Security Management Platform (SMP)

The scope of the SMP is to provide Security Operators operating in the different ATM environments with a common overview on the status of ATM systems (situation awareness). The SMP collects information from event detectors connected to the different ATM systems, monitors and reports security events and incidents, and disseminates security information through a multi-level infrastructure that foresees instances of SMP at national level and a central SMP at European level.

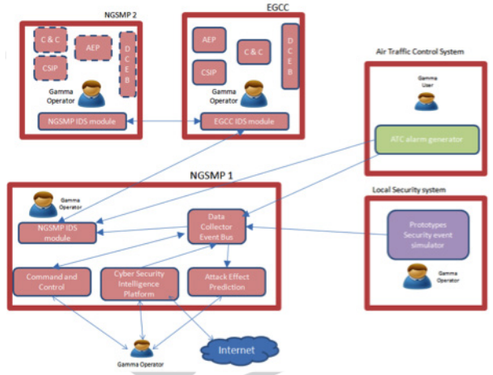

Figure 11: SMP validation exercise lay-out

Validation of the Prototypes

Information Exchange Gateway (IEG)

The validation exercise was designed to involve one test person and one cybersecurity engineer for the duration of one day. The test person took the position of the end-user and did not need to have a huge experience in air traffic control. The test person had to be familiar with IT solution and sensitized with Cybersecurity aspects. The cybersecurity engineer involved in the exercise did not need to have experience in air traffic control. The exercise has been conducted utilising the platform designed for the validation of the IEG. The validations successfully met all the acceptance criteria and triggered all the KPIs identified for the evaluation of the IEG performance. The IEG single prototype validation has demonstrated the ability of the IEG to cope with the threats that were identified in the Validation Plan.

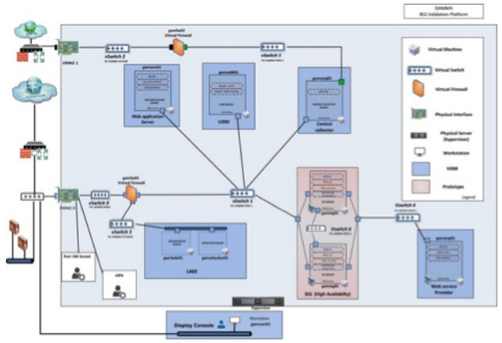

Figure 12: IEG validation platform

SATCOM Security (SATCOM)

The SATCOM validation exercises involved a test leader, a test person and observers. The duration of one exercise was not more than two days. The validation environment used can be divided into two parts; the first one to simulate the whole environment needed to create the most realistic environment for the SATCOM security prototype and the second part (containing the SATCOM security prototype and the HMI client), which is needed to receive the alerts and perform the required actions by the SATCOM operator. The main result of the validation exercise show that without using the SATCOM, the number of false alarms produced were higher than the number of threat inductions (166,7%).

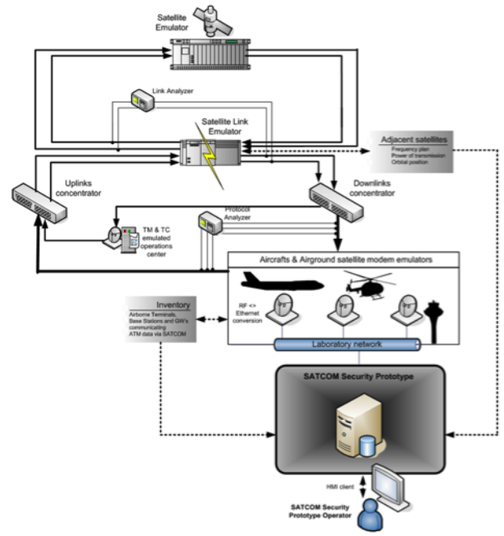

Figure 13: SATCOM validation platform

Information Security System (ISS)

The validation exercise of the ISS intends to involve the prototype in one or more operative scenarios with duration of about 60 minutes. Different scenarios have been executed and described in the validation result documentation. A test person, who takes the position of a Controller, Pilot and Security expert, was joining the validation exercises while an ATM domain expert and Network Manager Experts supervised the exercises. The security functionalities developed for the ISS prototype in the GAMMA project and tested through the stand-alone validation have achieved the required security objectives.
The ISS stand-alone validation exercise demonstrated these main results:

1. The test demonstrated that the vulnerability attacks have been identified and automatically blocked by the ISS IPS system using ISS Security Policies configuration.

2. The Network Security Manager was able to set and apply the new policies with the specific threshold value required to mitigate the security threats.

3. The vulnerability attacks performed on the ISS ground system didn't produce A/G communication loss.

Figure 14: ISS threats sessions detected and mitigated

Integrated Modular Communication (IMC)

The validation exercises of IMC have been performed on a windows PC. The IMC, IMC Traffic Generator (data traffic producer) and Security Management Platform emulator are all software modules and have been running on the same PC without the need for external communication links. The validation exercises have been conducted by an IMC tester. The tester initiated the running of various software tests by using the IMC Traffic Generator VEBB as well as performed some IMC administrator roles. During the validation exercise, three validation scenarios have been simulated following a time line. Namely an online attack to IMC through on-board systems, an online attack to IMC through off-board systems and an abuse of administrator privilege has been conducted. Customers require security that ensures the integrity of IMC by separating the different domains. The conducted tests validated the separation between the cabin and the safety domains, by showing that attempts to communicate between the domains are blocked.

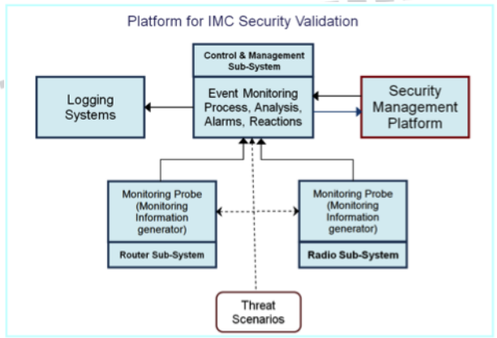

Figure 15: IMC Platform Configuration for Validation Purposes

Secure ATC Communication (SACom)

The validation exercise was designed to involve one test person for the duration of one day, while the supporting team to drive the simulations consisted of 5 persons. Due to the fact that security tests are typically just possible to be conducted if they happen with no advance warniong, the exercise was repeated multiple times, but with different test persons to avoid training effects. The test persons, who took the role of an ATCO, were recruited from the German Air Navigation Service Provider DFS.

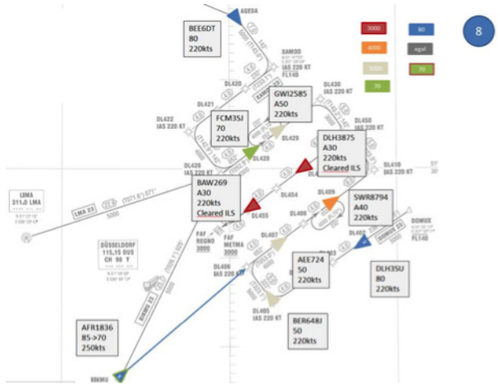

Figure 16: Briefing sketch for one short-time simulation

The validation exercise consisted of a briefing, the enrolment of the speakers (to store the voice characteristics in a database), the validation of the enrolment, a training session to familiarise with the simulator, a validation phase with 20 short-time simulation scenarios containing specifically designed conflicts, a debriefing and a second validation phase with a simulated intrusion of an unauthorised attacker to the voice communication. The SACom validation campaign was performed within the ATMOS facility in Braunschweig. The activities showed, that match values of 90% or more are possible and where occasionally achieved for speaker verification by automatic voice analysis. Furthermore the conformance monitoring module also delivered very promising results. Unfortunately this is not true for the stress detection module which again proves the fact that detection of stress is still in its infancy. Nevertheless the invited ATCOs confirmed the added value the developed prototype would when experiencing security breaches like the ones which were considered.

Secure GNSS Communication

The goal of the Secure GNSS Monitoring System (GMS) prototype is to detect GNSS interference or spoofing and to provide information to the SMP to support an overall security threat evaluation.ATC is then informed by the GAMMA system and subsequently informs aircraft in approach to cancel GNSS procedures. This information will then be sent to national and European authorities.

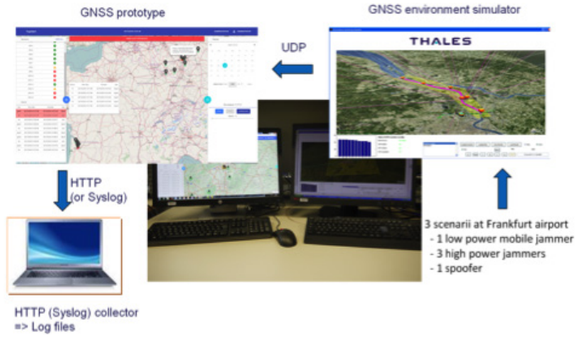

Figure 17: Single GMS prototype validation

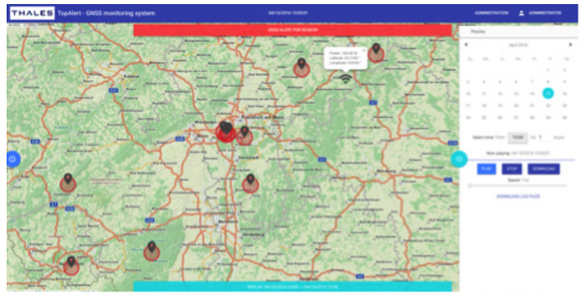

Figure 18: GMS prototype view

Within the validation exercise one test person was involved to start and stop the simulation. This person did not need any kind of GNSS experience. Each validation exercise was planned for duration of one day and consisted of a briefing, the configuration of the GMS prototype and the conduction of the scenarios. The prototype showed its qualification to deliver the expected results.

Security Management Platform (SMP)

Participants of the SMP validation exercise noticed the good visualising performance of the alarm on the Command & Control HMI. The offered function to obtain alarms due to a particular correlation of security events was seen favourable and the participants of the validation exercises noticed a good performance for dissemination of security information when alarm information needed to be transferred from a National GAMMA SMP (NGSMP) to European GAMMA Coordination Center (EGCC). Other functions such as a list of countermeasures (provided by the decision support functionality) were rated as a good support for the GAMMA operator.

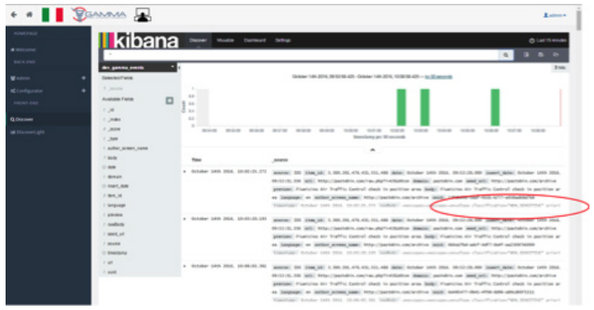

Figure 19: Security report displayed in NGSMP Command and Control interface

The capabilities of the Attack Effect Prediction Module were considered to be very interesting. During the validations it appeared to be beneficial when some of the complex actions of the configuration phase are accompanied by a dedicated training. Furthermore the predictive capabilities of the Cyber Security Intelligence Platform were regarded to be of high interest because they provide the ATM system with information about possible attacks.

DISSEMINATION

NEWS

First integrated validation workshop

On 4th May 2017 a geo-distributed validation workshop was organized to coincide with the execution of the first integrated validation exercise in the GAMMA project. This demonstration follows the stand alone validations which were conducted at the end of 2016 involving the separate prototypes in their own environment.
The demonstration and associated workshops were focused on the ability of GAMMA prototypes to identify a correlated attack on two separate countries in Europe. More specifically, the scenario involved:

- Two coordinated attacks applying the same methods in two different European countries;
- One fully independent, uncoordinated attack of a passenger on board a commercial airplane who is trying to get access to important cockpit systems, such as the electronic flight bag

The demonstration, which applied the GAMMA Conops in the specific case of coordinated attacks, was intended as the starting point for a wider discussion with a group of experts of the relevance of the Concept, including the layered approach to managing security in Europe, and how it could be applied in the real world. Discussions were therefore centered around concepts of information sharing, sanitization, automation, decision making processes and countermeasures.
The demonstration involved the following GAMMA Partners: DLR (coordinator of the exercise and hosting a parallel workshop in DLR Braunschweig), Leonardo (hosting the Chieti workshop), Airbus DS CYB, Thales UK, 42Solutions and BRTE.

GAMMA at World ATM Congress 2017

GAMMA was very prominent at the World ATM Congress 2017 organizing a Seminar in which the work and results of the GAMMA project were presented to an audience with a specific interest in ATM. The presence of GAMMA during WAC 2017 was further enhanced through the separate dissemination actions carried out by those consortium partners (Leonardo, Airbus, DLR and BOEING) with a stand in the exhibition hall. The separate partner stands provided the opportunity for widespread dissemination of GAMMA brochures as well as platforms for displaying overview presentations of the project.
The GAMMA seminar was the occasion to promote the forthcoming validation workshops and advertise the final event planned for autumn 2017. The seminar laid out a general template for the many dissemination actions planned in the next future and stimulated the appetite of the ATM community and stakeholders to follow the Project during its final validation phase.
The initial presentation of the seminar, given by Rainer Koelle (University of Lancaster), served to set the work performed in GAMMA on ATM Security Risk Assessment within the wider context of similar initiatives, most notably SESAR. This laid the ground for a presentation by Francesco di Maio (ENAV) aimed at placing the vision and Operational Concept developed for GAMMA within the wider institutional context. The Seminar then moved on to the practical developments carried out within GAMMA, including an overview presentation on GAMMA Prototypes, focusing on the SMP (Giuliano d'Auria – Leonardo), Attack Effect Prediction (Denis Kolev – RNCA) and SACOM (Tim Stelkens Kobsch – DLR). Finally the GAMMA Validation activities and scenarios were presented jointly by Tim Stelkens Kobsch (DLR) and Frédéric Duten (Airbus DS), who included in their presentation an insight into the three integrated validation exercises planned to be carried out in the next months.

NETWORKING

GAMMA injecting expertise to EREA

The European Research Establishments in Aeronautics (EREA) invited the DLR (project partner of GAMMA) to join the ad-hoc working group "Security in Aviation". This group will perform a study as an input for FP9. Another white paper more focusing on technical implementation will be written during the work of this group, additionally. The request for engagement is a clear consequence and direct impact from the GAMMA work.

GAMMA Advisory Board meeting with SJU and EASA

An Advisory Board meeting was held in Brussels on 10th November 2016. The GAMMA Advisory Board is formed by SJU and EASA and this meeting is part of periodic contacts with reference institutions in Europe to assure alignment and gather feedback for the strategic direction of the project. The November meeting was the first to be organized jointly with both SJU and EASA. The Advisory board was mainly focused on the forthcoming validation activities and provided the opportunity to illustrate the scenarios which will be enacted in the tests planned for spring 2017. During the meeting invitations were made to both EASA and SJU to the workshops expected to be organized as part of the validation activities.

GAMMA at final workshop of ARIEL

The GAMMA project was present at the final workshop of the project ARIEL (Air Traffic Resilience). The German Aerospace Center (DLR) as representative of GAMMA was invited to speak during a plenary talk, where the different challenges in the area of ATM Security were discussed. With this action ATM Security expertise from the GAMMA perspective was provided to a broad audience of security in air traffic management. The plenary talk could therefore also be used as a starting event for future collaboration.

GAMMA meeting with EDA

On 17th November 2016 a meeting was organized with several representatives from EDA in their Brussels premises to illustrate progress of the GAMMA project. The workshop follows a similar meeting organized in 2015 and regular contacts maintained during the years with this important European institution. Links with EDA are especially relevant in view of the GAMMA activities on Civil Military Cooperation that have led to the delivery of a document produced also with input derived from EDA. This meeting was mainly focused on the illustration of the GAMMA 'Partial 1' validation scenario, which is centered around civil military cooperation concepts. During the meeting, an invitation was made to EDA to take part in the validation workshop planned for this specific exercise.

FUNDING OPPORTUNITIES

H2020-CS2-CFP06-2017-01
Deadline 21 June 2017

By spearheading European aeronautics research culminating in demonstrations of game-changing new vehicle configurations, Clean Sky 2 will enable the aeronautics industry to introduce innovations in timescales that would otherwise be unachievable. The 6th Call for Proposals is now published and it includes 74 topics covering the following areas: Large Passenger Aircraft IAPD, Regional Aircraft IADP, Fast Rotorcraft IADP, Airframe ITD, Engines ITD, and Systems ITD., Technology Evaluator.

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-cs2-cfp04-2016-02.html#c,topics=callIdentifier/t/H2020-CS2-CFP04-2016-02/1/1/1/default-group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identifier/desc

H2020-LCE-20-2016-2017 Enabling pre-commercial production of advanced aviation biofuel
Deadline: 7 September 2017

Projects should target the most promising advanced aviation biofuel production pathways incorporating upgrading technologies and valorisation of co-products that improve the economic viability of the fuel production. The ultimate production target of aviation biofuel for the complete plant shall be in the range of several tens of thousand tonnes per year. The aviation biofuel must be fully compliant with international aviation fuel standards and therefore suitable for commercial flight operations.

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/lce-20-2016-2017.html

SMEInst-10-2016-2017: Small business innovation research for Transport and Smart Cities Mobility
Deadlines Phase 1 in 2017: 8 November 2017 (cut off dates: 6 September 2017, 8 November 2017)
Deadlines Phase 2 in 2017: 18 October 2017 (cut off dates: 1 June 2017, 18 October 2017)

The SME instrument addresses the financing needs of

internationally oriented SMEs, in implementing high-risk and high-potential innovation ideas. It aims at supporting projects with a European dimension that lead to major changes in how business (product, processes, services, marketing etc.) is done. Actions to develop new services, products, processes, technologies, systems and combinations thereof that contribute to achieving the European transport and mobility goals defined in the 2011 Transport White Paper could be particularly suited for this call.

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/smeinst-10-2016-2017.html

H2020-MSCA-IF-2017

Deadline: 14 September 2017

Individual Fellowships provide opportunities to acquire and transfer new knowledge and to work on research and innovation in a European context (EU Member States and Associated Countries) or outside Europe. The scheme particularly supports the return and reintegration of researchers from outside Europe who have previously worked here. It also develops or helps to restart the careers of individual researchers that show great potential, considering their experience. Support is foreseen for individual, trans-national fellowships awarded to the best or most promising researchers of any nationality, for employment in EU Member States or Associated Countries.

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-msca-if-2017.html#c,topics=callIdentifier/t/H2020-MSCA-IF-2017/1/1/1/default-group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identifier/desc

H2020-FETOPEN-01-2016-2017

Deadline: 27 September 2017

This call aims to support the early stages of joint science and technology research for radically new future technological possibilities. The call is entirely non-prescriptive with regards to the nature or purpose of the technologies that are envisaged and thus targets mainly the unexpected. A bottom-up selection process will build up a diverse portfolio of projects.

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/fetopen-01-2016-2017.html

For more information about funding opportunities, please contact: c.salas@ciaotech.com

CONSORTIUM

LEONARDO
WWW.LEONARDOCOMPANY.COM

Airbus SAS
WWW.AIRBUS.COM

Boeing
WWW.BOEING.COM

Airbus Defence and Space
WWW.AIRBUSDEFENCEANDSPACE.COM

Airbus Defence and Space Cybersecurity
WWW.CYBERSECURITY-AIRBUSDS.COM

CiaoTech
WWW.CIAOTECH.COM

DLR
WWW.DLR.DE/FL/

Airbus Group Innovations
WWW.AIRBUSGROUP.COM

ENAV
WWW.ENAV.IT

Isdefe
WWW.ISDEFE.ES

Lancaster University
WWW.LANCASTER.AC.UK

RNC Avionics
WWW.RNC-AVIONICS.COM

Romatsa
WWW.ROMATSA.RO

SEA
WWW.SEAMILANO.EU

Thales Alenia Space
WWW.THALESALENIASPACE..COM

Thales Avionics
WWW.THALESGROUP.COM

Thales UK Research& Technology
WWW.THALESGROUP.COM/UK

Ustav Informatiky
WWW.UI.SAV.SK

42 Solutions
WWW.42SOLUTIONS.NL

ACKNOWLEDGEMENT

The GAMMA Project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under Grant Agreement Nº 312382.