Global ATM security management

Project type:	Collaborative project		
Start date of project:	1st September 2013	Duration:	48 months

GAMMA Concept of Operations

Version	Rev. 01.00

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement nr. 312382

Document Revision History

Revision	Date	Author/Editor/Contributor	Summary of main changes
00.10	05.11.2014	R. Koelle	Initial draft for project consultation
00.20	12.12.2014	R. Koelle	Inclusion of first set of comments
00.21	27.01.2015	R. Koelle	Inclusion of working meeting decisions on open issues
01.00	09.06.2015	R. Casar	First Delivery, updates with the comments from GAMMA Project Management Board

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

REFERENCE DOCUMENTS

[1]. IEEE Computer Society. IEEE Guide for Information Technology - System Definition - Concept of Operations Document, IEEE Std 1362-1998. 1998.
[2]. American National Standards Institute. Guide to the Preparation of Operational Concept Documents, G-043A-2011. 2011.
[3]. GAMMA Consortium. Global ATM Security Management. 2012.
[4]. ICAO. Global Air Traffic Management Operational Concept, ICAO Doc 9854. 2005.
[5]. Air Traffic Management Security Guidance, ICAO Doc 9985. 2013.
[6]. Annex 17 to the Convention on International Civil Aviation, Securty, Safeguarding International Civil Aviation Against Acts of Unlawful Interference, Ninth Edition. 2011.
[7]. SESAR B.04.03. -- check title -- D73.
[8]. SESAR 16.06.02. SESAR Security Reference Material, Level 1. 2013.
[9]. ISO/PAS 22399:2007. Societal security - Guideline for incident preparedness and operational continuity management. 2007 (reviewed in 2011).
[10]. Multi-agent situation management for supporting large-scale disaster relief operations. J. Buford, G. Jakobson, and L. Lewis. 2006, International Journal of Intelligent Control and Systems, 11(4), pp. 284–295.

LIST OF ABBREVIATIONS AND DEFINITIONS

Acronym	Definition
ACC	Area Control Centre
AESA	Agencia Española de Seguridad Aérea
AIAA	The American Institute of Aeronautics and Astronautics
AIM	Aeronautical Information Management
ANS	Air Navigation Surveillance
ANSI	American National Standards Institute
ANSP	Air Navigation Service Provider
ASSIM	Airspace Security Incident Management
ATC	Air Traffic Control
ATM	Air Traffic Management
ATS	Air Traffic Service Provider
ATSP	Air Traffic Separation
CAA	Civil Aviation Authority
CIA	Confidentiality, Integrity and Availability
CIMACT	Civil-Military ATM Coordination Tool
CNS	Communication Navigation and Surveillance
CONOPS	Concept of Operations
DFS	Deutsche Flugsicherung
DOW	Description of Work
DSNA	Direction des Services de la Navigation Aérienne

Acronym	Definition
EACCC	European Aviation Crisis Coordination Cell
EASA	European Aviation Safety Agency
EC	European Commission
ECAC	European Civil Aviation Conference
EDA	European Defense Agency
EGCC	European GAMMA Coordination Centre
ENAC	Ecole Nationale de l'Aviation Civile
ENAV	Ente Nazionale Di Assistenza Al Volo
EU	European Union
FAA	Federal Aviation Authority
FDP	Flight Data Processor
GA	General Aviation
GAMMA	Global ATM Security Management
GNSS	Global Navigations Satellite System
HW	Hardware
ICAO	ICAO
IDS	Information and Dissemination System
IEEE	Institute of Electrical and Electronics Engineers
IPOCM	Incident Preparedness and Operational Continuity Management
IR	Implementation Rule
ISO	International Organization for Standardization

Acronym	Definition
IT	Information Technology
LBA	Luftfahrtbundesamt
LGSOC	Local GAMMA Security Operation Centre
NATO	North Atlantic Treaty Organization
NATS	UK Air Traffic Service Provider
NCASP	National Civil Aviation Security Programmes
NGA	National Governmental Authorities
NGSMP	National GAMMA Security Management Platform
NM	Network Manager
NSA	National Supervisor Authorities
OCD	Operational Concept Description
PAS	Publicly Available Specification
PCP	Pilot Common Projects
PDA	Portable Device
SELEX	Italian Air Traffic Management Industry
SESAR	Single European Sky ATM Research Programme
SMP	Security Management Platform
SOC	Security Operation Centre
SW	Software
SWIM	System Wide Information Management
UK	United Kingdom

Acronym	Definition
ULANC	University of Lancaster
US	United States
WP	Work Package

Front Matters

Overview

This document presents the GAMMA concept of operations (CONOPS). The GAMMA CONOPS is drafted to provide top-level guidance and to serve as a common reference for all GAMMA work packages/tasks.

The objective of this document is to describe the operational environment so that all GAMMA project members (and stakeholders) gain a common understanding of the operational characteristics of the GAMMA solution and the associated capabilities (including the associated implied changes in operational procedures and practices).

This CONOPS is drafted based on the ANS/AIAA G-043A-2011 standard that is targeted at the support of new system development.

This version of the CONOPS addresses the conceptual building blocks. The further development of the operational scenarios (i.e. Chapter 8) will be subject to the further decision taken with respect to identifying validation exercise scenarios to demonstrate the GAMMA capabilities. The conceptual elements in this document allow for the design and development of the security related capabilities of the prototypes as these will have to address the different phases and stages of the dynamic security management and internetworking for the management of incident situations. The scope of this document is limited to capabilities within the scope of the validation and demonstration of GAMMA solution elements. The full width of GAMMA capabilities will be reflected in the respective GAMMA deliverables (e.g. WP3). In this context, the CONOPS is complementing the contractual GAMMA deliverables.

This version of the CONOPS is drafted for project internal consultation.

Preface

A recognised system engineering best practice is the early development of operational concepts and their refinement during the system development life-cycle. This includes the documentation of these concepts at different levels in one or more (operational) concept documents.

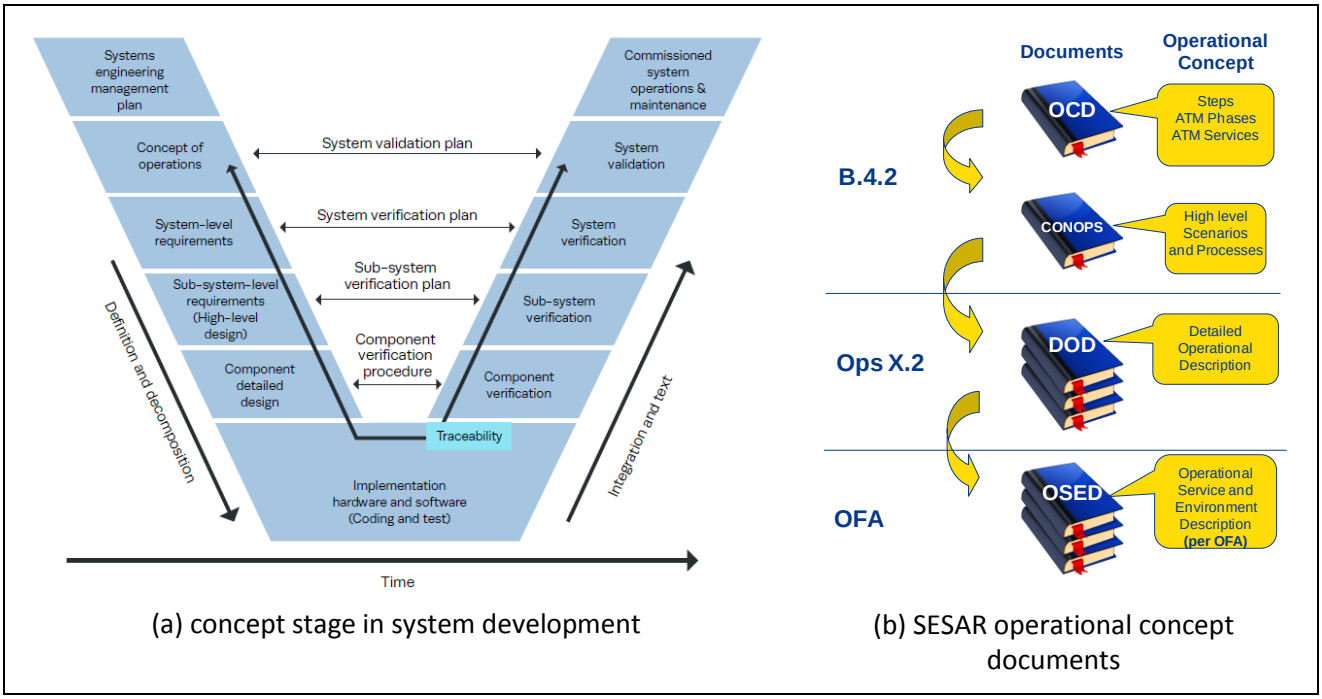
Fundamentally, an operational concept is prepared initially to support the concept and development stages of the system life cycle and is then maintained throughout the various stages (i.e. production, operation, support, decommissioning).

The terms “operational concept” and “concept of operations” (and the associated documents) are often used interchangeably in system development. Though there are similarities between the two terms, it is important to understand the differences. For the purpose of GAMMA, this document makes a clear distinction between these terms as each concept document has a separate purpose and is prepared to meet separate ends.

A concept of operations (CONOPS) presents an abstract model of a system and how it is intended to operate to achieve its goal and objectives without addressing the technical solution or implementation. In that respect, the CONOPS is independent of particular (sub-) systems used in the operations. A CONOPS is a user-oriented document that “*describes systems characteristics for a proposed system from a user’s perspective. A CONOPS also describes the user organisation, mission, and objectives from an integrated point of view and is used to communicate overall … system characteristics to stakeholders*” (1).

Within the context of GAMMA it is essential to recognise the scope of ATM security in that the GAMMA solution is embedded in the operational context of the ATM System while the GAMMA solution purpose is to ensure the envisaged security capabilities. Considering this interplay, the “user-orientation” of the CONOPS breaks down into the operations for the envisaged security capabilities (GAMMA operator perspective) and the interfaces between the GAMMA solution and respective ATM and ATM security actors (GAMMA user perspective).

The CONOPS is designed to give an overall picture of the system’s / organisation’s operations (i.e. series of connected operations carried out simultaneously or in succession) and answers the questions “what” and “how” the operations shall be enabled. It provides the overall concept level guidance to ensure consistent development of the operational concept components and capabilities. The CONOPS is typically further detailed in operational concepts, detailed operational descriptions describing the concept at a more detailed, e.g. functional, level (c.f. Figure 1 (b)).



(a) concept stage in system development

(b) SESAR operational concept documents

Figure 1 -Concepts

Standards for the development of concept of operations comprise can be broadly categorised for new system developments and system upgrades.

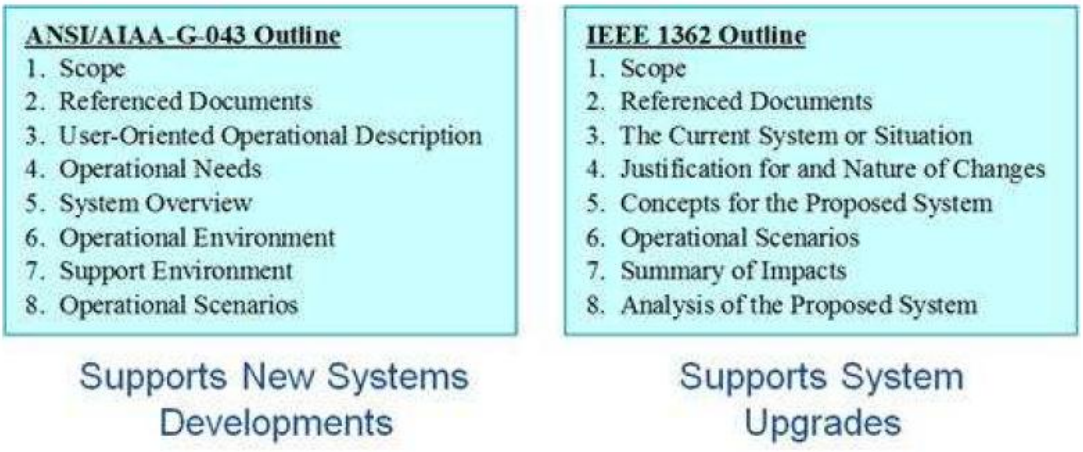


Figure 2 – CONOPS outline comparison (ANSI/AIAA-G043 and IEEE 1362)

The IEEE Guide (1) takes an opportunity-driven approach (we can do it) rather than a capability-needs-driven approach (what the user or intended operations need) followed by the American National Standards Guide (2). Within the context of the GAMMA project, the IEEE Guide describes an operational concept document (OCD) and some essential parts are developed as part of the GAMMA statement of work (3) already (i.e. motivation / justification for change). This approach is also reflected in the SESAR hierarchy of documents in which the OCD drives the development of a CONOPS which will then be further detailed in form of DODs and OSEDs (c.f. Figure 1 (b)).

This CONOPS follows the ANSI G043A-2011Guide (2) addressing the user-oriented perspective describing the characteristics for the proposed GAMMA solution from the viewpoint of any individual user or organisational entity that will use it in the series of connected operations.

1 Executive Summary

The GAMMA concept of operations is a working document developed within the WP3 activities to be included in the Deliverable D3.1. It describes at a high-level how the GAMMA solution will be employed to meet the GAMMA mission objectives and drive the development of the identified – prototypical – capabilities with a view to the validation and demonstration of some parts of the GAMMA concept. In that regard, the CONOPS supports the development of the rest of the contractual deliverables which altogether describe the full width of the GAMMA solution.

This CONOPS document was developed in preparation of the validation work packages and the discussions surrounding the operation of the GAMMA solution. The CONOPS describes the required characteristics, the core capabilities, and the envisioned operational use. Therefore this working document is used as a direct input for WP4 activities which addresses the definition of GAMMA ATM security solution. This includes the GAMMA security requirements specification and the architecture of the GAMMA solution.

As an indirect input, this working document serves as inspiration for the definition of the validation activities to be planned and designed within WP5 as well as for the development of the prototypes within WP6 to be used in the validation exercises. The GAMMA solution comprises the following major conceptual elements:

- GAMMA organisation – the establishment of a distributed set of GAMMA operators and users within the operational context jointly collaborating in the management of security;
- GAMMA continuous security management capability; which is related to the 24/7 operations of the security management component for the establishment of “security situational awareness”;
- GAMMA situation management / incident management capability – the set of functions and capabilities to manage security incidents;
- GAMMA distributed network and information exchange – the technical means for the day-to-day dynamic management of system security.

A CONOPS is neither a specification nor a formal statement of requirements. It is used as a source of information for the development of such documents and for project planning and decision making. This document provides an initial mapping between the CONOPS and validation requirements by addressing operational scenarios for each of the envisaged GAMMA demonstrators.

The GAMMA CONOPS is not defined as a living document for the design and development phase of the project. However, changes to the operational concepts surrounding the GAMMA solution will be developed under the umbrella of WP3 activities within D3.1 ATM Security Framework deliverable.

2 Introduction

2.1 Document Scope

This document presents the GAMMA concept of operations (CONOPS) and describes at a high-level how the GAMMA solution will be employed to meet the GAMMA mission objectives and drive the development of the identified capabilities. It documents the organisation, roles and responsibilities, processes and operations of the GAMMA solution.

The scope of this document comprises the conceptual aspects of the operations envisaged to be enabled through the GAMMA solution. It is out of the scope to set out the capabilities supported by the GAMMA prototypes / demonstrators leaving this aspect to the validation activities to be developed within GAMMA project.

2.2 GAMMA Purpose

The overall purpose of the GAMMA project is to define and then demonstrate a comprehensive approach to ATM security by providing a concrete proposal for the implementation of capabilities to address and manage dynamically security risks. For that purpose it is envisaged to demonstrate and validate the most important parts of the GAMMA solution concept elements on the basis of prototypes.

GAMMA addresses a gap in today's capabilities by addressing security risks stemming from the evolution of the ATM system, its operations, and emerging vulnerabilities by addressing both aspects of ATM security:

- Self-protection / resilience of the ATM system; and
- Collaborative support to other aviation security stakeholders.

The GAMMA system context is described by ATM system context comprising the dynamic and integrated management of all space-, airborne-, and ground-based functions, facilities and services, to ensure the safe, orderly, efficient flow of air traffic (c.f. ICAO Doc 9854 (4)). The major objective of the ATM system is to provide air navigation services to airspace users. Within the hierarchy of air navigation services, separation and traffic synchronisation form the immediate safety-critical services which are operated on the basis of the ATM system components and its underlying communication, navigation, and surveillance infrastructure.

Self-protection / resilience therefore address the assurance of these air navigation services. With regard to security, the ICAO Doc 9854 further specifies: "The ATM system should therefore contribute to security, and the ATM system, as well as ATM-related information, should be protected against security threats. Security risk management should balance the needs of the members of the ATM community that require access to the system, with the need to protect the ATM system."

This vision has been further developed in SESAR ultimately culminating in the ICAO Security Manual (ICAO Doc 9985 (5)) and confirming the aforementioned dual requirements on ATM Security. In ICAO 9985 ATM Security is now formally defined as "the safeguarding of the ATM system from security threats and vulnerabilities, and the contribution of the ATM system to civil aviation security, national security and defence, and law enforcement."

The GAMMA solution will therefore have to address the context and purpose established for ATM security in terms of embedding the GAMMA capabilities within the ATM system context; developing associated GAMMA solution (sub)-functions, including addressing the requirements and constraints of the operational environment (and support environment) (c.f. Figure 3).

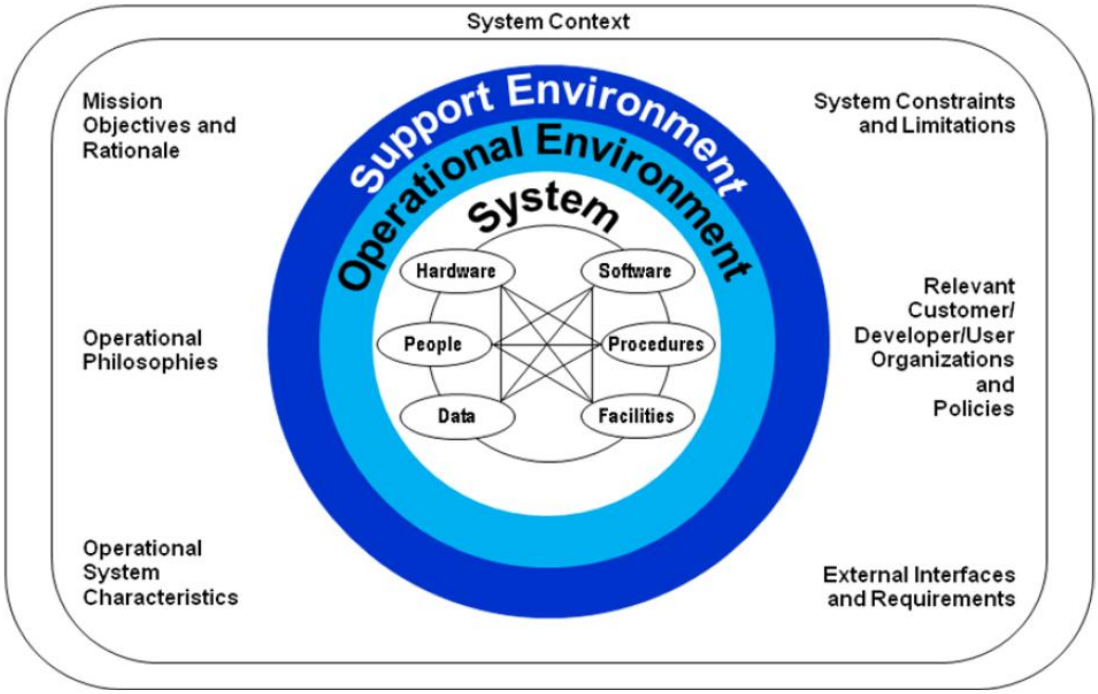


Figure 3 – CONOPS System Context

The ATM security function, as established by the GAMMA project, is an additional air navigation system service. This service establishes the dynamic and continuous security management, incident management capability, including collaborative support.

The ATM security role has a traditional internal focus on (self-)protection of the ATM system itself and an operational role in the support of certain aspects of aviation security as well as national security and law enforcement. ATM self-protection refers to internal security services provided and consumed by the Air Traffic Service Provider (ATSP), such as cyber-security services to protect cyber systems and physical protection of facilities.

The GAMMA solution can be conceptualised comprising the following conceptual elements:

- GAMMA organisation – the establishment of a distributed set of GAMMA operators and users within the operational context jointly collaborating in the management of security;
- GAMMA continuous security management capability; which is related to the 24/7 operations of the security management component for the establishment of "security situational awareness";
- GAMMA situation management / incident management capability – the set of functions and capabilities to manage security incidents;
- GAMMA distributed network and information exchange – the technical means for the day-to-day dynamic management of system security.

GAMMA prototypes will take into account these conceptual elements enabling the validation of part of the GAMMA solution. They will consist of a set of local security (sub-)system in charge of the detection of security attacks interconnected to the local security operation centre or national security management platform (SMP) and/or the GAMMA network.

2.3 Document Structure

This CONOPS details the concepts and processes by which the GAMMA solution will establish the envisaged capabilities and perform its functions within the European air navigation system and ATM security context and as enabled by the envisaged GAMMA validation and demonstrations.

This CONOPS is not designed as a living document. However, it is recognised that – as the GAMMA work programme unfolds – this CONCOPS matures and will be revisited, revised, and extended to reflect the dynamic nature of the system context, the refined understanding of the operational environment and system capabilities and its elements as far as applicable to the GAMMA validation and prototype demonstration. The full width of the GAMMA solution will be represented within D3.1 deliverable.

3 Background

This chapter establishes key drivers for the mission objectives and intended operations. It focuses on the "why" of the system and its anticipated capabilities. In particular, it establishes the institutional drivers for ATM security in response to regulatory requirements.

3.1 Aviation Security and ATM Security.

Security of civil aviation is framed by ICAO Annex 17 (6) as the *"safeguarding civil aviation against acts of unlawful interference. This objective is achieved by a combination of measures and human and material resources*."

Within this context, ICAO Doc 9854 and Doc 9985, establish the dual scope of ATM security as described above.

Though security of civil aviation is not a new subject, ATM security is still in its infancy stage. Considerations of ATM security, its scope definition, and initial developments have emerged following the September 2001 attacks and the associated global review of critical infrastructure protection and continuity of (public) services.

Immediately following the September 2001 attacks an operational focus was put on the establishment and improvement of operational procedures and coordination means between ATSP and national authorities, including national defence with a view to addressing the needs of responding to such an incident.

In the wake of the September 2001 attacks, several States have further reviewed their critical infrastructure posture and expanded their review to the overlap between critical infrastructure protection and security and service continuity requirements for air transportation infrastructure, i.e. ATM system.

The latter approach formed also the basis for the development efforts identified by SESAR and NextGen Programmes. Furthermore, a joint European-US activity led to the establishment of the ICAO security manual (5) which is primarily based on the experience of EUROCONTROL and FAA developing an initial set of guidance and best practices for ATM security.

With its latest revision, ICAO Annex 17, Chapter 3, para 3.5, recognises the role of air traffic service providers within the context of aviation security by requiring ATSP to establish the appropriate security provisions in accordance with the national aviation security programme and recommending measures addressing cyber threats to the safety of aviation (c.f. Chapter 4, para 4.9).

3.2 National Security and Organisational Security

Security is a national responsibility. This principle is recognised in the sovereignty of each state for its territory, and ultimately the public services provided within this frame. Equally, the primacy of national sovereignty permeates security-related decision-making processes.

This principle has been highlighted in ICAO Annex 17 and related guidelines (e.g. ICAO Doc 9985 – ATM Security Manual, Doc 8973 – Aviation Security Manual), under the framework of National Civil Aviation Security Programmes (NCASPs). The sovereignty of a Member State regarding security and defence matters has also been highlighted in European Single European Sky Regulation (EC n. 549/2004, ref. art. 13).

States are responsible for providing air traffic services and related supporting services in their airspace. This responsibility extends to the contingency situations for instituting measures to ensure the safety of international civil aviation operations and, where possible, for making provisions for alternative facilities and services. Such measures must include security provisions.

States may delegate the responsibility for the provision of air navigation services to appropriate entities. Throughout the recent years, liberalisation in air transportation has also led to the establishment of

partially state-owned or completely privatised entities. This has been recognised in the European legislation. In particular, the European directive on critical infrastructure protection (2008/114/EC) as well as the Single European Sky legislation, i.e. Implementing Rule 1035/2011, recognise the role of the State in security governance requiring to establish an appropriate oversight body and enforce the establishment of security plans or security management systems to discharge their institutional responsibility for national security.

To that extent, appointed entities (i.e. Air Navigation Service Provider (ANSP)) are required to establish an organisational security management system to ensure the security of their system operations and service provision and comply with national security processes / procedures.

3.3 State-of-the-art in ATM Security

The infancy stage of ATM security was briefly introduced above.

The major research and development programmes, i.e. SESAR and NextGen, have postulated the need for ATM security. However, prevailing political priorities and focus on operational improvements left a substantial gap in establishing a security management and incident handling capability. Within SESAR, ATM security focuses on the establishment and implementation of security risk management practices within the system-engineering life-cycle. However, initial deployment activities like the current pilot common projects (PCP) cover only principal requirements in terms of self-protection through preventive security measures. A similar stance is taken by the NextGen programme in terms of self-protection / resilience. With a view to collaborative support, the US / FAA has embedded a flight monitoring capability within their central air traffic service organisation centre.

Further related research activities are reported in the GAMMA DOW (3) which – in summary – have not lead to actual implementations so far.

A limited number of national initiatives have been established across Europe to address the better coordination between different national authorities, e.g. German Central Air Situation Centre comprising staff from the Bundeswehr, Ministry of Interior, and DFS. The United Kingdom has established a Gold-Silver-Bronze structure for incident management and across different organisations that allow for the coordinated response to emergencies and crisis situations. Within Europe, under the umbrella of the NATO integrated air defence system, operational procedures have been developed to streamline the change of authority and coordination during aviation security incidents.

Based on the requirements of IR1035/2011 (repealing IR2096/2005) European ANSPs have established organisational security management systems and associated processes. As concerns the development of dedicated security operation centres within ATM, Italy / ENAV has established the first SOC (Security Operation Centre). Dedicated resources for cyber security monitoring and response programmes within ATM are also reported in France / DSNA[1]and United Kingdom / NATS[2].

In summary, the level of implementation of operational capabilities and technical resources dedicated to the day-to-day management of security of ATM and CNS (Control Navigation and Surveillance) sub-systems varies widely across the EU Member States. Equally, there is a lack of a pan-European approach to ATM security related information exchange and coordination including the underlying technical enablers for an associated wider incident management capability, and tools for collaborative support.

A more detailed discussion on the state-of-the-art in ATM security can be found in the GAMMA DOW.

[1] French Air Navigation Service Provider
[2] UK Air Navigation Service Provider

4 User-Oriented "Existing" Operational Description

This section describes the existing system context and the nature of the operations being conducted. This section does not specifically address security management system processes and procedures within an ANSP organisation. The focus of this section is on the capability gap identified by the GAMMA proposal (i.e. dedicated resources and technical systems for the day-to-day management of security, dynamic incident management, and collaborative support).

Note: *the GAMMA solution revolves around a national security management platform and operations centre based approach. This does not pre-empt any national or ANSP decision on the adaptation or implementation of such an approach. In that respect, the "existing" operational description addresses the void identified and targeted by the GAMMA proposal.*

4.1 Operational Environment

Security is not a categorically "new" requirement within air transport and air navigation. The classical focus of aviation security concerns preventive security measures targeted at ensuring the integrity of aircraft and preventing the seizure of aircraft.

4.1.1 Self-Protection / Resilience

Security of air traffic control centres, supporting technical infrastructure and systems is still primarily understood as basic physical security to prevent unauthorised access to the installation or interference with the technical component through vandalism or destruction. The technical monitoring of (sub-)system components is primarily driven by technical requirements to meet the stringent safety standards.

Throughout the recent years, a combination of international and national guidance and regulation has been put in place that require ANSP to establish a security management system, assume operator responsibility for the operation and continuity of the services provided, etc.

This resulted in the establishment of principal security functions, processes and procedures within European ANSPs.

Note: *The [pro-active] coordination with civil and military authorities to ensure the security of ATM and CNS facilities, staff, and data (c.f. IR 1035/2011, Annex I, para 4) falls under the scope of self-protection / resilience. National procedures and requirements for the protection of facilities vary. National vetting procedures govern the processes surrounding the security clearances of ANSP staff.*

The GAMMA CONOPS anticipates that an ANSP addresses these requirements as part of the SecMS (Security Management System) / national processes.

In-situ alerting / coordination of security incidents – as far as covered by this CONOPS – are understood as information exchanges under the umbrella of collaborative support.

To a very limited extent – as reported above – ANSPs have established dedicated resources and technical means (i.e. security operation centres) for the continuous security monitoring and the coordination of security responses to attacks.

National or pan-national capabilities for security situation awareness / information exchange are not implemented in the majority of the States. Security incident coordination (and management) is typically addressed on a voice communication basis between the different units involved (e.g. centre-to-centre and centre-to-authority coordination / reporting).

4.1.2 Collaborative Support

In the classical aviation security context (prior to the September 11th attacks, 2001), the role of ANSP units in response to unlawful acts against civil aviation is primarily defined in procedural terms (c.f. changes to Annex 17, 9th edition with amendment No.14). This comprises the priority handling of aircraft subject to unlawful interference as distress traffic (e.g. enabling re-routing or uncoordinated manoeuvres while maintaining separation to other traffic) and ensure the separation between national response measures (e.g. intercept, forced landing at intervention airfield). The associated operational procedures and support function can be understood as the forerunner to the collaborative support role of ATM as defined in today's scope of ATM security (c.f. SESAR, ICAO Doc 9985).

In the wake of the September 11th attacks, the reporting procedures between ANSPs and national authorities, in particular airspace incident management centres and air defence control centres, have been reviewed and refined accordingly. This further includes wider security-related information and coordination with national authorities (e.g. law enforcement, intelligence, critical infrastructure protection, national cyber-security agencies).

The collaborative support function is still primarily based on voice coordination between the respective ATS unit and the national centre / air defence control unit or other relevant party. While different solutions for national or pan-national technological support have been tested and demonstrated throughout the last years, no structured technological support for the collaborative support function has been deployed yet across Europe.

Note: *Different ANSPs have established an ad-hoc crisis centre or coordination cell approach. This function is typically performed by a variety of staff. This is subsumed under "respective ATS unit", though the centre/cell may be not physically located within the ATS unit. It also covers wider joint operations approaches, such as airport emergency operation centre which may also include non-ATS staff.*

Note: *Dependent on the local implementation technological support for situational awareness and information exchange may be deployed. This should not be confused with the technical capabilities envisioned as part of the GAMMA solution.*

4.2 Roles

Introductory Comments – "Existing" Operational Description Personnel"

> The GAMMA CONOPS addresses operations performed by GAMMA operators (i.e. dedicated resources operating the GAMMA solution). The CONOPS covers from a high level perspective, and then more detailed in WP4 tasks, the global generic GAMMA solution that will be adapted for the validation and prototype demonstration.
>
> Conceptually, security functions and roles within an ANSP not acting as a GAMMA operator (i.e. situated at a national security management platform or local sub-system security operation centre) shall be considered as interfacing with the GAMMA solution as a (dedicated organisation-internal) GAMMA user in combination with the associated process / procedure to be defined as part of the operations (e.g. involvement of security manager / post holder in decision-making on deployment of additional security controls).

The previous sections describe the limited level of implementation of security operation centres across Europe. With the noted exemptions, this CONOPS considers that no dedicated personnel are deployed within the ATM system context at the time being for both aspects of ATM security, i.e. self-protection / resilience and collaborative support in a 24/7 set-up.

Operational and technical staff assumes their security role as part of their secondary role(s)/function(s):

- technical monitoring of (sub-)system functions is typically performed as part of the technical operational assurance and rests with the technical maintenance organisation of the ANSP;
- air traffic controllers ensure separation and synchronisation of air traffic based on existing operational procedures which are linked to the capability level of the supporting technology;
- for collaborative support, it depends on the local procedures; coordination between the ATC centre and the respective air defence control unit is managed by Air force and by the watch supervisor or other ad-hoc coordination functions;
- equally, staff working within these centres and air defence are typically tasked with other day-to-day activities and assume the coordination role in case of an incident situation. It is noteworthy that for non-operational units (e.g. national crisis centres) this may require a considerable activation time.

From an organisational perspective, ANSPs of EU Member States have established security management roles within their organisation as part of the SecMS requirements stipulated in IR1035/2011 and other relevant European or national requirements. These roles may be assumed by staff outside the aforementioned groups (i.e. operational and technical staff).

In terms of "existing operations" it is assumed that the processes and procedures are established to meet the procedural and regulatory requirements. However, within the scope of this CONOPS and the noted exemptions, no dedicated resources and means for dynamic security management are in place. One of the shortcomings today – to be addressed by the GAMMA solution – is that there is no comprehensive approach to the dynamic management of security and the associated situation / incident management for both, self-protection / resilience and collaborative support.

4.3 System Overview and Support Environment

This CONOPS is based on the overall research goal of GAMMA to investigate, devise, and demonstrate conceptual elements of the GAMMA solution. While the GAMMA solution addresses security related capabilities, it is not an end in itself. The GAMMA solution is conceptualised within the current ATM System.

The overall starting hypothesis for GAMMA – as presented throughout this chapter – is that with the exemption of isolated initial deployments (e.g. ENAV security operations centre) no dedicated ATM security operation centres are deployed within today's ATM system context providing capabilities for the dynamic management of security risks and collaborative support.

The current level of implementation is targeted at national and organisational procedures and requirements, and varies from Member State to Member State. Dependent on the national context or operational aspect (e.g. coordination of airspace security incidents) procedures and to a limited extent technological support are in place.

Existing solutions do primarily address local / national constraints and requirements. There is no harmonised approach to pan-organisational or pan-national coordination or security incident management.

In the absence of the major conceptual elements identified by this CONOPS, there is no "current" system and associated support environment.

Note: *This CONOPS complements other GAMMA deliverables that describe the GAMMA solution in its full width. From that perspective, this CONOPS will not address deployment-, maintenance-, and decommissioning-related support environment aspects. Equally, GAMMA operator-/user-training related aspects are out of scope of this CONOPS.*

5 Operational Needs

The GAMMA project stems from the recognition that – to date – no comprehensive ATM Security capability exists to address the envisaged operations.

In particular, the operational needs are:

- The establishment of a GAMMA organisation, i.e. distributed network of security operations centre capable of addressing self-protection / resilience functions and ensuring the collaborative support (c.f. section 6.1), including the interfaces to the identified GAMMA users;
- The definition and integration of operational procedures and supporting technological support (i.e. interconnectivity, networking, information dissemination) across the GAMMA organisation and between the GAMMA solution elements and the ATM System and collaborative support stakeholders and their systems (i.e. GAMMA users).

6 GAMMA Solution Overview

This chapter provides an overview of the proposed GAMMA solution within the scope of this CONOPS. The full width of the GAMMA solution is represented by the set of formal deliverables (D3.1, D4.1, D4.3).

To do this, firstly the goals and the boundaries of the GAMMA solution are described. Next section will address the proposed GAMMA Reference Model in which the main elements of the GAMMA solution are depicted. Afterwards the interfaces and communication aspects are presented.

Finally the description of the operation nodes will allow to get the global picture of the proposed GAMMA solution. It will be the baseline for the detail of the GAMMA solution concept through the requirement specification and the architecture definition. In addition to this, CONOPs will set the basis for the definition of the scope of the validation, and also the basis for the scenarios to be used and the high-level capabilities expected within GAMMA prototypes to support the validation of the GAMMA concept as detailed in the validation plan.

6.1 GAMMA Solution Scope, Goals, and Objectives

The GAMMA solution scope and system context has been described throughout this document.

The operational and technical scope of the GAMMA solution is given by the existing ATM system .The GAMMA solution will be embedded in this context and ensures the organisational and procedural requirements, including the envisaged technological support to establish the GAMMA solution capabilities for ATM security.

The primary use(s) of the GAMMA solution is targeted at establishing the envisaged capabilities for the GAMMA organisation to address for:

- self-protection / resilience of the ATM system:
  - the dynamic operation of the day-to-day management of the established security (sub-) systems through the provision of monitoring and analysis capabilities; and
  - the handling of security incidents across the complete spectrum from identification, decision-making / response, and post-incident activities.
- collaborative support:
  - the provision of appropriately sanitised data/information in support of the aviation security mission of the respective stakeholder; and
  - the support to aviation security response by ensuring the mission requirements in terms of separation and synchronisation of air traffic, and provision of incident support related information.

Note: *The GAMMA solution will not process "marked" (e.g. national or international organisation level classified) information. Data / information containing "organisation-sensitive" information shall be sanitised on the local or national level in order to exchange security information beyond the organisational (i.e. ANSP-level) and the national remit.*

6.2 GAMMA contribution to ATM Reference Model

This section intends to describe how GAMMA concept will contribute to the ATM Reference model in which the main elements of the GAMMA solution are identified. They basically consist of two main inputs:

- the definition of new roles and responsibilities and;
- the GAMMA nodes which define the high level structure of the GAMMA solution. New and existing roles will interact within GAMMA nodes, possibly resulting in changes on their current operations and responsibilities.

6.2.1 GAMMA Roles

This section describes the list of stakeholders, existing or new ones, which have been identified within the security boundaries of GAMMA. Each of them will have a direct impact within their operation and responsibilities when GAMMA solution is put into operation.

Furthermore, a list of internal and external stakeholders has been defined and showed in the next section.

Within the GAMMA solution two main groups of stakeholders have been identified: GAMMA solution "users" and GAMMA solution "operators", here forth **GAMMA users** and **GAMMA operators**, for the establishment of the GAMMA solution "organisation". Furthermore, a list of internal and external stakeholders has been defined within the group of the GAMMA users.

6.2.1.1 GAMMA Operator

"GAMMA operator" refers to any individual (or function performed by a human) interfacing with the GAMMA solution system(s) as part of the assigned operations and responsibilities. This includes staff located at the different levels, local, national and European security management platforms and local (sub-system) security operation centres.

Note: *The GAMMA project does not pre-empt the deployment decision on a national and/or ANSP-level. States / ANSPs may opt to implement a centre-approach or decide to interface with the GAMMA solution via / through their own systems. This may in fact result in various units / functions being interconnected to the GAMMA solution capabilities.*

For this CONOPS, it is assumed that the various GAMMA operators are provided with a dedicated (set of) Human Machine Interface(s) providing:

- situational information on the status of the supporting assets (e.g. technical / operational performance), the established security controls, and the availability of additional not deployed security controls;
- situational information concerning the analysis and identification of security threats, projection of impacts;
- interfaces to launch and/or complement situation / incident management related information exchange across the GAMMA security organisation, and if applicable with the respective GAMMA users ('need-to-know' principle);
- information to support decision making process (provision/proposal of solution to respond to a potential or real attack);
- guidance on post-incident activities.

6.2.1.2 GAMMA User

In contrast to GAMMA operators, "GAMMA user" refers to any individual (or function performed by a human) interfacing with the GAMMA solution through its own interfaces and during the execution of its operational tasks. Two classes of GAMMA users can be distinguished:

a) ATM internal stakeholders Internal: "classical" ATM system "stakeholder"; e.g. ATCOs.

b) External security stakeholders: They are "non-classical" ATM stakeholders within the scope of collaborative support; e.g. national governmental authority.

Below the set of the GAMMA users under the umbrella of the GAMMA solution are identified:

Internal stakeholders

- Airspace users
  - Aircraft crew
  - Airspace user operation centre (for all types of aviation, including the military)
- Air navigation service providers[3]
  - Approach ACC
  - Airport Tower
  - En-route ACC
  - Airspace Management Cells
- Airport operator and/or authority
- Airport ground handling service providers
  - EUROCONTROLNetwork Manager
- Aeronautical Information Providers
- Meteorological service providers
- SWIM service providers
- Security Manager
- European Commission
- European Civil Aviation Conference (ECAC)
  - airspace management coordinator for ECAC
  - air traffic flow and capacity planner for ECAC
- EASA: European Aviation Safety Agency
- European Aviation Crisis Coodination Cell (EACCC)
- National Supervisor Authorities (NSA)
- National Civil Aviation Security Programme (NCASP)
- Civil Aviation Authority (CAA)
- ICAO
- Military Authority for ATM Security
- National Security Authority

[3] ANSP can be indifferently civil, military or combined organisations on national or FAB level.

Example of External stakeholders

The European ATM system is interworking with multiple external systems (these have been listed by SESAR B.04.03: [5] "Development of the high level logical system architecture and the technical system architecture"):

- External (non-European) ATC;
- Non-aviation users;
- Non-ATM Meteo service providers;
- GNSS Service Providers;
- Air Defence;
- The "North Atlantic Treaty Organization" (NATO)
- National Governmental Authority (NGA)
- Member State Authority for the national critical infrastructure protection (CIP)
- External (Non-European) Aeronautical Information Management (AIM).

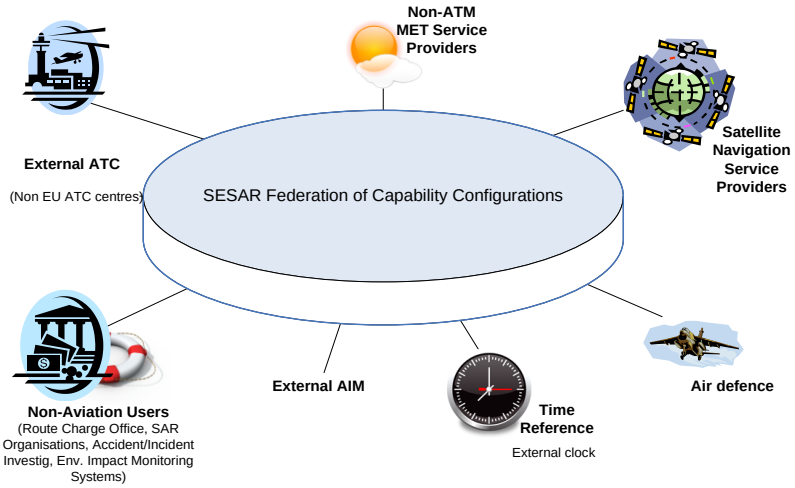


Figure 4 - European ATM System Context Mode (7)

Note: *as part of the further development of this CONOPS, the operational processes between the GAMMA operators (i.e. staff manning the GAMMA solution nodes at different levels, local, national or European, and respective security management functions (e.g. security manager) need to be developed. Conceptually, these roles and function can be modelled as GAMMA users interacting with the GAMMA solution so their responsibilities and operation could change since they could exchange information with the solution. This could impact the decision making process and the procedure to share information. This could be done through dedicated interfaces (for example, security manager interfacing with PDA to endorse operator decision/activity).*

6.2.2 GAMMA Solution Nodes

The GAMMA concept revolves around the establishment of a distributed network of nodes, (related to security), embedded within the ATM system context.

A Distributed (Security) Situation Management System can generally be defined as a collection of independent network nodes (agents) that jointly address the management of a security situation and synchronise their individual actions (and resources).

The GAMMA solution entails a functional / relationship between the identified GAMMA operators and users. Both, operators and users, including associated sub-system interfaces / capabilities can be understood as network nodes which drive the operational information exchange needs between these nodes.

Therefore a GAMMA Node can be defined as any actor (operator and user) and / or technical function designed as part of the GAMMA solution contributing to the joint management of security. The relationship of the individual nodes, e.g. role, level of information exchange, depends on the operations either supported or performed by the node. . This abstraction allows for the delineation of not yet well defined technical capabilities or information (exchange) relationships between different actors.

The nodes which are part of the GAMMA solution are formed by national GAMMA security management platforms and interconnected local (sub-system) security operations for security management and situation / incident management. This CONOPS also conceptualises a node at European level called European GAMMA Coordination Centre for the pan-national exchange and coordination of ATM security related information. Herewith a more detailed description of the different GAMMA nodes is included:

- **Local GAMMA SOC (LGSOC)/Local security systems** – the level of a security (sub-) system interconnected to the national security management platform (SMP) and/or the GAMMA network.
    - A LGSOC ensures the local GAMMA operator having access to the GAMMA solution capabilities and providing defined information feeds to the national GAMMA SMP / network defined in this document in terms of continuous dynamic security management for controls deployed or available at local level, and the associated situation management functions. A LGSOC is the principal fusion center for monitoring data on the supporting assets and respective controls.
    - The local security systems are the current or future ATM systems that address security aspects. They operate independently on the systems proposed within the GAMMA solution and they could even be only procedures. The main feature of the “local security systems” within GAMMA solutions is to send information either to the LGSOC or directly to the NGSMP.
- **National GAMMA Security Management Platform (NGSMP)** – This node is the national reporting center for a set of LGSOCs belonging to the corresponding nation. It is also operated by a GAMMA operator. This level may be provided with additional control capabilities for the continuous dynamic security management which are not available on local level or complement the local level. Dependent on the national context, these centers may serve as the focal point for dedicated collaborative support related information exchange. NGSMPs serve also as the control node for GAMMA services, e.g. cyber intelligence, national data fusion, security alerting, threat prediction, etc.
- **European GAMMA Coordination Center (EGCC)** – This node represents the European-level reporting and coordination center for ATM security operations. It exchanges information with the NGSMP and it is managed by a GAMMA operator. Its features are very similar to the NGSMP (for example cyber intelligence information, security alerting and prediction) but services for undertaking decisions are not implemented since this node mainly acts as an advisory and dissemination centre. Another difference is that the information received is previously treated and filtered at the national node.

The implication of the GAMMA solution is that the aforementioned GAMMA nodes require an underlying communication infrastructure (i.e. network) with associated information dissemination scheme.

From that perspective, the GAMMA solution can be conceptualised as a network of distributed nodes embedded within the ATM system and providing interfaces to (ATM-) internal and external security stakeholders. A specific set of these nodes (for example, security operation centres) is providing interfaces and technical support to the GAMMA operators. On the national level this is represented by the GAMMA security management platform.

Dependent on the national / local decision-making process / procedures supported by the GAMMA solution, support of the respective function (e.g. security manager of ANSP) shall be ensured by the GAMMA solution for the purpose of collaborative support. GAMMA shall also devise information services to interconnect stakeholders on the basis of agreed procedures / processes and information needs (i.e. 'need-to-know' principle).

Note: *The sub-set of demonstrated / validated GAMMA capabilities requires the definition of process / procedure related data / information exchange needs between the different GAMMA nodes and interfacing users. This shall conceptually be covered by the scenarios driving the GAMMA validation.*

The GAMMA solution is targeted at an intelligent push, i.e. situation management related information dissemination, across the different levels of operators.

GAMMA users will be provided with relevant information concerning the ATM system state, its service assurance, and further information related to their profile articulated in form of the need-to-know principle.

For the purpose of this CONOPS a distributed network (i.e. GAMMA organisation, spanning the GAMMA operators and users) is envisaged as in the figure below:

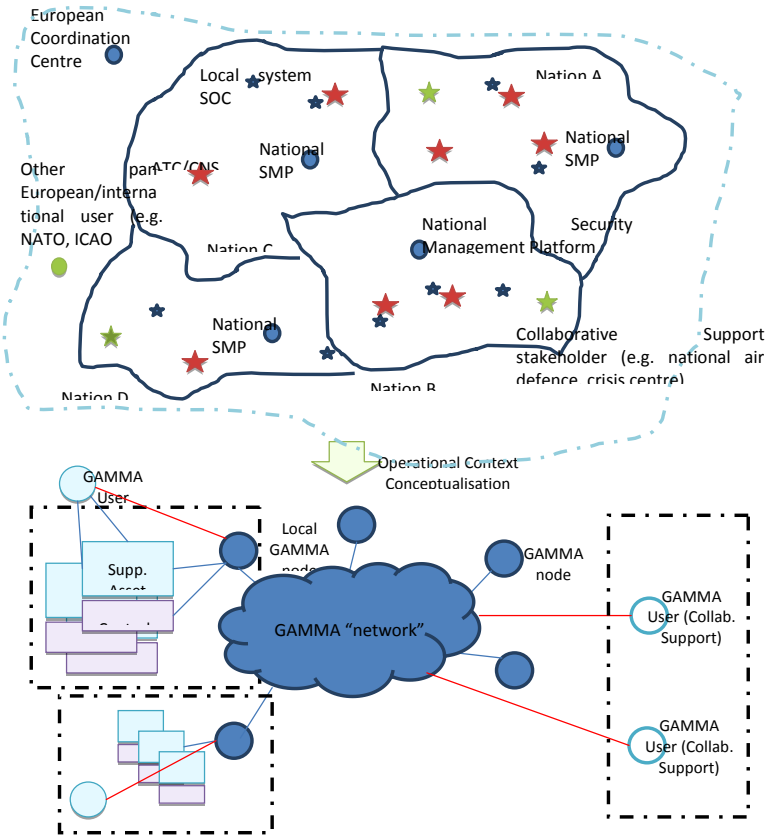


Figure 5 – GAMMA Distributed (Security) Situation Management System network

Note: *The "lowest" level of a GAMMA node is represented by the local security (sub-system) operation centre. This allows for national variances in implementing the procedural, organisation, and technical control of security controls embedded within the ATM/CNS infrastructure (~sub-) system component level (i.e. supporting asset level).*

Dependent on the prevailing data / information sharing policy, the local SOCs are either connected directly to the respective national security management platform or via the GAMMA networking capability (i.e. network and information dissemination system).

Among all the terminology previously mentioned, there are two terms that deserves an special treatment since they can be found out confusing due to the few but important differences between them. They are: Security Operation Center (SOC) and Security Management Platform (SMP).

6.2.2.1 Differences between Security Operation Centre and Security Management Platform

The concept of a Security Operations Center (SOC) is mainly focused to provide services for the security of Information Systems of an organization, providing also Incident Response capabilities.

To provide such services, a SOC uses SW/HW component dedicated to monitor the IT structure in timely fashion manner, in order to promptly identify intrusion attempts, attack or misuse of systems. Even proactive tasks can be performed in order to improve the security level of the organization (security assessments, vulnerability assessments, early warning, security awareness).

The concept of a Security Management Platform is wider. It has the aim to cover any kind of security threats and any scenarios (including the global ATM security scenario) beyond the self-protection concept, enabling the collaborative support.

While SOCs operate at "tactical" level, the Security Management Platform provides a "strategic" level where data provided by SOCs or by any Security Systems are fused, correlated and enriched with information provided by other sources (i.e. the Web) in order to obtain a cooperative environment in which attacks can be predicted, avoided and possibly controlled and countered by operating with a comprehensive view of the network and of the security situation.

To achieve these goals, the Security Management Platform incorporate function such as Cyber Security Intelligence, Attack Effect Prediction, Decision Support and Dissemination Capabilities, other than provide the Global Situation Awareness of all the connected systems, in the light of Critical Infrastructure protection concept.

6.3 GAMMA Solution Interfaces and Boundaries

The GAMMA system context is described by ATM system context and the dual nature of ATM Security. Accordingly, the GAMMA solution interfaces with the classical ATM stakeholder community and needs to establish additional interfaces to collaborative support stakeholders (part of the GAMMA users).

The GAMMA WP2, WP3, and WP4 deliverables provide a presentation of the GAMMA solution system interfaces. In particular, the GAMMA ATM reference models provide extensive listings of roles and system-to-system interfaces, both internal and external systems.

6.3.1 Collaborative Support

As defined by SESAR / ICAO Doc 9985, collaborative support is the provision of services or information from ATM to another agent such as law enforcement, military agencies, emergency services or incident investigation agencies relating to aviation security (i.e. an act of unlawful interference) or other national/international security.

Collaborative support is a function of ATM in that is pre-planned and coordinated between ATM and outside agencies. It concerns situations which, to a certain extent, are preconceived, rehearsed and well understood (such as hijacks, entry into restricted airspace, large scale system degradations) and where principles of operations are reflected in the national agreed processes and procedures between the respective parties. These form the basis for even non-rehearsed situations.

Therefore each party in the activity understands their role and those of the other parties. Procedures are coordinated and have been rehearsed; some procedures may be local whilst others coordinated at regional or international (e.g. ICAO) level. (8)

The GAMMA solution ensures the collaborative support capability through interfacing with organisations in support of their tasks addressing and responding to aviation security (or other national security) incidents.

Note: *Collaborative support stakeholders (i.e. external stakeholders defined within GAMMA users) are outside of the security boundary of GAMMA system of systems and the associated external interfaces of the GAMMA solution have to be secured in a manner commensurate to the need and in accordance with the prevailing regulatory requirements. Information exchange between the GAMMA organisation and collaborative support stakeholders (i.e. external stakeholders within GAMMA users) is based on the 'need-to-know' principle.*

The following list of entities/actors will be cleaned up and further developed in WP3. In principle, the list should be understood as an "e.g." listing rather than a comprehensive list. As part of the coordination tasks surrounding the further development of this CONOPS it is planned to coordinate a comprehensive "actor model" for GAMMA.

GAMMA solution will have to specify (and implement) the information exchange between the GAMMA components and these agencies:

- Interfaces with the National Security Authorities listed below:
  - SOC of National Critical Infrastructures, the centre includes the management of critical national assets: Smart Grid, Communication Provider, Railways systems, etc.
  - SOC of National ATM system, (as will be defined in SESAR and Gamma security risk assessment and treatment);

    Note: *this needs to be reviewed: The GAMMA hypothesis is that there is one national level security management platform for ATM security. In principle this is a self-reference.*
  - National Civil Aviation Authorities (ENAC, UK CAA, Luftfahrtbundesamt (LBA), Direction générale de l'aviation civile, AESA, ...);
  - Military National Authorities (Aeronautica Militare Italiana, Royal Air Force, Luftwaffe, Armée de l'air, Ejército del Aire, ...).

    Note: *there is a general misconception about the provision of air traffic related information to national authorities for the purpose of the identification of civil aviation. The latter is governed by the provisions of ICAO and framed by the national sovereignty and associated rules for providing flight related information to – for example – national air defence. From a collaborative support perspective, "other" incident related or supporting information complementing the aforementioned flight-related information can be envisioned.*
- Interface to EU Security Authorities or relevant European / pan-national level organisations / entities:
  - European Aviation Crisis Coordination Cell;
  - EU Military Authorities (EDA, NATO, Eurocontrol,…).
- Interfaces with International Security Agencies:
  - NextGen Security Authority;

- Other Regional Security Authorities for Critical Infrastructures.
  Note: *dependent on the modelled processes / procedures and identified 'need-to-know' principle.*

Since Militaries entities and roles have been especially assessed within GAMMA project, it is worth dedicating one specific section in order to detail how the communications and interfaces are expected to be. This information come from the Task 3.5 which is the first task addressing military security aspects and how is and how is expected to be integrated within GAMMA solution.

6.3.1.1 Military interoperability and integration

Before starting to define how interoperability between civil and military is expected to be, a complete description of systems available for the management of security threats is presented. These tools are used to support Aircraft Renegade and Hijacking attacks as well as the related procedure interoperability among the States.

- **Civil-Military ATM Coordination Tool (CIMACT)**: The Civil-Military ATM Coordination Tool (CIMACT) is developed by EUROCONTROL as a common co-ordination system to exchange information between civil and military units. The proposed CIMACT improvements are based on the Airspace Security Incident Management (ASSIM) concept described by NEASCOG. The Civil-Military ATM Coordination Tool (CIMACT) currently provides situational awareness used for Civil-Military Coordination, traffic identification, airspace security.
- The **European Aviation Crisis Coordination Cell (EACCC)**: EACCC is used to face important crises (its role is only coordination, as the management of the crisis remains in the remit of each State). Any type of incident that can affect aviation is in the scope of EACCC, which performs one exercise each year (e.g. volcanic ashes, cyber-attack, FDP malware, etc).The aim of the exercises is to contribute to minimize the impact of the incident on the European ATM Network.
- **NATO Integrated Air Defence and Missile System (NATINAMDS)**: In the case of a country which is part of NATINAMDS and which uses this system for airspace security incident management, arrangements concerning ATM security are in place between the military authorities of different countries.

Civil-Military Operational Systems (CMOSs) such as CIMACT tools implementing the ASSIM concept are predisposed to activate and coordinate Civil and Military interoperability during the security event management, as described in D3.2 "as-is situation" section.

The GAMMA solution is designed to collect security information relating to National and European levels so as to support a GAMMA User during incident management operations. Associating the GAMMA security information with the solution derived from the ASSIM concept would open the way for a more complete situational awareness covering both military and civil environments.

The capability to combine the flow of information derived from the GAMMA solution with CMOSs would therefore lead to a broader level of correlation enhancing the level of alerts.

A complete situation awareness view would for instance allow CMOSs operators to correlate a suspected renegade or hijacking event with a concomitant ATC cyber-attack.

Following this approach, the National GAMMA Security Management Platform (NGSMP) could send information (attack predictions, attack impact, countermeasures) to National Civil Military Operational Systems using the Gamma Information Dissemination (IDS) capabilities.

These GAMMA reports should respect the current CMOSs chain of command and procedures (i.e. ASSIM MoU among States) so as to facilitate the implementation of this vision in the current military environment.

The vision outlined above will be elaborated further within the GAMMA activities relating to Task 3.1 with the aim of proposing a more complete integration of the Civil-Military Operational systems described in the D3.2 document with the overall GAMMA solution.

Moreover, specifically improvements, depending on their nature, will be taken into account in: ATM Security Management Framework Definition (T3.1), Roles and Responsibilities in a Global ATM Security Management System (T3.2), International Cooperation (T3.3) and Human Factor and Training (T3.7).

6.3.2 GAMMA Network

6.3.2.1 Principles

Throughout the previous sections the following communication related principal capabilities have been identified.

- No processing of marked (i.e. classified) information via GAMMA capabilities. Data / information that may stipulate organisation / national level “sensitive” data shall be sanitised before exchanged via the GAMMA network.
- Need-to-know principle. Information exchange with other national SMPs, LGSOC, the European GAMMA Coordination Centre, and GAMMA users will be based on a set of node-specific data sharing policies in support of the identified operations. The principal means for enforcing the policies is the information dissemination system as a GAMMA networking capability. Sanitising of sensitive information shall be performed on the level of the respective national SMP.
- In support of cross-border or pan-organisational information exchange, the data sharing policies deployed by LGSOCs or collaborative support stakeholders (i.e. external stakeholders within GAMMA users) may differ (i.e. more open vs more restrictive information exchange). This is a local / national decision and depends on the operational procedures developed as part of the GAMMA developments.
- For the information exchange via the GAMMA network, standing practices / standards within ATM shall be re-used to the maximum possible and incentivise the deployment of GAMMA interfaces / capabilities (e.g. reasonable customisation effort potential).

6.3.2.2 Conceptual information relationships between GAMMA operators and users

This section will be further developed and refined about the understanding developed in WP4 (and others as appropriate).

6.3.2.3 Information Relationship of Supporting Assets / GAMMA prototypes

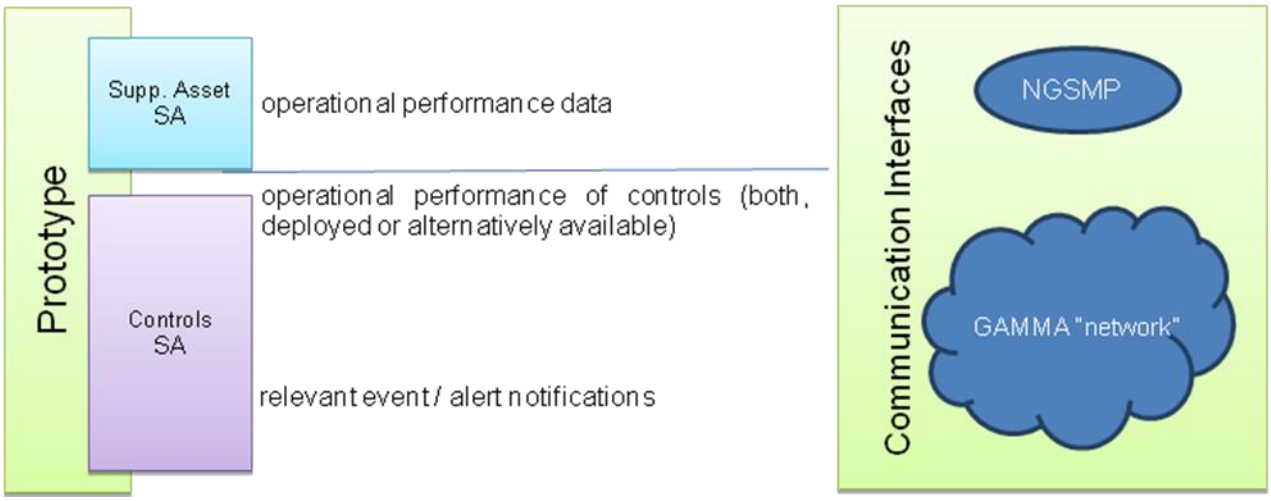


Figure 6 – GAMMA Principal Information Relationship

The general aim of GAMMA is to validate and demonstrate security related capabilities on the basis of a subset of sub-system capabilities. From that perspective, the prototype represents a supporting asset within the scope of risk assessment.

The following principal information / interface requirements can be identified within the scope of GAMMA:

- (abbreviated) operational performance and status of the supporting asset;
- operational performance of the deployed security control (which in itself represents a supporting asset).
  This data / information is also required for deployable security controls.
- event / alert notification messages.

Note: *across the GAMMA documentation, there is no reflection so far on the "content" of information relationships between GAMMA network nodes. In particular, the information concept as regards security controls needs to be further developed. For the time being, a general purpose model expressing the 'services' provided by a security control in terms of confidentiality, integrity, and availability shall be applied. This may need to be refined with the on-going maturing of the information exchange model in WP3 and WP6.*

6.4 GAMMA Operation Modes

The GAMMA solution is conceptualised as an embedded security function within the air navigation system comprising a distributed network of nodes and spanning GAMMA operators and users (c.f. CONOPS, 6.2.2, and Figure 5). These nodes interact in three principal operation modes, i.e.

- normal operating mode;
- situation / incident management operating mode;
- collaborative support.

As part of the standard operations, local processes / activities can be distinguished from joint operations performed by a subset (i.e. a collection) of GAMMA actors (operators and users).

Three principal operation modes and a support mode can be differentiated:

- **normal operating mode**
  - continuous operations relate to the 24/7 operations of the security management component for the establishment of "security situational awareness"
    - basic continuous monitoring of the operational performance and technical status of the respective ATM system component (i.e. supporting asset);
    - basic continuous monitoring of the operational performance (possibly expressed in terms of security services for confidentiality, integrity, and availability.
      ***Note**: to be further defined as part of validation / prototype development;*
    - Processing and coordination of the security coordination messages shared on the national level, or shared across the GAMMA network.

  - aperiodic operations – are currently scoped out of the GAMMA developments and - relate to maintenance related activities for the day-to-day management of the security management component.

- **situation / incident management operating mode**
  - this mode refers to the handling of attacks and its repercussions on ATM supported by GAMMA, including 'preventive' (additional) action as part of the coordination on-going across the GAMMA network
    - in-situ identification and assessment of (observed) threat propagation, risk / impact containment, and deployment of alternative security controls;
    - launch of situation / incident information exchange across the respective nodes in accordance to the GAMMA supported processes and procedures.
      ***Note**: a user-comment identified the need to support ANSP organisation level decision-making by security managers. At the time being there is no mapping between the 'standard operations' and the 'operations requiring endorsement'. This needs to be taken up as part of the refinement of the aforementioned operations.*

- **collaborative support mode**
  - The principal understanding of the dual nature of ATM Security and the definition of operations from SESAR and ICAO Doc 9985 have been introduced in section 6.3.1. This mode refers to the management of the security activities from the perspective of ATM as a whole and taking into account external GAMMA users, i.e. not exclusively-related to ATM. They can however play an important role in the pre-incident and post-incident phases improving radically the security management system.
  - Collaborative Support represents a specialisation of the Security Situation Management Operation defined in section 7.2 revolving around airspace security incidents.
    ***Note**: The GAMMA CONOPS / project scope is currently not envisioning collaborative support functions to 'widen aviation security or national security incidents beyond the classical ATM scope. For example: 'wider' aviation security incident: bomb threat at airport or within terminal*

building; 'wider' national security incident: mass political protests including vandalism which may impact the safe operation of air traffic.

- **support mode**
  - This CONOPS does not specify in detail the support concept and environment for the GAMMA solution. Pointers such as training and simulation will be addressed within GAMMA project. More concretely within Task 3.7.

In summary the main modes of operation addressed within GAMMA will be **normal operating** (continuous operations), **security incident management** and **collaborative support** modes. **Support** Mode will be further addressed within Task 3.7 and it will be out of the scope of the validation and verification tasks.

7 Operational Environment

This chapter describes the operational processes and operations and their dynamic flow and/or sequence of operations. This dynamic description of the system will be further detailed in particular operational scenarios for the envisaged GAMMA prototypes.

In alignment with SESAR (8) the dynamic spectrum is defined around the "Incident Preparedness and Operational Continuity Management" (IPOCM) timeline as presented in Figure 7. The IPOCM timeline can be broken down into the following phases:

- pre-incident (i.e. prevention, preparedness, dissuasion, and detection / monitoring);
- post-incident (i.e. detection, reaction/response [i.e. emergency response, continuity response, recovery response], and post-incident analysis / forensics.

This timeline is generic enough to frame the situation management concepts of the three basic types of situation management (i.e. predictive, control, and investigative) to describe the activities / processes between a collection of GAMMA actors. It is worth mentioning that apart from the phases taken from the IPOCM, some additional phases have been added to enhance the granularity needed to categorize the different controls/requirements to be defined within GAMMA (i.e. dissuasion or post-analysis forensics phases).

All in all the timeline can be broken down into the following distinct phases:

- Pre-incident
  - Prevention/ Avoidance – preventive measures to ensure the operational objectives, i.e. preventive security controls deployed for the respective supporting asset; and
    - Preparedness – (available ["ready to be deployed"] or deployable ["controls can be established within reasonable time frame"]) preventive controls[4].
  - Dissuasion: Measures to be developed in order to dissuade the attacker to undertake any malicious act.
  - Detection (pre-incident): Measures to assess the available information (status of the supporting assets, logs or faults) in the different systems. This phase will allow identifying possible malfunctioning or faults that can develop to real attacks. Potential, suspicious or also real attack can be reported. The time at which a real attack takes place is called "time of incident".

- Post-incident:
  - Detection (post-incident): Measures to assess when a security attack has/is being taken place. They can usually be the same measures than in the pre-incident detection phase, but they are structured in this way in order to be consistent with the pre-post incident timeline.
  - Reaction: Countermeasures to be taken in reaction to one attack. They can be split by the timeframe in which this response is given:
    - Emergency Response – the initial / immediate response to the incident
    - Continuity Response – (available) processes, controls and resources are made available to ensure the continuity of the critical objectives (i.e. ensure ATM service provision to be safe[5] and provide required collaborative support)

[4] The deployment of preparedness measures may be triggered due to heightened security (alert) states.

- Recovery Response – resources, processes, and capabilities of the ATM system or the GAMMA solution, i.e. respective supporting assets, are re-established to meet regular operations.

- [6]Post-analysis forensics – resources and processes to review and analyse the performance, including refinement of processes / procedures once the attack has happened and the normal situation has been recovered.

Note: *The scope of the GAMMA project is focussing on prevention, detection, and emergency reaction.*

Conceptually, long-term recovery can be supported by the same capabilities and processes designed / defined by GAMMA. However, this is perceived as out-of-scope of the project.

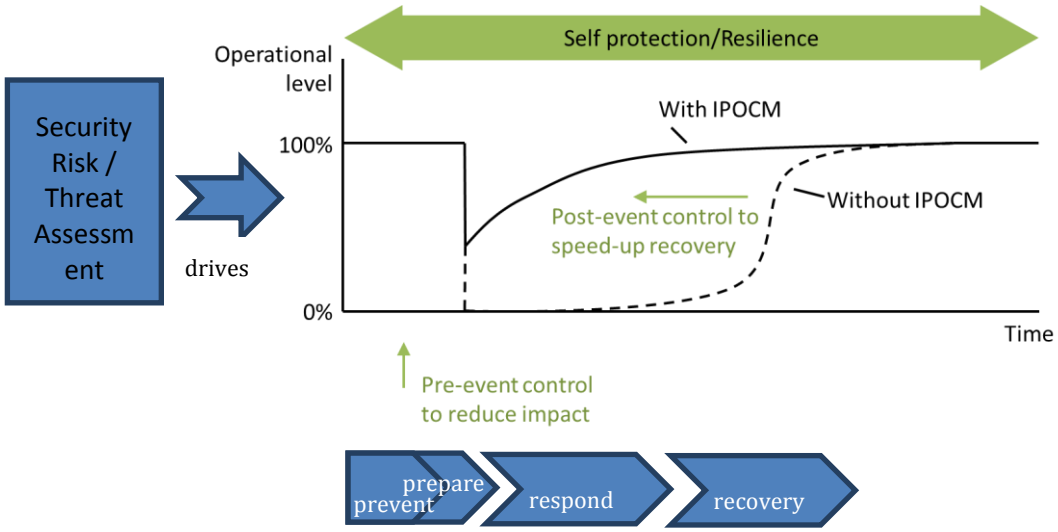


Figure 7 – Incident Preparedness and Operational Continuity Management7

Throughout the following sub-sections, the GAMMA operation modes and timeline phases as listed above will be mapped with a view to (re-)define the operational processes and operations. The mapping is performed as a matrix spanned by the two dimensions for the local context and joint action by a collection of GAMMA actors. These two dimensions are the two operational environments considered within GAMMA:

- **Continuous Local Security Management Operation** which describes the local activities foreseen to address and react with security events taking into account the approach proposed within GAMMA.
- **Security Situation Management Operation** which is focused on how the reaction to security activities should be performed since a higher level point of view involving to different roles, either external such as internal. These activities will thus be part of what is called “joint action” and they are hence all related to collaborative support management.

[5] The main objective of ATM is to provide separation (safety) and synchronise air traffic (capacity & efficiency). In an emergency / continuity response set-up, safety overrides all other aspects. Similarly, collaborative support functions shall be established asap to ensure ATM’s contribution.
[6] Originally not included in the scope of GAMMA now it is proposed to be included.
[7] It has been adapted from SESAR 16.06.02 Reference Material

7.1 Continuous Local Security Management Operation

The principal concept stems from the continuous monitoring of the "local" security situation and the action in response to the changes of the security situation (i.e. local incident management). The principal outcome of this operation is situational awareness for GAMMA operators including the situation dependent deployment of (additional / alternative) security controls.

Note: *related concepts / terms cross-referenced within the GAMMA documentation include: security risk management (in operational terms), crisis / emergency management, service continuity, (system-level) security response. Within these related concepts, the normal operating mode refers to the processes / activities performed in the pre-incident phase, while the local situation / incident management mode refers to the post-incident phase.*

These concepts all describe the capability to monitor the security status of (ATM and GAMMA) system components, the deployed security controls, and address changes to the security status.

Within the GAMMA CONOPS the operations, (described in **Table 1** below) apply primarily to the local GAMMA (sub-) system security operation centre (LGSOC)/Local Security System (i.e. supporting asset level), though information is received, processed, and disseminated to the GAMMA network.

Based on the devised decision-making process, the competence to manage the dynamic deployment of security controls may rest with the LGSOC and / or NGSMP given the local context and agreed modus operandi. The precise modelling of ANSP-level and NGSMP-level decision-making processes (e.g. dependent on observed security situation) will be further developed within the on-going and future GAMMA activities.

Based on the deployed data sharing policies and need-to-know principle, the local GAMMA SOC or local security system (i.e. GAMMA user) shall further:

- receive relevant security information to enrich the local operators; and
- provide relevant security information to the GAMMA network.

The local incident management process closes with incident. Post-incident activities are performed within the subsequent forensic activities.

The local normal operating and situation / incident management operations / GAMMA capability are based on the continuation of the security risk assessment and associated control identification, including the dynamic deployment of controls.

The **Table 1** below shows a summary of the main activities foreseen for the main operation modes structured by the timeline of the security incident.

Operation Mode	Principal Operation	Pre-incident	Post-incident
Normal local operating mode	basic continuous monitoring	establishing (basic) situational awareness on local security situation, operational performance (supporting assets), status of security services (CIA controls & operational state) ***note:*** *the presentation / user interaction is adapted to the respective (sub-)phases*	

Operation Mode	Principal Operation	Pre-incident	Post-incident
	reception, processing of GAMMA message	the local security situational awareness is enriched with received GAMMA messages	
	dissemination of GAMMA messages	the local security system provides the respective information on the operational performance of the SAs, associated controls, and relevant notifications	
Local situation / incident management	in-situ identification (and assessment)		Provision of additional situational information, e.g. alerting, threat prediction
	Local dynamic security management support		Deployment of (additional) technical or operational controls, including local decision support
	Local incident information dissemination		Dissemination of GAMMA incident information (e.g. event, operational status, control status, intelligence) and incident close-out.
	Forensics		Local post-incident investigation and security audit
Collaborative Support	collaborative support information	(*)	Relevant local information dissemination in case the local node is involved in the incident ***Note:*** *non-involved notes may receive updates via the GAMMA messages (c.f. normal operating mode)*

Table 1 – Mapping of Local Operations to Incident Timeline

(*) ***Note:*** *Collaborative support stakeholders form a specific group of GAMMA users (c.f. CONOPS, section 6.2.1.2, and* ***Figure 4****). During the pre-incident phase, these users will receive (and may disseminate) respective GAMMA information as part of the normal operating mode, both locally and in joint operations.*

7.2 Security Situation Management Operation

The principal concept of this type of operation is the joint action by a collection of actors addressing emerging or materialising security (incident) situations. This type of operation is different from the aforementioned operation in that the processes are not triggered locally. For example a software exploit infringes with the operational performance of a supporting asset in an adjacent centre, or a collaborative support role triggers security support processes.

Situation management is defined as a synergistic goal-directed process of (a) sensing and information collection, (b) perceiving and recognizing situations, (c) analyzing past situations and predicting future situations, and (d) reasoning, planning and implementing actions so that a desired goal situation is reached within some pre-defined constraints (10).

Depending on the specific situation, Buford and Jakobson identify three basic types of situation management based on the in-situ situation model:

- Investigative;
- Control; and
- Predictive.

Each of these types has its specific goals and information needs. Investigative situation management is concerned with the retro-perspective analysis why a certain situation evolved. Control-type situation management focuses on the in-situ management of situations, while predictive situation management addresses the projection of possible future situations.

Note: *These types of situation management are described throughout the GAMMA proposal in different forms. For example, classical incident management can be subsumed under the "control" type describing the interactions between the different nodes, including information exchange requirements.*

The Security Situation Management Operations are restricted to in-situ situation management (i.e. control-type operations).

Note: *The GAMMA threat prediction capability envisions a semi-real-time horizon. Thus, a classical predictive situation management as defined above is not entailed within the GAMMA project scope.*

For each of the situation management phase the general management cycle can be applied to drive the interaction between the different GAMMA nodes.

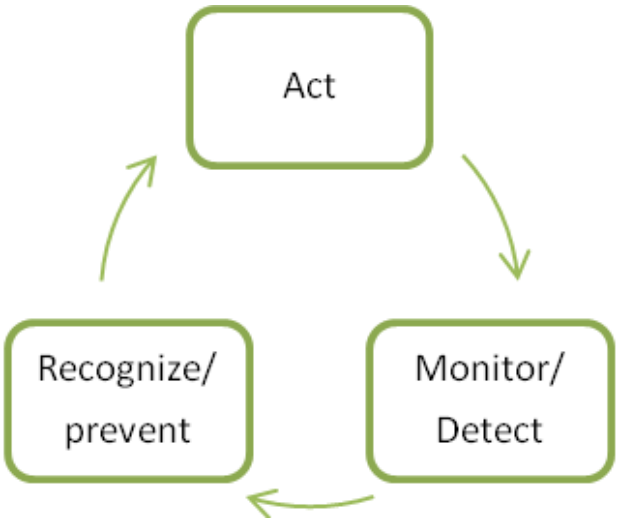


Figure 8 – Management Cycle

The key element of this capability is that the continuous dynamic security management is targeted at the control level. Situation management comprises the interactions between the nodes to tackle operational and non-local scenarios or security threats.

For example, the NGSMP may monitor the occurrence of multiple attacks on similar supporting assets within its area of responsibility (i.e. monitor / detect) or receive conclusive information from adjacent NGSMPs or the European GAMMA Security Coordination Center (EGSCC). The assessment (or threat prediction module) recognises a structured attack against the ATM infrastructure component which will result in operational degradations (i.e. recognise / prevention trigger). The NGSMP alerts all LGSOCs and requires the air traffic service units to apply a different operational procedure (i.e. act).

Note: *Implications for the GAMMA prototype development / validation exercises: While the concept is easily graspable, the devil is in the detail. It is expected that the associated information exchange needs will be identified as part of the architectural work and the prototype developments and adaptations.*[8]

The **Table 2** below shows a summary of the main activities foreseen for the main operation modes structured by the timeline of the security incident.

[8] To be further developed in WP4, WP5 and WP6.

Operation Mode	Principal Operation	Pre-incident	Post-incident
Normal Joint operating mode	c.f. normal local operating mode	c.f. above **Table 1**	
	management of GAMMA information exchange	GAMMA supported information exchange based on the devised operational regimes and data sharing / need-to-know policies. This may include, situation dependent definition of the "collection" of involved actors.	
situation management operation	predictive situation management	Processing of security related information addressing the projections of future changes to the security situation.	
	dynamic in-situ (control) security management	In-situ management of security situations across the GAMMA network or respective subset of GAMMA actors based on prevailing situation/incident.	
	investigative security situation management		dissemination of GAMMA incident information (e.g. event, operational status, control status, intelligence) and incident close-out.
	GAMMA security situation management information exchange	extension of the generic GAMMA information exchange (c.f. above) as concerns situation management related information	
Collaborative Support	collaborative support information	(**)	relevant collaborative support information dissemination for airspace security incidents in accordance with the data-sharing policies

Table 2 – Mapping of Normal Operations to Incident Timeline

*(**) **Note:** Collaborative support stakeholders form a specific group of GAMMA users (c.f. CONOPS, section 6.3.1, and Figure 5). During the pre-incident phase, these users will receive (and may disseminate) respective GAMMA information as part of the normal operating mode, both locally and in joint operations.*

8 Operational Scenarios

Note: *This Chapter needs to be further developed based on the operational concept introduced above, the associated information exchange requirement, proposed GAMMA security processes and procedures, and GAMMA prototype demonstration capabilities.*

8.1 Instantiation of Model based on Airspace User Operations - Flight Phases

Air navigation ensures the safe, efficient, and orderly flow of air traffic. Air traffic, i.e. airspace user intentions, is described in form of trajectories that evolve from initial intentions through refinement steps, culminating in the actual flown trajectories at the day of operation. For the purpose of this section, the actual flown / executed trajectory is considered.

With a view to the European ATM System, different types of abstraction and presentations can be chosen. From a flight / trajectory perspective the following principal phases of flight can be separated:

- en-route portion; and
- approach

This separation is useful to describe two principal operational ATM scenarios within which the distributed GAMMA situation management capability / network shall be embedded and along which dedicated operations (e.g. processes, information relationships, supporting assets, etc.) can be defined without running the risk of generalisation.

The following is a proposal and will have to be refined in light of the WP4 outputs and business platforms and simulation capabilities.

Scenario 1 – en-route

This scenario embraces the multinational airspace comprising (southern) UK, the Netherlands, Belgium & Luxembourg, (northern) France, and (the northern part of) Germany, possibly extending into Switzerland, and Italy.

This area can be considered as one of the busiest volumes of airspace in Europe comprising intercontinental traffic and serving several major European hub airports (i.e. London Heathrow, Amsterdam Schiphol, Frankfurt Main, and Paris Charles de Gaulle).

Scenario 2 – approach

The operational context of an approach scenario is developed for a generic airport and terminal area context. Approach (and departure) services are generally provided within a defined volume of airspace around the aerodrome (or set of closely collocated aerodromes).

Given the prevailing airspace structure or air traffic characteristics this volume of airspace may be termed “terminal airspace”. For the purpose of this paper, a generalised “cylindrical” airspace of (e.g.) 40NM is assumed to cover the respective approach / departure and aerodrome control services.

8.2 Security Incident Scenarios

The basic operations for the GAMMA solution have been described (and will be refined) in several documents. Related conceptual operations are already identified in this CONOPS. Although the main content related to the GAMMA concept operations is included within WP4 activities (GAMMA security requirements and GAMMA architectural model).

At the time being the set of the most dangerous threat scenarios are developed. In fact, Task 4.2 has produced a threat model based on the threat scenarios coming from WP2. These models give information

about how some security attacks are currently being managed. Based on them, the security incident scenarios envisage how these scenarios are managed taking into account the approach performed within GAMMA.

The aim of these security incident scenarios is to demonstrate how the security management is improved since GAMMA solution (nodes and roles) takes place within ATM environment.

According to the operational environment two different security incident scenarios can be described:

- *Continuous Local Security Management Operations* (See more in section 7.1): these scenarios will be focused on the security events triggered at local level. The scope of the actions could be only limited to local level (LGSOC/local security system) although interaction or exchange of information with the National level (NGSMP) or European level should be detailed if needed.
- *Security Situation Management Operation* (See more in section 7.2): these scenarios will be triggered by the joint action of other roles which are related to the collaborative support activities.

Based on the instantiation of the aforementioned operational scenarios, the security incident scenarios must include at least:

- flight phase addressed,
- a mapping of the threat scenarios,
- information exchange requirements,
- modes of operation addressed, (see more in section 6.4),
- operational environment addressed
- associated security operations and processes
- roles and responsibilities involved within these scenarios
- expected improvements to be found

The detail of the scenarios to be used during validation activities will be done as part of the development of the WP5 Validation Plan.