SECURITY SITUATION MANAGEMENT – DEVELOPING A CONCEPT OF OPERATIONS AND THREAT PREDICTION CAPABILITY

Denis Kolev, Rinicom, Lancaster (United Kingdom)
Rainer Koelle, Lancaster University, Lancaster (United Kingdom)
Rosa Ana Casar Rodriguez, Isdefe, Madrid (Spain)
Patrizia Montefusco, SELEX, Napels (Italy)

Abstract

This paper addresses a collaborative security situation management capability for air navigation. In particular, we formulate the development of a threat prediction capability as a situation management problem mapping the concepts of situation awareness and information fusion. Air transportation and air navigation is undergoing a fundamental transformation. This also requires novel approaches to system security and the management of security incidents across a network of actors. The Global ATM Security Management project addresses this problem space. The work reported in this paper, conceptualizes a security function that supports the management of security incidents on a local, national, and regional level supporting the collaborative effort of classical air traffic management stakeholders and security stakeholders. The security function is based on a network of distributed nodes and capabilities. One such a capability is the threat prediction model. This component is based on a representation of the (sub-) system context as a network of supporting assets, event detection sensors, and associated security controls. Based on the description of the (sub-)system context as a sequence of situations, the threat prediction capability addresses the identification of a security incident and its potential impact as an optimization problem. This paper reflects the work of the first year of the project. In particular, it demonstrates the general feasibility of the approach and the further modelling and preparatory work for further validation activities.

Introduction

From the beginning of the 21st century, aviation has been undergoing a continual transformation with novel technologies being readied for deployment in ground-based, airborne and space-based systems. Throughout the past decade, the security of the air navigation system has become more prominent [1]. Today, efforts are ongoing to embed security risk management into the overall system engineering approach in air traffic management system development. However, the political goals and priorities for transformation programs like SESAR and NextGen put a strong emphasis on the early deployment of operational concepts and technological enablers with little focus on the identified security threats and emerging vulnerabilities stemming from these developments.

One particular research gap is the lack of a system-wide collaborative security function to support the decision-making in terms of security across the different air navigation system stakeholders. The Global ATM Security Management (GAMMA[1], http://www.gamma-project.eu/) project, funded under the 7th Framework Program of the European Commission, stems from the growing need for targeted research in addressing this capability gap.

Initial work on a collaborative security capability has been conducted as part of pan-European research projects, for example, SAFEE – Security of Aircraft in the Future European Environment, PATIN – Protection of Air Transportation and Infrastructure, and ERRIDS – European Regional Renegade Information Dissemination System, an initial NATO/EUROCONTROL demonstration project. Similar research efforts have been reported in the United States [2]. However, the results are not carried forward under the umbrella of the on-going transformation programs SESAR and NextGen.

---

[1] GAMMA, http://www.gamma-project.eu. The research leading to the results presented in this paper has received funding from the European Union's Seventh Framework Programme under Grant Agreement n° 312382.

The GAMMA approach builds on the opportunities opened by a collaborative framework for managing security. The project activities flow from a comprehensive security risk assessment enabling the definition of requirements and architecture components for a comprehensive set of security capabilities in the future air navigation system [3].

This paper addresses a collaborative security situation management capability for air navigation that allows for the dynamic identification and assessment of security threats, and the coordination of security measures. The security function is formulated as a situation management problem and the associated threat prediction capability is based on a network of security information nodes formed by the air navigation system components. Both modelling approaches support a deployment strategy for such a security capability in future air traffic management contexts like SESAR and NextGen that are complementary to current developments and can be easily embedded.

This paper is organized as follows: Following this introduction, a short overview of the state of ATM security is given. The third section introduces the modelling approach. Next, the threat prediction capability is described. Then a short discussion of our results is presented. The paper closes with conclusions and recommendations for further work.

Background – State of ATM Security

Operational Risk Assessment and Emerging Regulatory Requirements

Operational risk assessment is not a fundamentally new approach in aviation or air traffic management. However, the classical approach to operational risk encompassed the concept of safety and the identification of system-inherent risks (e.g. human error, technical reliability). Security considerations were primarily focused on contributions of the air navigation system to national security and defense.

In the aftermath of September 11th 2001 and major outages of public services (e.g. electricity grip, public transportation), increased efforts were undertaken in the identification of adequate security measures and the protection of critical infrastructures. Within this context the criticality of the air navigation system has been confirmed and service providers have been mandated to implement security management systems.

In Doc 9854, ICAO defines the expectation for air navigation security as one of the eleven key performance areas [4]. In the European Context, the European Commission adopted this requirement in the Single Sky Regulation (i.e. EC Reg. 2096/2005, 1035/2011) and ECAC included a recommendation on ATM Security in Doc 30. EUROCONTROL in close collaboration with its stakeholders developed an initial ATM domain-dependent Security Management System and Security Risk Assessment Methodology as principal guidance in this field. This initial work served as an input to the SESAR Definition and Development Phase and the recently developed ICAO Manual on ATM Security, Doc 9985 [5].

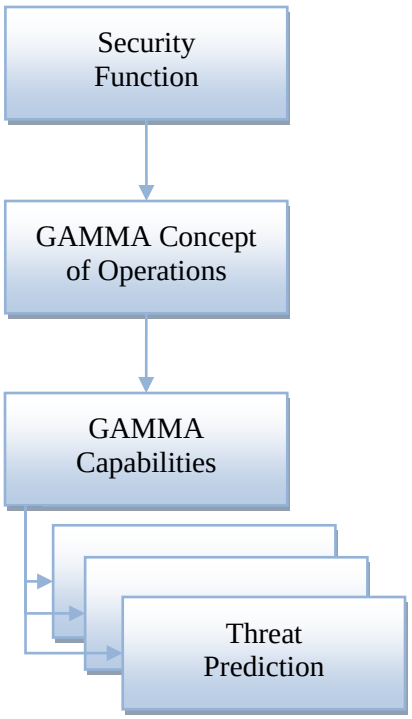
Current Developments

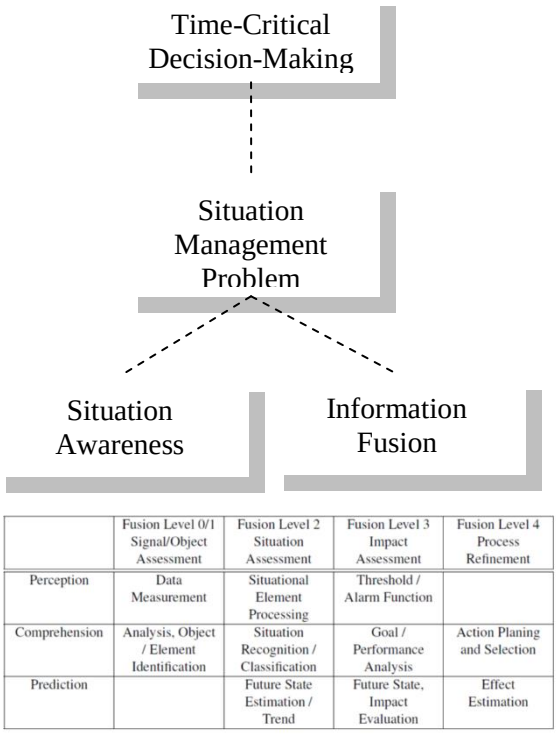
In Europe, SESAR is now moving into the deployment phase. In June 2014, the European Commission adopted implementing regulation IR716/2014 identifying six air traffic management functionalities to be deployed by a specific date. The associated implementation plan is established and managed by the newly created SESAR Deployment Manager (SDM). The SDM released its Deployment Programme Version 1 in June 2015 defining 44 families of implementation projects and their priorities for the 2014-2020 time horizon [6].

Though the SDM program recognizes the relevance and role of security, little effort has been undertaken to embed security into the system-development life-cycle or require a specific security function or supporting capabilities. References to security are typically on the technological level. For example, the SDM Deployment Programme vaguely requires security measures for certain projects with a view to ensure continuity of system operations.

GAMMA Project

The lack of a security function and its thorough implementation across the air navigation system and the current transformation programs has been identified by other research (c.f. above). GAMMA addresses this void and is designed to develop solutions to emerging security vulnerabilities of air





	Fusion Level 0/1 Signal/Object Assessment	Fusion Level 2 Situation Assessment	Fusion Level 3 Impact Assessment	Fusion Level 4 Process Refinement
Perception	Data Measurement	Situational Element Processing	Threshold / Alarm Function	
Comprehension	Analysis, Object / Element Identification	Situation Recognition / Classification	Goal / Performance Analysis	Action Planing and Selection
Prediction		Future State Estimation / Trend	Future State, Impact Evaluation	Effect Estimation

Figure 1. GAMMA Problem Space Mapping

navigation and provide validated proposals for the implementation of these solutions.

The GAMMA project stems from the growing need to address security threats to air traffic management / air navigation in a consistent manner. The security solutions proposed by GAMMA build on the principles and concepts related to security management in a collaborative multi-stakeholder environment. The proposal emerges from a detailed assessment of ATM security threat scenarios carried out in full compliance with SESAR methodologies and building on its results [3].

In that respect, GAMMA fills the void and complements SESAR, with a concrete proposal for the operational use of innovative technological enablers establishing an ATM security function as an additional service in the air navigation system.

Modelling the Security Function

Figure 1 depicts the modelling approach employed in this paper. In particular, we describe the security function of the air navigation system as an application of time-critical decision-making. The subsequent situation management problem is then described by the functions, modes of operations, and supporting capabilities of the GAMMA concept of operations. In this paper, we discuss one of the GAMMA capabilities, i.e. the threat prediction, as a mapping of two situation management concepts: situation(al) awareness and information fusion.

Air Navigation System Security Function

During the preparatory work for the SESAR Definition Phase, a novel definition for the term ATM Security emerged as it was recognized that the classical understanding of aviation security and the associated primarily supporting role of air navigation did no longer meet the future requirements. Today, ICAO Annex 17 and Doc 9985 both recognize the role of air navigation service providers and stakeholders within the wider field of aviation security. ATM Security is now defined in two dimensions:

1. self-protection and resilience of the air navigation system; and

2. collaborative support to other aviation system stakeholders.

This definition allows for a first conceptualization of an ATM Security Function (c.f. Figure 2). The primary purpose of air navigation is to ensure the safe, orderly, and efficient flow of air traffic. Accordingly, a security function needs to ensure the security of the associated air navigation systems and services to the airspace users and all participating stakeholders. From a self-protection/resilience perspective, the dynamic management of security across the air navigation system requires a security management capability that is an embedded function within the air navigation system.

This paper refers to function as the operational, procedural, and technical means to realize a desired system capability. Understanding the set of security solutions as a function allows for a clear separation from sub-systems or system components while establishing a clear interface within the air navigation system context and relevant internal security actors.

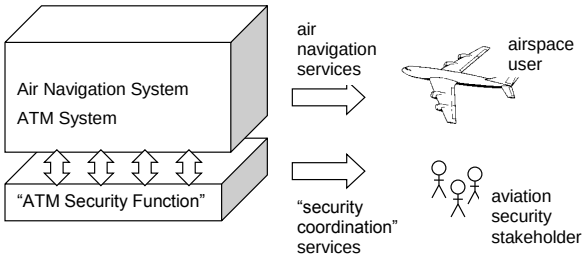


Figure 2. Security Function Concept

GAMMA Concept of Operations

The overall purpose of the GAMMA project is to demonstrate a comprehensive approach to ATM security by providing a concrete proposal for the implementation of capabilities to address and manage security risks in a dynamic and collaborative multi-stakeholder context (i.e. GAMMA organization). This requires for

1. 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.

2. collaborative support
- the provision of appropriately sanitized 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 synchronization of air traffic, and provision of incident support related information.

The security function conceptualized by GAMMA is a network of GAMMA operators and users, including local security (sub-)systems or system security functions, representing a network of distributed nodes embedded within the air navigation system. Next to this organization and set of technical functions, the GAMMA concept builds on a tailored information exchange between the different nodes on three principal levels:

- local – local security (sub-)systems or component embedded in the ATM/CNS infrastructure or a specific local GAMMA security operation center supporting the integration of local level information with GAMMA network wide information and support functions;
- national – the national reporting center for a set of local GAMMA security operations centers. 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; and
- pan-region/European – pan-regional reporting and coordination (e.g. European GAMMA Coordination Center).

Figure 3 presents the security situation management network for a generic four state context and how this context can be conceptualized forming a network of distributed nodes embedded in the current air navigation system context.

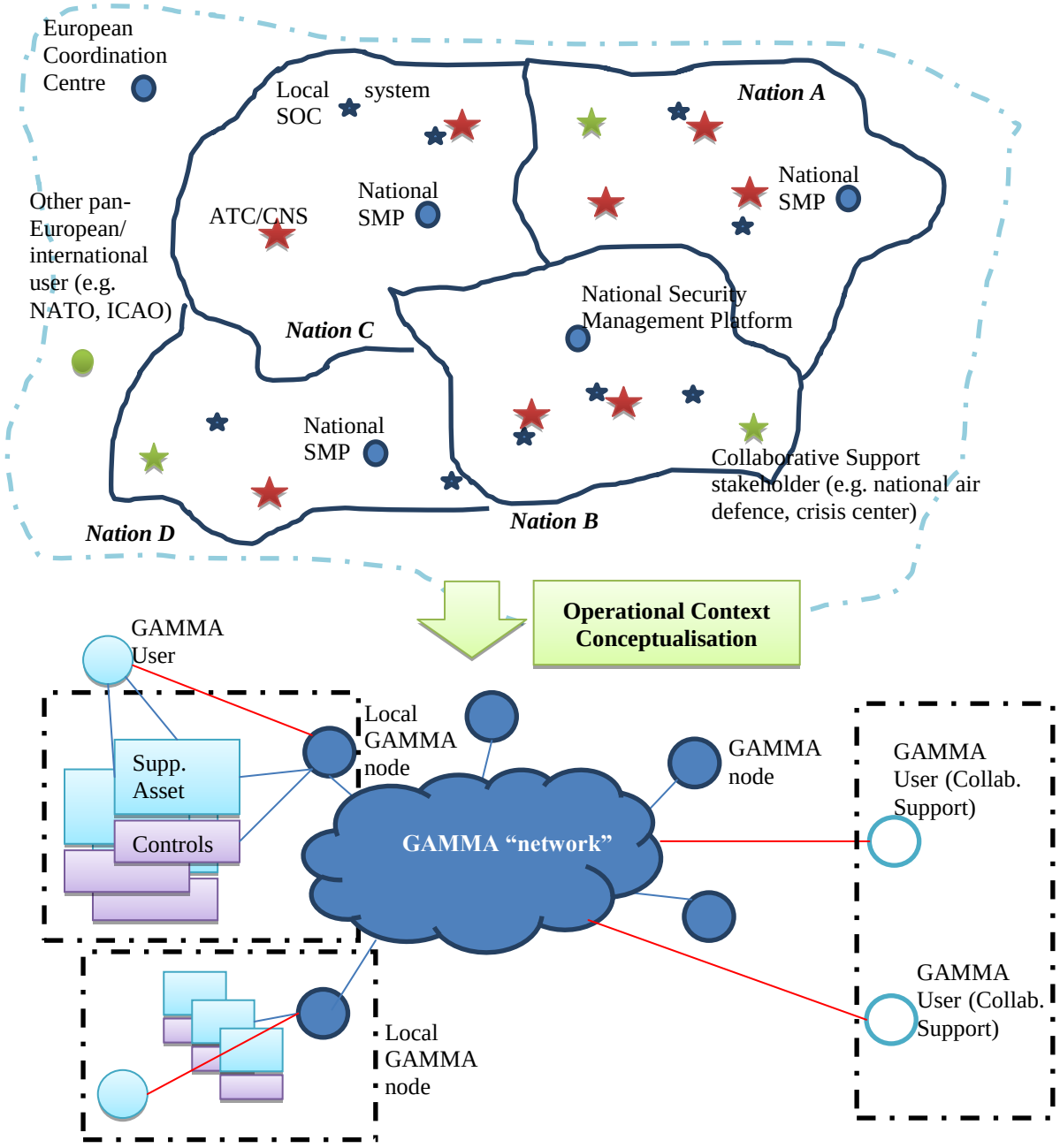


Figure 3. GAMMA Security Situation Management Network

Security Situation Management

Situation Management is an emerging paradigm. Jakobson et al (2005) introduces the term 'Situation Management' as collectively identifiable operations revolving around situation monitoring (sensing), awareness (reasoning), and control (acting) in dynamic and operational environments [7]. Alfredson (2007) stresses the process of managing dynamic situations by combining internal and external resources throughout the sense-reason-action cycle [8]. These concepts are combined by conceptualizing situation management as a distributed decision-making and multi-agent problem based on an

information-centric approach suitable for situation analysis and resource- and action-management [9].

Situation(al) Awareness

One key aspect of the situation management approach is the establishment of situational awareness coordinated and shared across the different collaborating actors. The Endsley model is the predominant model in the situation(al) awareness literature [10][11][12]. Conceptually, the Endsley model describes the human decision-making process within (safety-) critical decision-making contexts (e.g. aviation). The Endsley model defines Situation(al) Awareness as "[t]he perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future." [10] With this definition three separate layers of situational awareness can be distinguished: 1.) perception, 2.) comprehension, and 3.) prediction.

Ae we place our research into the time-critical decision-making domain, we can immediately postulate these situation(al) awareness layers as functional requirements on the GAMMA security solution.

Information Fusion

Due to the multi-disciplinary nature of fusion and its broad application, fusion has been researched and described from a variety of perspectives. There is some ambiguity in the terminology used in the fusion literature. Various researcher use the terms 'data fusion', 'information fusion', 'sensor fusion', 'multi-sensor data fusion', etc in an interchangeable manner, while others apply subtle differences. Recent research defined information fusion as the umbrella term: "Information fusion is the study of efficient methods for automatically or semi-automatically transforming information from different sources and different points in time into a representation that provides effective support for human or automated decision making."[13]

The dominant model used within the data fusion community is the JDL Data Fusion model; this defines a stepwise refinement of information [14]**Error! Reference source not found.**. The JDL however is a functional model, which means it does not itself describe how this information refinement is made. The current emphasis is towards a generalization of sensor fusion into so-called higher-level information fusion (HLIF). Recent work in HLIF concentrates on large dynamic sensor networks and higher-level information fusion [15], with a focus on the identification of objects, events and their relations.

The act of fusion serves to enrich the data / information. Fusion can serve different purposes; for example the fused information is of higher accuracy, reduced uncertainty, richer / completer. In that respect fusion serves to refine or expand our knowledge, information or beliefs about the real world [16, 17]. The processing, collection and combination of information is an essential step in time-critical decision making and the portrayed situation management approach.

Table 1. Mapping of Situation Awareness and Data Fusion Levels

	Fusion Level 0/1 Signal/Object Assessment	**Fusion Level 2** Situation Assessment	**Fusion Level 3** Impact Assessment	**Fusion Level 4** Process Refinement
Perception	Data Measurement	Situational Element Processing	Threshold / Alarm Function	
Comprehension	Analysis & Object / Element Identification	Situation Recognition / Classification	Goal / Performance Analysis	Action Planning and Selection
Prediction		Future State Estimation / Trend	Future State & Impact Evaluation	Effect Estimation

GAMMA demonstrators

The GAMMA project revolves around the demonstration of the GAMMA solution through a set of validation exercises. The demonstrators form part of the aforementioned functions and sub-systems that may be embedded in the ATM/CNS system context. In that respect, some of the GAMMA demonstrators reflect security enriched prototypes for ATM/CNS system components (i.e. supporting assets from a security risk assessment perspective). GAMMA will conceive solutions for

- security management capability by developing a national security management platform, including a supporting information dissemination system and threat prediction functions;
- security services in support of ATM/CNS components, in particular
    - network-level: information exchange gateway and information security system
    - communication: RF jamming detector, SATCOM security, integrated modular radio, GNSS communication, and secure ATC communication.

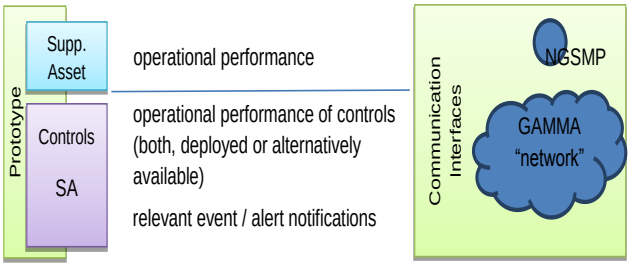


Figure 4. GAMMA Information Concept

Following the distributed security situation management network concept, these demonstrators will provide situational information on their operational status, the operational performance of their security controls, and relevant event and event information via the GAMMA network to the respective functions within the GAMMA solution context (c.f. Figure 4).

Threat Prediction Capability

The threat prediction capability is a decision support system function and hence represents a node in the distributed GAMMA security situation management network. The aim of the threat prediction capability is to process and analyze situational information received from other nodes, and establish a prediction for the actions of an adversary, including a rough assessment of the – expected – impact. The key functionality is based on the correlation of information from diverse data sources under the assumption of high false positive "alarm" rates. The threat prediction capability outputs associated alerts and threat levels, lists of potentially vulnerable supporting assets, and attack success.

Within the current GAMMA concept of operations, the threat prediction capability is envisaged as a potential local security sub-system function primarily working on sensor feeds from local sensors (e.g. event detection). On a national level, the capability may be embedded within the national security management platform. In this context, it will process information from various local systems and addresses the security situation on a higher than system component level.

In general, the threat prediction capability is based on a model of the system context. This model is built on deployment and initialized by describing all possible threats within the modelled (sub-)system through a graph structure. This includes the respective security controls and sensors in place. In that respect, security controls are assigned to the nodes of the graph (i.e. protected asset). Following the model initialization, the capability will process the information received from the sensors and interconnected security (sub-)systems. On the basis of this dynamic input, the internal state of the model is updated. Given that a possible threat is evaluated as likely based on the internal state update, the model evaluates the possible impacts of the anticipated attack mode including targeted supporting asset.

The model is constructed on the basis of a graph structure, i.e. threat path graph $G = (N,A)$. Supporting assets are referenced by a subset of nodes in the graph, $V \subset N$. Points describing the possible start of potential attacks, i.e. threat entry points, are defined

as a subset of nodes $T \subset N$. Each node in G defines a condition/configuration of the attacker resources, e.g. position, resource availability). Each edge in the graph defines the possible transition from one threat path node to another. Entry points denote possible pre-conditions of the attack. An attack scenario is formalized as a path P in the graph G from an entry point ($\in T$) to the respective supporting asset $SA \in N$ and the given type of the attack A, performed on SA, formally (P,A).

The principle of this formulation is depicted in Figure 5. For each depicted supporting asset also the type of security control and event detectors is encoded in the graph.

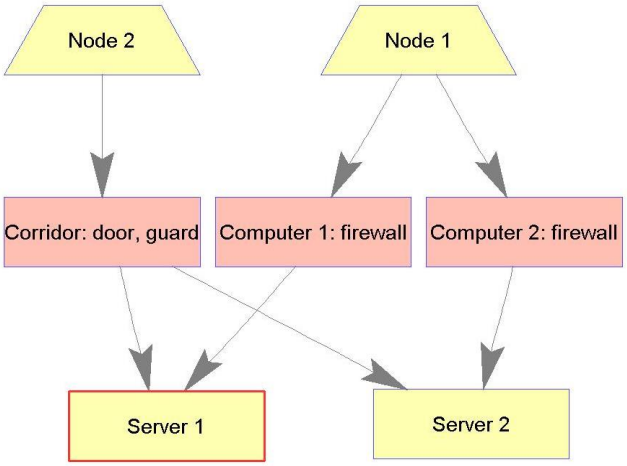


Figure 5. Threat Prediction Capability Graph

Through fusion of the sensor and event detection information it is possible to estimate the skill of the adversary. The skill level characterizes the competence level of the attacker which may be used to evaluate the effectiveness of already deployed security controls. This allows for the support to decision making as a decision to deploy additional security controls to overcome potential vulnerabilities of the controls and appreciate the possible impact after a successful attack. In that respect security controls can be categorized with a skill threshold that defines the minimum skill level an attacker requires to overcome the security control.

The mathematical formulation of the threat prediction algorithm is given as follows. An attack is formalized as a path P in graph G and its type of attack A. Let's assume a probability distribution over (P,A) - p. An event detector placed at node $n \in N$ is denoted by D_n. Event detectors are characterized by their false positive detection rate $P_{TP}(n)$ (i.e. the probability of an alarm in case of no event / attack) and their false negative detection rate $P_{FP}(n)$ (i.e. no detection in case of an adversary passing through the node). The event detection information received from a sensor at node n at time t is denoted by d_n^t. Each moment of time t a set of event detections is received $S_t = \left\{d_{n_1}^t, \dots, d_{n_{k_t}}^t\right\}$. describing the perceived signals refining the overall situation. The model assumes a discrete time basis.

The skill level of an attacker (i.e. level of competence) is characterized by the "skill" variable $s \in \mathbb{R}^+$. Each security control for each node is described by "skill" threshold. The adversary is able to overcome the security control, if the skill is higher than corresponding "skill" threshold.

Formally, the prediction task is defined as an estimation problem for p, s given the characteristic sequence S_t, the parameters of the event detectors (i.e. $P_{TP}(n)$ and $P_{FP}(n)$), and the graph structure.

In order to frame the estimation problem, we define a probabilistic graphical network over the variables of the system. Variable s is assumed to be distributed normally $\mathcal{N}(s|\mu,\sigma)$, where μ,σ are the corresponding mean and variance. We add auxiliary variable t, which denotes the threat selected by the adversary. $t \sim p$, and p defines the distribution of the variable t. The probability of the event detection is then given by the selected path and "skill" and is denoted by $p(d_n|s,t)$. It is equal to $P_{FP}(n)$ if node n does not belong to the path defined by t or if the "skill" of the adversary is not enough to reach node n using path defined by t. Otherwise the probability of detection is equal to $P_{TP}(n)$. Detections in S_t are assumed to be iid.

Given S_t, $p(s)$ and $p(t)$ we aim to estimate $p(s|S_t)$ and $p(t|S_t)$. This problem could be solved using approximate Bayesian inference. Thus, at each moment of time, the distributions of s and t are updated. These updates are used to identify the

existence of the adversary, his intention, and the level of competence. This allows for the prediction of potential impacts on the system.

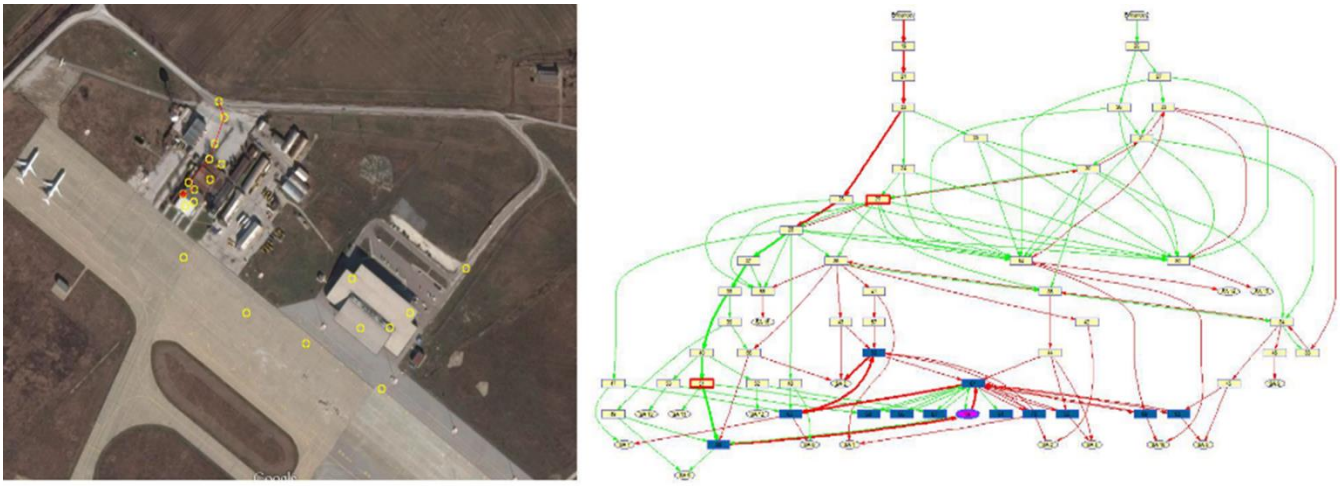


Figure 6. Threat Capability Demonstration

Discussion

Results from the GAMMA project have been discussed and presented during dedicated GAMMA user-group meetings and related security stakeholder meetings. The results so far demonstrate the general feasibility of the GAMMA solution and provide tangible input in the further refinement and development of the GAMMA prototypes. In this section, we focus on the main aspects of this paper.

Concept of Operations

The GAMMA user-group meeting in autumn 2014 supported the refinement of the GAMMA security risk assessment, threat scenarios, and GAMMA architecture model. A major discussion revolved around the different modes of operation (e.g. local security activities versus national policies) before, during, and in the aftermath of an incident.

One of the key stepping stones in developing the GAMMA concept of operations was the move from a classical security risk management and architecture description to a security situation management model (c.f. above). The confirmation of the building blocks through relevant previous research, the initial work of GAMMA, and the user-group feedback allowed for the conceptualization of the GAMMA solution as a network of distributed nodes collaboratively managing the security of the air navigation system.

The GAMMA concept of operations offers a valuable input to the further development of the validation scenarios identifying the relevant information processes between the different actors (i.e. GAMMA operators and users) and functions (e.g. information dissemination system, threat prediction capability, local security (sub-)systems, and GAMMA prototypes).

Threat Prediction Capability

The threat prediction capability has been recently showcased at the EUROCONTROL/NATO ATM Security Workshop (June 2015). The demonstration revolved around a local scenario at an aerodrome. The subsystem components and controls were modelled by approximately 80 nodes (c.f. Figure 6).

With this model and approach, we are able to bridge the situation awareness concept and data fusion concept (c.f. Table 1). In particular, the proposed threat prediction is mostly related to Fusion Level 3. According to the description of the threat prediction capability, it requires aggregated information characterizing the state of each of the system nodes. Lower level processing (level 2) may enhance the prediction performance, but it may involve significantly different kind of analyses (e.g. statistical streaming data processing, expert-based classification) which

are strongly related to the specifics of the analyzed sub-system. Therefore, from a system-level point of view, level 2 data analyses may be easily "encapsulated", so that alarm generation processes (level 2) and alarm correlation/threat prediction processes (level 3) are separated in a natural manner. The latter support the incremental implementation of the threat capability and iterative deployment of the GAMMA information concept (c.f. Figure 4) within the current or future air navigation system context.

Conclusions

This paper presented our approach to devise a concept of operations for GAMMA and develop an associated threat prediction capability for a security function embedded into the air navigation system. We describe this capability as a collaborative security situation management problem. Our present work has focused on the fundamental design aspects and underlying theory for the development of the concept of operations and the subsequent development of an initial threat prediction capability. The GAMMA threat prediction model / initial capability has been successfully demonstrated at a recent stakeholder workshop on ATM Security. As part of the GAMMA work program work is ongoing to integrate the threat prediction capability with other GAMMA demonstrators, ultimately enriching the coverage of sensor measurements and processed information in support of enabling GAMMA operators to collaboratively manage a security situation.

The results presented in this paper help to show the general feasibility of the security situation management approach expressed through the GAMMA concept of operations. While the concept of operations is wide enough to capture the generic context of air navigation, it must be recognized that the GAMMA activities target a subset of the security function. Nevertheless, the GAMMA solution builds on SESAR in such a way that the demonstrators could be easily embedded in the future ATM/CNS context.

The concept and capability presented in this paper mark the mid-point of the GAMMA project. This allows for a wider discussion of the project deliverables and a subsequent refinement to fully meet the project goals and address stakeholder requirements in terms of security capabilities. As part of the on-going activities a GAMMA security information exchange model is developing and will be further reshaped as part of the future work to enable the information exchange between the different GAMMA nodes and air navigation system components.

This paper described the principle initialization and operation of the threat prediction capability. One aspect that needs further attention is the fact that sensor and event detector may produce false read-outs or alarms, or that the event detector may not detect the adversary / method of attack. Another aspect is the temporal variation in the security control configuration. For example, controls considered during the initialization stage may degrade over time or are deactivated for maintenance reasons. Such dynamic variations of the configuration and the reliability of the sensor and detection feeds require a further refinement of the threat prediction capability modelling approach.

References

[1] Koelle, R., G. Markarian, and A. Tarter, 2011, Aviation Security Engineering, A Holistic Approach, Norwood, MA, Artech House.

[2] Koelle, R. and Tarter, A. (2012) "Towards a Distributed Situation Management Capability for SESAR and NextGen", Integrated Communications, Navigation and Surveillance Conference (ICNS 2012), pp.O6-1-O6-12.

[3] GAMMA Consortium, 2015, GAMMA CONOPS, The Ultimate ATM Security Framework, Newsletter, Issue No 1, pp. 2-3.

[4] International Civil Aviation Organization (ICAO), 2005, Doc 9854, Global Air Traffic Management Operational Concept, First Edition, Montreal, ICAO..

[5] International Civil Aviation Organization (ICAO), 2012, Doc 9885 AN/492-Restricted, Air Traffic Management Security Manual, Montreal, ICAO.

[6] SESAR Deployment Manager, 2015, Deployment Programme, Version 1 (DP v1), Work Package B2 – 4.1, Deliverable 4.1.3, Brussels.

[7] Jakobson, G., Lewis, L., Matheus, C., Kokar, M., and Buford, J. (2005) "Overview of Situation Management at SIMA 2005", Military

Communications Conference, 2005. MILCOM 2005. IEEE , vol.3, pp.1630-1636.

[8] Alfredson, J. (2007) Differences in Situational Awareness and how to manage them in the development of Complex Systems, PhD Thesis, Linköping University.

[9] Koelle, R. (2012) A Study into Situation Management applied to Time-Critical Decision-Making in Aviation Security, PhD thesis, Lancaster University.

[10] Endsley, M. R., 1995, Measurement of situation awareness in dynamic systems. Human Factors, 37, pp. 65–84.

[11] Endsley, M. R., 1995, Toward a theory of situation awareness in dynamic systems. Human Factors, 37, 32–64.

[12] Wickens, C. D., 2008, Situation Awareness: Review of Mica Endsley's 1995 Articles on Situation Awareness Theory and Measurement, Human Factors, Vol. 50, No. 3, pp. 397–403.

[13] H. Boström, S. F. Andler, M. Brohede, R. Johansson, A. Karlsson, J. van Laere, L. Niklasson, M. Nilsson, A. Persson, and T. Ziemke, 2007, On the definition of information fusion as a field of research. Technical report, University of Skovde, School of Humanities and Informatics, Skovde, Sweden.

[14] Llinas L., 2004, Revisiting the JDL Data Fusion Model II, proceedings FUSION04, Stockholm, Sweden, pp. 1218 – 12130.

[15] Scott P.D. and G.L. Rogova, 2004, Crisis Management in a Data Fusion Synthetic Task Environment, 7th International Conference on information Fusion, Stockholm, Sweden.

[16] E. Blasch, I. Kadar, J. Salerno, M. Kokar, S. Das, G. Powell, D. Corkill, and E. Ruspini, 2006, Issues and challenges in situation assessment (level 2 fusion). Journal of advances in Information Fusion, I(2).

[17] E. I. Bloch, A. Hunter, A. Ayoun, S. Benferhat, P. Besnard, L. Cholvy, R. Cooke, D. Dubois, and H. Fargier. 2001, Fusion: general concepts and characteristics. International Journal of Intelligent Systems, 16: pp. 1107–1134.

Acknowledgements

The authors would like to thank all GAMMA consortium members contributing to the development and continual refinement of the GAMMA concept of operations.

Disclaimer

The views expressed herein are the authors' own and do not reflect a GAMMA consortium and/or their employers' position or policy.

Email Addresses

denis.g.kolev@gmail.com
rainer.koelle@eurocontrol.int
racasar@isdefe.es
pmontefusco@sesm.it