Eighth USA/Europe Air Traffic Management Research and Development Seminar (ATM2009)

# SmartNodes – Towards supporting time-critical decision-making in Aviation Security

Rainer Kölle
ATM Security Domain
EUROCONTROL
Brussels, Belgium
rainer.koelle@eurocontrol.int

Alex Tarter
Communication & Integrated Systems
Ultra Electronics
Greenford, Middlesex, United Kingdom
alex.tarter@ultra-scs.com

***Abstract*— This paper considers decision support for incident management in aviation security. One of the key issues in Aviation Security is that despite their catastrophic magnitude, incidents are rare and their precursors are sometimes hard to identify. Typically decision-makers have a limited time window available to them in which to identify a situation, select an appropriate response and tailor it to the incident. Success in avoiding unwanted outcomes can diminish with delays in making decisions within the ever-decreasing time window.**

**In this paper the authors address the challenges in establishing timely situation awareness in order to support 'course of action' selection. We believe that smart systems can provide the technological capabilities required to efficiently manage a highly dynamic and complex environment, such as an aviation security incident. The goal of the research is to develop such a decision support system for incident management. This research-in-progress paper presents our approach in developing, designing and modeling the smart systems we call 'SmartNodes'.**

**We tested the performance of a network of SmartNodes within two recent European live trial scenarios in order to emulate real-time constraints and requirements. The results of these experiments indicate that automated support enhances the early identification of incidents and increases the situational awareness needed for time-critical decision-making in aviation security incidents. This ultimately gives decision-makers an increased time-window and thus a wider range of options for the deployment of responses.**

***Keywords – Aviation Security; ATM Security; time-critical decision-making; window of opportunity; decision-support***

## I. INTRODUCTION

The focus of this paper is on time-critical decision-making (TCDM) and a framework for reasoning about dynamic situations in the context of Aviation Security.

Aviation Security has been a growing concern since the first hijackings took place more than 40 years ago. The increased focus on the exploitation of asymmetric threats, such as the hijackings and use of civil aircraft as weapons culminated in the terrorist acts, which occurred in the United States on 11 September 2001 (9/11). This incident highlighted the need to enhance the situational awareness of national decision makers through reliable real-time information.

In light of 9/11 various solutions have been proposed aimed at enhancing information exchange between the various incident stakeholders. These solutions are based on the concept of network-centric operations; this postulates the precept that shared awareness, collaboration and self-synchronization can be attained through a network of knowledgeable, typically geographically dispersed units/entities.

Information-centric operations have become the mantra for implementing efficient response and counter measures in the 21st century; the central tenet being 'to provide the right information to the right person at the right time'. However as seen from the responses to recent natural and man-made incidents (e.g. Tsunami, 9/11, Hurricane Katrina) current incident management capabilities are deficient in regard to effective and time efficient information fusion and sharing.

The air transportation and ATM communities face various challenges in the future: an average annual air traffic growth in Europe of 5%, a fundamental paradigm shift, the SESAR/NextGen concepts of operation [1] etc. These trends will increase the security challenges as efforts so far have been focused on disparate local preventive measures, e.g. detection of threats at airports (e.g. passenger screening for weapons and liquid explosives). Little attention has been given to implementing a holistic and networked approach with other security response stakeholders.

The main problem surrounding Aviation Security is that we are trying to protect against catastrophic impacts which have a very low probability of being carried out. Every day hundreds of planes are flown, and thousands of passengers travel through the system, and in the midst of all of this we are trying to search for an extremely small number of attackers or attack vectors. Given the limited resources available for Aviation Security, it is therefore paramount that they are focused on identifying these attackers and preventing them from carrying out their intentions.

Enhanced Situational Awareness (SA), as a product of higher-level information fusion, has been identified as a key enabler to improve reasoning and decision-making. Situational

awareness is defined as the result of sorting through data on your environment, obtaining information from that data and comprehending what is exactly meant by it. Endsley [2] describes SA as "knowing what is going on around you". To know what is happening around oneself implicitly requires that one knows what information is relevant. This complex reasoning poses challenges in implementing an information technology based solution to providing SA.

Our research addresses these challenges within security incident management (SIM), and help create a real-time decision support system for all its phases: prevention, preparedness, response and recovery. Our focus is currently on 'preparedness', which is the ability to respond to incidents, based on the input from a mix of heterogeneous sensors and an ad-hoc coalition of incident stakeholders (actors).

This paper will first present the background and motivation that led to the development of the SmartNode concept for SIM. The concept elements are described in section V and in section VI, we focus on the research approach and experiments. Finally, we present results from these experiments and close this research-in-progress report in section VIII with our conclusions and ideas for future work.

## II. BACKGROUND

### A. Related Research

The research described in this paper lies at the intersection of three related fields; cognitive system engineering, information fusion and multi-agent system as shown in Fig. 1.

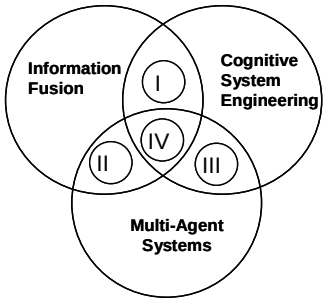


Figure 1. Convergence of the fields of Cognitive System Engineering, Information Fusion and Multi-AgentSystems; at the intersections lie (I), higher-level information fusion (II), distributed team, (III) cognitive agents, and (IV) smart systems

The field of cognitive engineering and decision making is concerned with the analysis of cognitive work and processes, and the application of this knowledge to the design and development of technology. This field has grown rapidly in recent decades due to the steadily increasing cognitive demands on human operators in socio-technical systems. Cognitive Engineering focuses on the techniques and methods of cognitive psychology [3]. Cognitive System Engineering (CSE), a variant of CE, gives a broader, system perspective to the analysis of socio-technological systems; to this end human users and technology are considered together to be a joint cognitive system [4]. In CSE human operators are viewed as goal directed agents that adapt to operational task requirements by utilizing available/supporting technology.

The area of information fusion grew out of the field of sensor fusion (sensing and estimation). This was traditionally a military discipline, where the data sources were sensors tracking moving objects represented by a set of state vectors. The goal of information fusion is to transform heterogeneously sourced data of variable validity, redundancy and often-contradictory content into timely, actionable information. Information Fusion provides the theory, techniques, and tools required for exploiting the synergy in the information acquired from multiple sources such that the resulting decision or action is in some sense better (qualitatively or quantitatively, in terms of accuracy, robustness, etc.) than would be possible if these sources were used individually.

The dominant model used within the data fusion community is the JDL Data Fusion model; this defines a stepwise refinement of information [5]. 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 [6], with a focus on the identification of objects, events and their relations. We see here the overlap into CSE, c.f. Fig 1 (I), as information fusion requires a greater amount of automated sourcing of situational elements and assessment of situational relationships (e.g. impact/threat assessment) with the ultimate aim at more effective integration with human operators [7].

Multi-Agent Systems have developed from the agent paradigm of Artificial Intelligence (AI). From within a distributed AI field, a multi-agent system originally referred to a loosely coupled network of problem-solving agents that work together to find answers to problems that are beyond the individual capabilities or knowledge of each entity [8]. More recently, the term multi-agent system has been given a more general meaning, and is now used for all types of systems composed of multiple autonomous components showing the following characteristics [9]:

- each agent has incomplete capabilities to solve a problem
- there is no global system control
- data is decentralized
- computation is asynchronous

Agents are computational entities that are situated in dynamic environments, acting to fulfil desired ends, and reacting to changing situations. Agents or, at least, an important subclass of agents, can be viewed as having mental states that comprise the beliefs, desires, plans, and intentions both of themselves and of others. While it is reasonable for us, as designers of multi-agent systems, to endow an agent with its own beliefs, desires, and plans (based on which it forms its intentions), it is quite natural for the agents then to recognize the beliefs, desires, plans, and intentions of the other agents in its environment.

(III) The behavior of cognitive agents can be considered both from an internal and external view. From an external perspective an agent can be described by temporal relationships between sensory inputs and outputs without needing to explicitly reflect on the internal (belief/mental) state of the agent. This view is addressed within the field of Behaviorism [10][11]. Functionalism [12] characterizes the behavior of an agent, from an internal perspective, as a causal temporal relationship between its mental state and its observable behavior. We follow the Functionalism approach, as we will argue that SA (a mental construct) is an enabler for decision-making and thereby assists in the implementation of a response (observable behavior).

(II) According to [13] information fusion is the synergistic integration of information from different sources on the behavior of a particular system, so as to support decisions and actions relating to the system. It is a common approach in research to model and design dispersed systems as a network of interacting agents. The net-centric operations paradigm is prevalent for the interoperability of larger constellations of sensors, systems and humans.

In our vision, incident stakeholders will utilize dynamic SA to understand the consequences of detected events, and to generate alternative responses while evaluating the associated impact of each, and to provide a basis for the synchronization of response measures. Our research builds on all the aforementioned overlaps (IV), as TCDM has the following features:

- A need for automated support, as security incidents involve multiple distributed heterogeneous information sources.
- The SIM context can be described by rapidly changing situations. These situations involve a large number of inter-dependent entities that change their states in time and space, and engage in fairly complex relations.
- Actionable information is a fusion product, balancing the technical capabilities (e.g. computational processing, high-bandwidth communication) against the human cognitive capacity.

### *B. Relevance for ATM*

As stated in ICAO Annex 17 Aviation Security is defined as "a combination of measures and human and material resources intended to safeguard civil aviation against acts of unlawful interference". Historically, Aviation Security entails three main partners: airlines, airports and governments. With the latter primarily performing a regulatory role, airlines being responsible for passenger and baggage screening and airports responsible for law enforcement and general security in the airport vicinity.

Future concepts (SESAR, NextGen)[1] strengthen the emphasis of interconnectedness of all air transportation system stakeholders. Hence, a sufficiently high level of security must be provided throughout the entire system (security is only as strong as its weakest link). Explicitly, this means that the air transportation community must be tied together, in a joint and collaborative manner, in its effort to counter threats and vulnerabilities as distortions and security breaches will have an impact on the wider system.

A fundamental role of any government is the security of its citizens. As a result, national defense requirements determine the role and mission of the military forces. In this context, Airspace Security is defined as the "safeguarding of the airspace or area of responsibility from unauthorized use, intrusion, illegal activities or any violation". In order to fulfill this mission, Air Policing remains the key air deterrent against air attacks [14]. Since the end of the Cold War in the late 80s and after 9/11 contextual changes and changes to the national threat assessment have emerged. Explicitly, in light of 9/11 military capabilities are utilized for Homeland Security functions.

The latter is important in order to understand the challenges of a 9/11 type of attack. Rogue aircraft ('Renegade'[1]) are not considered a purely military threat, therefore in these types of scenarios the national authorities tasked with providing a response to aviation security incidents will assume responsibility. Dependent on national regimes this might involve various incident stakeholders on top of the respective military units (e.g. national crisis centers, national governmental authority, etc).

In the majority of countries, ground interventions are the role of police or special law enforcement units. The handling of these incidents is typically further backed-up by local crisis and medical forces.

For the time being there is no mutually agreed definition of ATM Security. A workshop on ATM Security, Dec 2006, developed a common understanding as ATM Security being concerned with "… threats that are aimed at the ATM System directly, such as attacks on ATM assets, or where ATM plays a key role in the prevention or response to threats aimed at other parts of the aviation system (or national and international assets of high value) and limiting their effects on the overall ATM Network."

Based on the findings of SESAR [15], a 3-tiered approach to ATM Security was developed as depicted in the following figure. From Fig.2 it can be seen that ATM has a supporting role to play in any joint response to aviation security incidents. There are two dimensions to this role: (1) ensuring the required support to national authorities (clearing of airspace, data provision, etc.), and (2) mitigating the impact on overall network performance.

In conclusion we can derive that the management of aviation security incidents is a multi-agency issue. The number and diversity of actors is dependent on national legal regimes and responsibilities. In cross-border scenarios this number of actors grows significantly. On the operational level there is an overlap of several regimes (aircrew – safety of flight), national defense (integrity of airspace and protection of society), ANSP (separation of aircraft, support to distressed traffic, support to national authorities) all centered around the concept of a flight.

[1] Renegade: An aircraft operating in such a manner as to raise suspicious that it might be used as a weapon to perpetrate a terrorist attack.

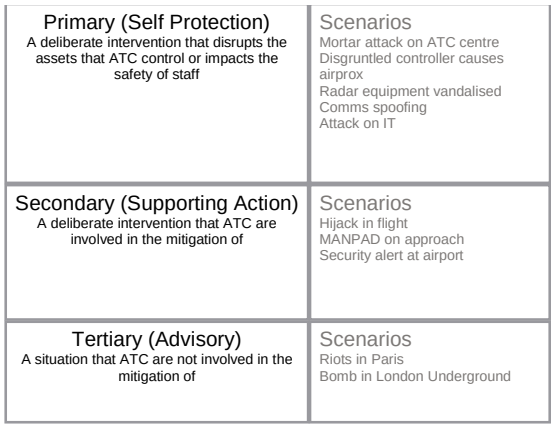


Figure 2. 3-tier framework for ATM Security

However, on an organizational level, there are various decision-makers that work from a different set of data input and might thus come to differing or even contradicting conclusions, even if their objectives are not different (which they can't be assumed to be).

### *C. Recent European Research*

Following 9/11, the European Commission launched 2 research projects in the field of Aviation Security:

- SAFEE – Security of Aircraft in the Future European Environment
- PATIN – Protection of Air Transportation and Infrastructure

During 2003 and 2006 EUROCONTROL and NATO jointly managed a validation and demonstration project coined:

- ERRIDS – European Regional Renegade Information Dissemination System

Below is a brief review of the scope and main characteristics of these projects:

#### *1) SAFEE*

The focus of SAFEE was on the development of an advanced aircraft security system designed to operate during on-board terrorist scenarios. The scope of the project entailed automatic on-board threat detection, threat assessment and response management, aircraft flight re-configuration, robust air/ground data exchange and associated evaluation activities.

#### *2) PATIN*

The scope of PATIN entailed the protection of critical ground infrastructure and aircraft at or in the vicinity of an airport against terrorist attacks. The project also assessed any required crisis management capabilities and interoperability and optimization of security networks.

The derived set of operational concept elements were tested during a real-time exercise involving a hijack flight between 2 European airports (c.f. experiments).

#### *3) ERRIDS*

The project aimed to validate and explore requirements for timely, reliable and accurate provision of relevant information to decision makers and organizations involved in the response to airborne aviation security incidents. Emphasis was given to multi-agency collaboration and information sharing in cross-border scenarios. Further development of this concept and implementation roadmap is now being carried on under the joint EUROCONTROL/NATO Security Incident Management activity.

During 2004 and 2006 a series of trials were executed with a view to validate the ERRIDS concept and demonstrate its operational principles. This series also included interoperability trials with the participation of the SAFEE project. During these trials interactions from a flight crew in a flight simulator (as well as aircraft derived data) were fed directly into an ERRIDS demonstration test bed. In October 2007, elements of the ERRIDS test bed were used to support the net-centric information exchange under the umbrella of PATIN.

A general finding of all reviewed projects is that it is vitally important to exchange information and synchronize response activities during an aviation security incident. As a matter of fact, today's operational complexity is such that given the number of stakeholders involved, there needs to be real-time information sharing beyond traditional organizational (inter- and intra-agency) and national boundaries (cross-border).

The key lessons learnt from these series of trials were that:

- fusion of information from diverse ATM stakeholders helped to improve situation awareness (e.g. estimated remaining flying time/range based on departure time [Airport, ATC], fuel amount [Airline Operation Center] and average fuel consumption [Airline Operation Center, Manufacturer Specs]).
- automated support for the identification of non-nominal behavior or mode of operation is essential for a timely reaction, as the majority of functions listed above do perform their normal duties.

## III. MOTIVATION

If we use last year's air transport figures, around 240 million people flew through UK airports. Given this number of people, even if the tests are 99.9% accurate (giving a 0.1% chance of misidentifying an anomalous situation/person) then they will still raise a false positive on 240,000 people or 657 people every day, which equates to 1 person roughly every 2.5 minutes! Given that terrorists/criminals are rare, even with an improbably high figure of 1000 of them flying every year, a 99.9% accurate test with will end up miss-identifying 239,000 people.

People are very good at detecting patterns in random data, but very bad at detecting exceptions in uniform data. Give someone too many good examples and they become 'numb' by them, and thus not sensitive to the bad examples. This effect can be explained by the fact that people can't keep a high level of concentration for extended periods of time. Computer's on

the other hand are very good at detecting exceptions but fall down when asked to make considered judgments; therefore it would seem reasonable to assume a combination of human and machine detection would work best. This would be an example of overlap between CSE and Information Fusion disciplines.

A situation where this could work is with security profiling. Traditionally, computer generated security profiles are only based on easily assigned and computer enterable characteristics such as ethnicity, age, sex, travel history, credit history etc. The problem with these characteristics is that they are not very accurate at distinguishing attackers from non-attackers, and certainly not anywhere near 90% accurate! When asking security personnel what causes them to judge someone 'suspicious', their answers are usually 'fuzzy' characteristics such as avoidance of eye contact, sweating, nervousness etc. These factors do not lend themselves very well to a tick box style profile; instead other more complex analytical techniques must be used.

Fuzzy logic has been used for over 40 years as a method to perform reasoning using approximate variables, i.e. variables such as 'hot' or 'cold' rather than 80 $^{o}$F or 30 $^{o}$F. Membership functions are used to define a degree of association between a value and a fuzzy construct. Once we have identified a range of values and their degree of association to a given concept, we can begin to map between them and perform logic on the outputs. One issue with using fuzzy logic is how you create these membership functions and be assured of their validity. Our method is to use a database of historical values and clustering techniques to identify typical states and their measurement ranges. Continued use of fuzzy clustering and neural-fuzzy techniques allow us slowly adapt the membership functions to real-life changes in the environment, which techniques used depend on the sensor and the environment variable.

Within the realm of security, fuzzy allows us to use terms such as 'nervousness' or 'paranoid' that aren't possible with traditional computing, and perform logic such as 'If someone is young, nervous and an infrequent traveler then ….'. We use fuzzy logic to combine many different types of inputs together into a security profile which can then be further assessed by a human as to if further investigation is required. It should be stressed that these systems are not making a decision on whether or not a person is actually 'dangerous', only that they are an anomaly from within the programmed scope compared with others. Profiling typically falls down when the results are blindly accepted, this system however does not attempt to form firm conclusions, as it still requires a human in the loop to do complex deduction and reasoning.

The same techniques can be used in TCDM by flagging early on when there are anomalies, either present or developing, and what they are. Decision makers need situational awareness information, so while giving them a temperature may be useful, a more helpful piece of information would be if it was too hot, cold or normal. Fuzzy logic effectively provides context to a raw piece of information. Decision makers will therefore have more time and a more conscious assessment of what the differences actually are. By requiring people to make the decisions, and by informing them of where the discrepancies lie, they will not be subject to 'numbing' from uniform data sets. If a certain state is consistently being flagged as anomalous then a human should be used to modify the membership functions as the original model could be flawed in some way and not accurately represent the environment. Evolving fuzzy algorithms could also be used in conjunction with operators to more closely model what's normal over time, and therefore reduce the number of consistently occurring false positives. The main premise for decision makers to remember is that the system is only as good as what people have programmed it to be, and thus will only identify anomalies in the data sets it is asked to look at.

## IV. PROBLEM STATEMENT

Time-critical decision-making problems exist in several areas in Aviation Security, and are characterized by a finite time window in which specific questions must be answered before a response decision can be made. Within this time window, information needs to be gathered, digested and comprehended. This limited window of opportunity is one of the key challenges in the decision-making process, as the success of mitigating unwanted outcomes can diminish with delays in taking an appropriate decision. Thus analytical techniques to problem solving/decision-making are not applicable within our domain. The inherent complexity (dynamic nature, uncertainty, partially observable variables) would make computation intractable and time consuming. Research in naturalistic decision-making [16] and SA [2][3] suggests that good decision-making is intimately linked with situational awareness. However, decision-making and situational awareness are cognitive processes and so the results might differ from one operator to another one. One of the research questions we are addressing is therefore: How to model TCDM in order to facilitate it through technology?

As we mentioned in the Introduction section, experiences have shown us that in highly complex and dynamic emergency situations (e.g. Tsunami, 9/11, Katrina) effective decision making is hampered by a lack of time efficient data gathering and information processing. The prevalence of technology means that while a decision maker is capable of receiving vast amounts of data from many different sources there is still a striking need for effective information processing to turn that raw data into an actionable situational awareness picture. If the data isn't processed before being presented to a decision maker it can lead to information overload, or a 'numbing' to any anomalies. If the data isn't properly processed then the decision maker could end up with a seemingly correct assessment whereas in reality their situational awareness picture is distorted (this was most noticeable during Katrina with the disparity between the SA pictures presented by the victims, news outlets, local government & national government).

Security Incident Management represents a complex form of decision-making. This inherent complexity stems from various sources e.g. uncertain dynamic environments, high stakes/risks, ill-structured problems with varying goals, multiple actors with different organizational forms and objectives. The multitude of its uncertainties, dynamic nature, rapidly shifting information needs and time-critical context

complicates the decision-making process and pushes the limits of human sensory and cognitive capabilities. Based on the lessons from recent incidents there is obviously a need to develop and implement effective ICT support for incident management. However it must be remembered that only providing more data or information to the decision-maker will not reduce the complexity, in contrast, this could actually overload the human cognitive processing capacity.

In a previous paper the authors describe the challenges to decision-making and situational awareness [17] in TCDM:

- Scale and complexity of scenarios may develop rapidly, and to a varying extent in an unplanned or unexpected manner
- Diversity of available information and data sources which may be dispersed over various heterogeneous systems, processing units or sensors
- Diversity of users with changing roles, objectives and information requirements
- Infrastructure that might not be (partially) available at all times

Overcoming the difficulties with creating SA for different actors in an effective and timely manner is key to information- or network-centric operations.

In the SIM context, information fusion is one of the challenges in creating actionable information (or SA). There are two conflicting reasons for this, firstly data sources do not per se know the end requirements of the decision-maker(s), and secondly decision-maker(s) need the data provided to them to be fit for purpose (i.e. relevant & in context) rather than leave the sense-making and interpretation tasks to them. In the authors' wide experience of information requirements in SIM, the fusion of information from disparate incident stakeholders (e.g. Airline Operations Center: fuel quantity, aircraft configuration; ATC: flight profile, weather conditions) will provide invaluable SA elements for operational decision making e.g. in Air Defence where the threat assessment is based on a maximum range calculation. TCDM is therefore directly linked with relevant and actionable information.

## V. CONCEPT

Based on the discussion above, we now describe the main conceptual building blocks.

### A. *Decentralized Architecture and Multi-Agent Framework*

Central processing suffers from a variety of drawbacks such as single points of failure, point-to-point vulnerabilities, and limited communications and processing capacity. The nature of the chosen application domain (uncertainty, dynamic, etc.) and the challenges addressed above suggest a distributed, cooperative approach on the basis of ad-hoc coalitions. In the European context, with a huge number of national airspaces and differences in roles and responsibilities of authorities involved in the handling of aviation security incidents, there is a need to develop scalable incident management support systems.

We formalize our approach based on a formal team framework [19]. Such problems can be stated as two tuples:

$$\langle S, A_\alpha, \Sigma_\alpha, P, \Omega_\alpha, B_\alpha, R, T \rangle, \langle \pi_\Sigma, \pi_\alpha \rangle \quad (1)$$

where for each agent 'i' in a team $\alpha$: S denotes the world states, $A_i$ the agent's domain level actions, $\Sigma_i$ the agent's communication actions, $P_i$ the world model; $\Omega_i$ the agent's observations, $B_i$ the agent's belief state, R the common reward function, T the time horizon, $\pi_\Sigma$ the communication policy, and $\pi_\alpha$ the action policy.

This representation of teamwork is general enough to allow us to examine influences on the belief state, subsequent actions and communication patterns among the various incident stakeholders.

### B. *Smart/Intelligent Decision Making Model*

We have adopted the work of Endsley [2][3] to develop a framework and model our system. In this context Situational Awareness is a fundamental enabler for decision making. Situational Awareness can be further subdivided into Perception PC, Comprehension C, and Prediction PR, enabling it to be described by the tuple SA = <PC, C, PR>.

Orasanu and Martin argue in [18] that poor decisions arise from a failure to assess the situation thoroughly, not from the kinds of strategies used to select one option over another. We argue that SA is also pivotal for early reaction while events might still be unfolding. As stated above, our interest is in designing and developing incident management systems that support time-critical decision-making. Our emphasis is therefore on modeling SA to facilitate decision support rather than concentrating on choice selection.

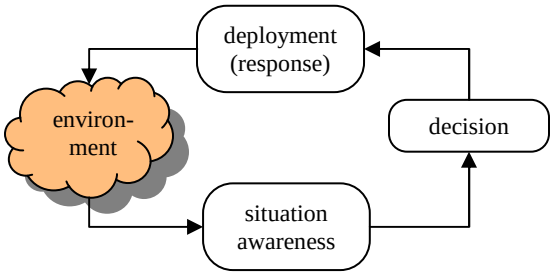


Figure 3. High-Level Decision-Making Model.

Based on results from psychology and cognitive engineering we refer to SA as a state of knowledge that results from a process [3][16]. This process may vary widely among individuals and contexts, but it is closely linked to acquiring and maintaining information about the state of the environment. We explicitly consider uncertainty in our model as sensor measurements may be noisy and information may be incomplete, unavailable or wrong. The features required to characterize situations may be described in a non-Boolean and non-quantitative manner, and thus to express these gradual nuances our SmartNode approach utilizes Fuzzy techniques which are further detailed in [17].

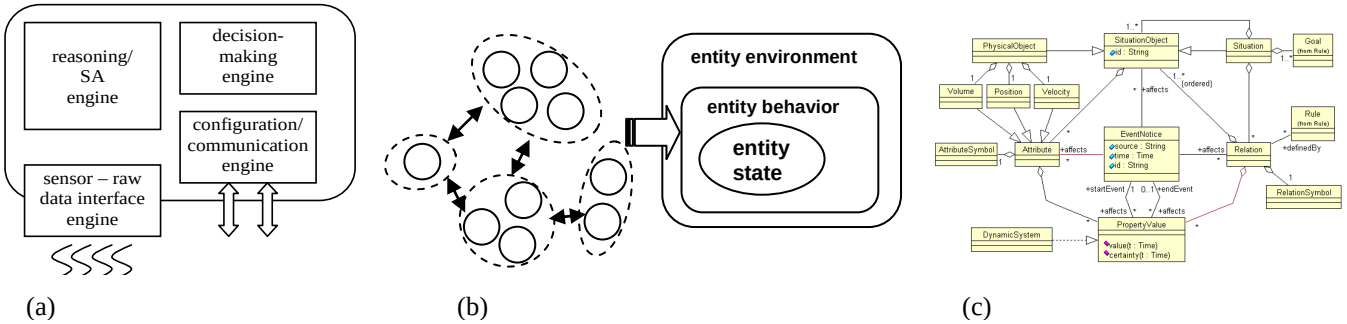


Figure 4. (a) SmartNode architecture, (b) network of SmartNodes and layers of information, (c) SA ontology [20].

## VI. Research Approach – Experiments

This section describes our experimental demonstrations. Implementation details are given first, followed by a short description of the two example use cases.

### A. SmartNodes

SmartNodes [17] automate intelligence and information fusion in support of the identification of environment states (S, P) and associated meta-information ($\Omega_I$, T)

In the design of the software implementation we have developed nodes in a modular manner comprising the following fundamental building blocks:

- Reasoning/Situational Awareness Engine
- Decision-making engine that encodes choice selection algorithms based on SA
- Configuration and Communication engine that implements the distributed communication processes
- Sensor/Raw data interfaces; dependent on the simulation some SmartNodes may be equipped with an interface to interconnected sensors.

Fig.4(a) depicts the architecture of a SmartNode. SmartNodes use Neuro- and Cluster-Fuzzy techniques to identify and maintain membership functions and convert the raw data into feature set variables (pieces of situational awareness). SmartNodes can be programmed to produce the same information and context from the data that an operator is able to infer, they can then fuse that information together with others to produce the required environment variables for SA, i.e. determine the state of the environment according to pre-determined variables. Decision-makers can then subscribe to the environment variables they require.

Based on the reasoning algorithms applied, SmartNodes are able to perform time efficient scenario recognition and provide decision-makers (human operator or an internal decision-making engine) with similarity calculations and meta-information in real-time. By defining and learning the information requirements for each element of SA (both through historical analysis and modeling), SmartNodes can actively fuse information; thereby reducing resource requirements, e.g. communication and processing, and minimize observable complexity rather than just providing raw data.

### B. System Model

SA is a mental construct. Hence, it cannot be directly interacted with by the use of traditional discrete computational algorithms. In our research we aim to externalize SA in order to enable information sharing, collaboration and facilitate the development of decision support tools. For this purpose we had to develop and model the SIM environment and an associated SA ontology. The SA ontology supports the technical representation of situational elements to form SA. We are hence able to map world states $S=\{s_j\}$ with agent observations $SA(a_i)$: $\Omega_I \rightarrow S$.

We expanded [20] and further developed a SA ontology for SIM on the basis of the 9/11 commission report. It was reviewed by senior operational staff in several incident/crisis management centers during our demonstrations. To model the SIM context, we distinguished between 3 layers of information (Entity State, Entity Behavior and Entity Environment, Fig. 4(b)) for each entity (e.g. aircraft, airspace, ANSP, Air Defense, etc). The boundaries between these layers may not be clear-cut, however, these three classifications have proved valuable during the user information requirement elicitation and ontology development process.

For example, when modeling the aircraft control state – a sub-component of the aircraft state – it is relevant to ask 'Is the pilot alive?', 'Is the pilot in the cockpit?', etc. Aircraft behavior can be characterized by a set of features such as compliance with clearance, radio contact, etc. The aircraft environment, for example, could be described in terms of flight/meteorological conditions and proximity to non-flying zones or critical infrastructure.

Following our cognition-based approach, identification of a situation is dependent on a minimum number of cues (SA elements). These cues are constructed from the information on entity states, behaviors or environment features. Dashed ellipses in Fig. 4(b) denote information agents contributing to a particular SA element. Each of these agents can be composed of several SmartNodes. All agents together form our system model network.

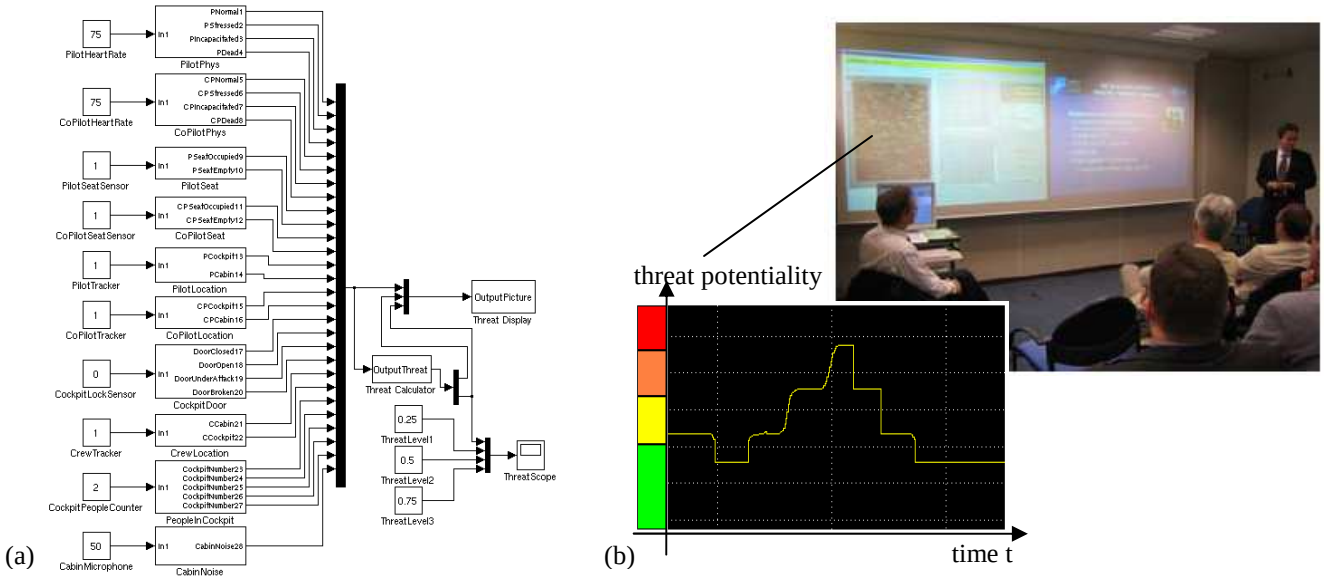


Figure 5. (a) Simulink Aircraft SmartNode, (b) Threat potentiality – live trial scenario (photo courtesy NATO NC3A, The Hague).

### C. *Use Case Scenarios*

We tried to realistically simulate and model an aviation security incident by configuring a particular SmartNode Within recent years two aviation security live trials were conducted in Europe. In September 2005, a live-trial under the umbrella of the ERRIDS project took place. This three-state scenario included a hijacked aircraft changing its flight trajectory heading towards the two adjacent countries. This flight was intercepted by fighter jets and ended with a forced diversion into a designated airport. In October 2007, an exercise took place involving two major European airports. The scenario entailed the landing of a hijacked aircraft with subsequent negotiations taking place while the aircraft was on the ground. It then departed with unknown intentions and landed at the second airport.

We are using these live trial scenarios for demonstration purposes as actual security incidents and raw data from those incidents are rare. In order to increase coordination complexity we have introduced further entities, e.g. a further state including an ANSP, Air Defense and law enforcement units.

### D. *Simulink Implementation*

We modeled our SmartNode networks in Matlab/Simulink, Fig. 5(a) depicts a simple example aircraft node. This collection of nodes takes raw sensor inputs on the environment (aircraft) and translates them into fuzzy variables, e.g. turning a microphone reading into measures of loud/quiet, sharp report, human noise, mechanical noise etc. The fuzzy nature makes it possible for the node to provide a measurement such as its 'fairly noisy, about 20% higher than normal', or 'the background noise has less human elements than normal'. The reasoning behind why this is the case is not performed by the nodes themselves, instead this is left to the decision maker. Depending on the decision-maker's objectives they may only want to receive information generated on the engines and not the passengers. By separating the collection of data from the network and utilizing it in 2 live exercises and comparing the results to the findings of the 9/11 commission report [21].

users of it, multiple stakeholders can receive the information they want without needing to collect each piece themselves.

The simulation uses recorded raw feature measurements by default, however an operator can alter the state of a feature resulting in a change to the environment, and thus an updated node observation and belief state. Dependent on the configured communication policy $\pi_\Sigma$ this information will be sent to interconnected nodes, fused and used to update the state vector of the receiving node.

## VII. RESULTS

In applying our SmartNode approach to the test scenarios, we aimed to demonstrate that SmartNodes are able to:

- provide actionable information,
- assess situational features and derive value-added decision-support information from it,
- provide an increased time-window for decision choice.

Fig. 5(b) shows an onboard threat profile that our system generated by fusing the output of position, velocity & heading sensors with the entity (aircraft) generated behavior features. This simulated threat potentiality was used as an input to a decision support node, which was then seen to propose the same actions for a set of inputs as an experienced operator. This implies that an inexperienced or time-pressured operator would benefit from the support capability.

While SmartNodes at their simplest provide identification of a feature at a given time, it is in their ability to compare a feature value against historical values that their power is seen. Most entities in ATM follow an identifiable and repeatable pattern. By mapping these measurements in a state space model

of all possible values, we will see clusters of readings representing different states. E.g. mapping the cabin pressure throughout a given flight on multiple journeys resulted in similar shaped patterns. SmartNodes use these similarities to identify anomalies or deviations from a known state.

Within our experiments we aimed to demonstrate that this clustering could be extended to multivariate data and thus provide decision-support information. As the cabin pressure correlates with the altitude of the aircraft and its stage of flight we reasoned that we should see a cluster of values and a path through a state space model when we plot the vector of these features values in time. We used fuzzy clustering techniques to characterize and identify the feature sets, which was then used to provide a measure as to the association of an actual observation $\Omega_i$ with an identified cluster. Hence, we can determine if we are in a known state, and if not where the discrepancies arise. Such a system could be used to describe other environments e.g. the cabin. When fused together these assessments of sub-environments could be used to determine the threat potentiality of a flight as described above.

Due to legal and regulatory constraints regarding the usage of experimental equipment on-board of commercial flights the experiment had to be low tech. The experimental procedure was to record the time and duration of passenger/crewmember movement in the aisle. This provided us with a measure of how much movement there was during the flight.

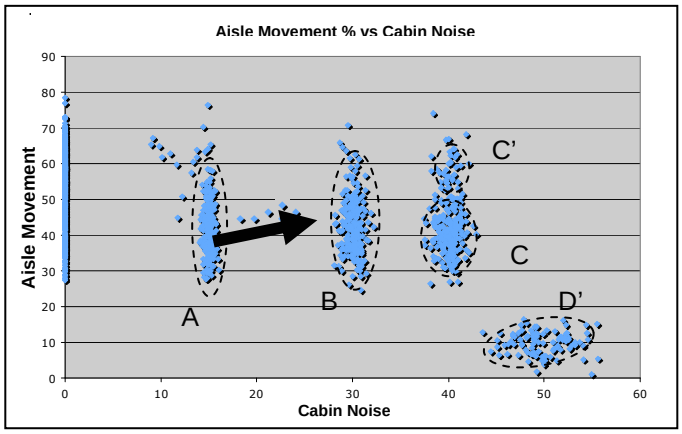


Figure 6. Cluster Analysis.

Fig. 6 shows the clearly defined clusters of correlation movement vs cabin noise level at that point in time. Using these variables is not always enough to clearly distinguish between different states (c.f. Fig.6; C - C'). These states can be distinguished if further variables are used (though the pictorial representation is less intuitive). In analogy to the described approach we generate situational information on aircraft behavior based on ATM data (track position, velocity, heading, cleared route, etc).

Useful meta-information can be derived from changes in the state space enabling us to reason about possible future states. Correlating previous state changes, allows the detection of deviations from a 'known' state/path (c.f. transition A to B) and correlating the trajectory through the state space gives us a measure of desirability (distance from a known 'good' state) or deterioration (velocity of leaving a known state).

The state space model used by SmartNodes helps to provide a base of knowledge from which effective situational recognition, even in highly complex environments can be used in TCDM. We further believe that this approach allows for (semi-) autonomous control or coordination activities to be initiated without further human interaction (e.g. civil/military information exchange between ANSP and Air Defense).

Each environment variable that a SmartNode is able to provide adds detail to the overall situational awareness in much the same way as a picture becomes clearer as more detail is added. At first we cannot be sure what the picture is of, but as finer detail and color are added, the subject of the picture is easier to understand. Note, there also comes a point when the viewer does not require any more detail, as any additional information (detail) only confirms the assessment (see Fig. 7). An experiment was designed to measure if any discernable increase in the decision time window can be achieved by using SmartNodes in the decision making cycle. In this experiment multiple decision makers are given example scenarios and provided with the outputs of a given number of nodes, they are then given a set amount of time to make a decision based on the information provided to them. The times recorded are a percentage of the total decision window into which the decision makers feel confident in making a decision.

While decision makers do not feel confident making a decision with zero or limited data, they are more comfortable when more information is provided to them. Though the amount of data required is not infinite, and as can be seen in Fig. 7, more information does not always equate to reaching a comfortable level quicker.

The SA functionality of the SmartNodes approach has shown highly satisfactory results regarding the early identification of state changes. This capability increases the window of opportunity for an operator to select the appropriate measure and synchronize these measures with others. The question of false alerts and associated thresholds, however, requires further validation.

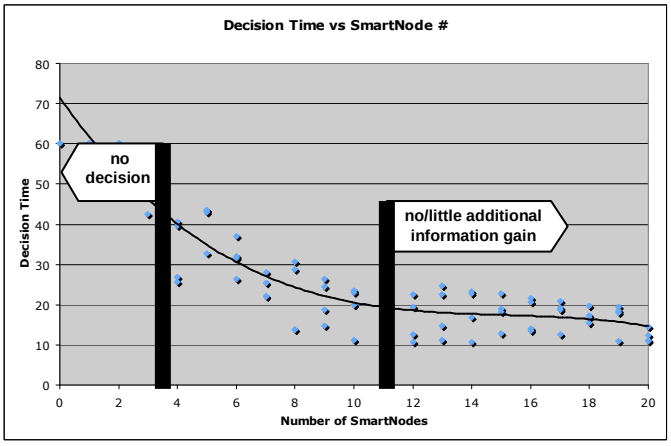


Figure 7. Decrease of decision time with increasing number of SmartNodes.

## VIII. Conclusions and Future Work

Our present work has focused on addressing the fundamental design aspects and underlying theory. In this paper we presented our contribution to security incident management and TCDM. We addressed enhanced situational awareness as a product of higher-level information fusion and as an enabler for dynamic real-time reasoning.

First, we linked the background and problem statement to time-critical decision-making; then we discussed the conceptual building blocks, our research approach and modeling aspects of SmartNodes; and finally, we outlined the experiments including those using case demonstrations based on recent aviation security incident exercise scenarios.

These results help to show the benefit from decision support systems based on networks of SmartNodes, and their effectiveness for multi-agency coordination and collaboration in aviation security incident management. The operational benefit seen is an increased time window for the selection and deployment of response measures. We envisage this as a security enabler and enhancement for the future ATM System, as much of the functionality could be built-in to SWIM.

We are concerned with the modeling effort required to build systems based on SmartNodes. Our work revolves around extending the node's capabilities to include autonomous learning and updating of a state space model. Another working thread aims at expanding the complexity of scenarios via the number of interacting SmartNodes, simultaneous attacks and temporary outages/availability of sensor readings and nodes.

We also plan to apply the SmartNodes approach to cyber-security. In a SWIM network, malicious intent detection could be based on non-nominal interaction. We believe that an analysis of the interaction patterns and connection matrix could serve as a discriminatory basis indicating cyber attacks.

## Acknowledgment

The authors would like to thank LtCol Anonio Nogueras, DCMAC, EUROCONTROL and Vu Duong, EEC, EUROCONTROL for proofreading and advice prior to the submission of the paper.

The views expressed herein are authors' own and do not reflect a EUROCONTROL or Ultra Electronics position or policy.

## References

[1] SESAR Consortium, The ATM Target Concept, SESAR Definition Phase Deliverable 3, 2007.

[2] Endsley M. R., "Theoretical Underpinnings of Situation Awareness: A critical review", in Endsley M. R. and Garland D. J. (Eds.)(2000) Situation Awareness Analysis and Measurement, Laurence Erlbaum Associates, Mahwah, NJ., retrieved 28. December 2008 from http://www.satechnologies.com.

[3] Endsley M. R., Hoffman R., Kaber D. and Roth E., "Cognitive Engineering and Decision Making: An Overview and Future Course", Journal of Cognitive Engineering and Decision Making, Volume 1, Number 1, Spring 2007, pp. 1-21.

[4] Woods, D. D., & Hollnagel, E. "Joint Cognitive Systems: Patterns in Cognitive Systems", Boca, 2006. Raton, FL: CRC Press.

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

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

[7] D.A. Lambert, "A blueprint for higher-level fusion systems", Information Fusion, vol 10, pp. 6-24, 2009.

[8] Durfee, E.H., Lesser, V.R. and Corkill, D.D., "Trends in Cooperative Distributed Problem Solving", in: IEEE Transactions on Knowledge and Data Engineering, March 1989, pp 63-83.

[9] Jennings, N.R., Sycara, K. and Wooldridge, M., "A Roadmap of Agent Research and Development", in: Autonomous Agents and Multi-Agent Systems Journal, N.R. Jennings, K. Sycara and M. Georgeff (Eds.), Kluwer Academic Publishers, Boston, 1998, Volume 1, pp. 7-38.

[10] Kim, J., Philosophy of Mind, 2nd Edition, Westview Press, Boulder CO, 2005.

[11] Heil, J., Philosophy of mind: a contemporary introduction, 2nd edition, Routledge, New York and London, 2004.

[12] Putman, H., "Mind, Language, and Reality: Philosophical papers", vol.2. Cambridge, Cambridge University Press, 1975.

[13] Andler, S. F., L. Niklasson, B. Olsson, A. Persson, T. Planstedt, L. J. d. Vin, B. Wangler, and T. Ziemke 2004. Information Fusion from Databases, Sensors and Simulations, University of Skövde, SE-54128 Skövde, Sweden, Skövde, 2004.

[14] Butler C., Major, USAF, "NATO Air Policing: Past, present and future roles", Air Command and Staff College, Air University, Research Report, Maxwell Air Force Base, Alabama, 2006.

[15] SESAR Consortium, Task 1.1.3, Milestone 3, Security, 2007.

[16] Klein, G. A. and D. Klinger, "Naturalistic Decision-Making", Human Systems IAC Gateway magazine, Volume XI: Number 3, 1991.

[17] Kölle R. and A. Tarter, "Combining & displaying results from aeronautical Smart Nodes", Intelligent Computing: Theory and Applications VI., Proceedings of the SPIE, Volume 6961, 2008, pp. 696107-696107-10.

[18] Orasanu, J. and L. Matin, "Errors in Aviation Decision Making: A Factor in Accidents and Incidents", Proceedings HESSD, 1998, pp100-107.

[19] D. Pynadeth and M. Tambe. The communicative multi-agent team decision problem: Analyzing teamwork theories and models. Journal of AI Research, 2002.

[20] Matheus C.J., M.M. Kokar, and K. Baclawski, "A core ontology for situation awareness", in Proceedings of the 6th International Conference of Information Fusion, 2003, pp 545-552.

[21] National Commission on Terrorist Attacks, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States, W.W. Norton & Company Inc., New York, London, 2004.

## Author Biography

**Rainer Kölle** is an ATM Security expert with EUROCONTROL in the ATM Security Domain, Brussels. Rainer holds a Diploma (MSc) in Electrical Engineering (Communication Systems) from the University of the German Federal Armed Forces, Hamburg, 1994. He is currently enrolled in a part-time PhD program with Lancaster University in the Aviation Security Group.

Prior to joining EUROCONTROL in 2005, he served as a career officer in the German Air Force with 18 years service experience in total.

Rainer represents EUROCONTROL in standardization activities, R&D projects and policy working groups (e.g. EUROCAE WG72, SESAR, ECIP).

**Alex Tarter** Born 1980 in the UK, went to Imperial College London where he attained a Masters in Engineering studying Information Systems Engineering. He subsequently worked in the fire rescue and defense industries and currently works for Ultra Electronics in London on UAV projects.

Alex is also the secretary and an active member of the EUROCAE WG 72 on Aeronautical Systems Security. He is also currently undertaking a PhD study through Lancaster University in Aviation Security Assessment.