

# Information Sharing Systems At Airports

## Progress Available Soon

Ronald J.F. Grosmann and Ernst Kessler  
 National Aerospace Laboratory NLR, The Netherlands  
 {grosmann, kessler}@nlr.nl

**Abstract**— Information sharing has been identified as fundamental in new air traffic management concepts that are based on collaborative decision making concepts. In these concepts a flight comprises a continuous flow of pre-flight, flight, and post-flight events in which air traffic management, air navigation service providers, airline operators and airport operators provide a seamless and coherent performance. The overall objective is to collectively plan, implement and manage optimal and flexible the use of airspace and airports with regard to safety, capacity, productivity, and flight efficiency. This paper discusses the need for information sharing, the current practice in air traffic management, some collaborative decision making concepts, an information sharing infrastructure to support these concepts, and the security implications of a near-future information sharing application such as software mobility.

**Index Terms**—Information sharing, air traffic management, software mobility, security environment

### I. INTRODUCTION

Flying commercial aircraft is a major technical achievement. A lot of effort has been spend to make flying the safe transport mode it is today. Many rules have evolved to regulate the operational part of flying. Consequently its organization is primarily focused on technical issues, leading to sophisticated systems for flying the aircraft and independent advanced systems for air traffic management. This justified concentration on safety has led to stand-alone solutions that are not optimal with respect to capacity, timeliness, environment and economy. For activities without safety implications, general commercial practices are applied.

Long term traffic growth, limitations on airport extensions and airway capacity restrictions combined with economic pressure require a more efficient flight execution, while maintaining or improving current safety levels. To achieve this goal, a global optimization integrates all activities which influence a flight's execution performed by all actors involved in that flight. This paper describes an innovative approach to realize these objectives by deploying a paradigm shift to an information sharing approach. Internet technology can enable these novel operating concepts, even when taking into account the safety requirements.

Work presented in this paper has been partially funded by a contract awarded by the European Commission (IST-2000-28744 aka. TALIS).

### II. CURRENT PRACTICE

The various aircraft systems are highly integrated to optimize the aircraft's flight within the applicable safety and capacity limits. However as aircraft are not connected to air traffic management systems, other then via an old-fashioned voice link between pilot and air traffic controller, this optimization does not take other traffic into account.

The raison d'être of Air Traffic Management (ATM) is to prevent collisions between aircraft. Aircraft operate in conditions (e.g. flying through clouds) where the pilots can not do this themselves. Traditionally air traffic management is a national responsibility, where use of civil airspace and airports is optimized to achieve maximum traffic flow. As the air traffic controllers traditionally only knew about aircraft from flight plans filed (long) before the actual flight, radar observations and voice messages, automated air traffic controller tools are restricted to this information. As airspace design differs per country and each country has full autonomy over its airspace, these systems are optimized on a national basis.

As in any safety-related industry, both aircraft and air traffic management systems tend to have a conservative approach to innovation. These systems are custom made for a very small market, compared to the general domain, resulting in relatively low innovation rate. Sector specific safety rules prevent the use of Commercial off-the-Shelf (COTS) software in aircraft, reducing the innovation rate even further. Currently the design of a new aircraft, like the Airbus A380, the Boeing Sonic Cruiser or the Joint Strike Fighter, is a major effort that takes well over a decade from initial idea to a flying and certified product. Even on the ground, Air Traffic Management systems take a similar time to produce and get operational.

Airlines fly aircraft within the limits set by the aircraft and the airspace, optimizing for commercial profit. As a result their automated support systems possess yet other information and optimize for different objectives.

Airports are independent organizations, increasingly run as commercial operations. Various supporting services like ground handling, security and fueling are run by competing organizations. All these organizations have different business objectives. So their information systems are different and optimize according to organization specific

criteria, as far as the strict procedures defining their co-operation allow.

Authorities are responsible for the environment by limiting noise, emissions, third party risk etc. This is yet another perspective, yielding different information supported by purpose-build information systems.

Over the years current procedures defining the cooperation between all these actors have evolved to a safe set. Due to the lack of information sharing, these procedures have to be based on worst-case assumptions. Within the limits of the current procedures each actor has optimized his activities. Figure 1 depicts the various current actors and their systems.



Figure 1: Overview of actors involved.

In busy airspace the current way of working is approaching its limits, resulting in safe but uneconomical flight execution with delays on the ground and in the air. As a considerable long-term air traffic growth remains expected [1], a paradigm shift towards information sharing is required to allow optimization across various actors involved.

III. COLLABORATIVE DECISION MAKING CONCEPTS

To improve this situation various ideas have evolved into the Collaborative Decision Making (CDM) concept. The COOPATS (Co-operative Air Traffic Services) concept [2] is the regional European elaboration. In the USA the Distributed Air-Ground Traffic Management (DAG-TM) [3] concept has been conceived.

A. Co-operative Air Traffic Services

The high-level objective of COOPATS is to support air traffic controllers, pilots, and all potential ATM users, in all phases of flight by progressively implementing fully seamless communications, data exchange, situational awareness and automation capabilities. The Co-operative Air Traffic Services concept is based on the human centered automation paradigm, as a consequence of the responsibilities defined by [4]. The key principle is improved situational awareness for both pilot and controller, enabled by data link technologies. For planning purposes, Co-operative Air Traffic Services is divided into two concept levels, level 1 for evolution up till 2008/2010 and level 2 for realization between 2007 and 2015. Figure 2

provides an overview of the data link services for a flight. The bottom three services (in italics) relate to level 2 services. To provide an indication of the complexity within one actor, the separate air traffic management organizational units involved are (see Figure 2):

- ACC (Area Control Center)
- AMC (Airspace Management Cell)
- APP (Approach Control)
- CFMU (Central Flow Management Unit)
- FMP (Flight Management Position)
- IFPS (Initial Flight Plan Processing System)
- TWR (Tower Control Service)

Note that the Co-operative Air Traffic Services concept naturally uses the word services and the notion that advanced services build upon more basic services as is common in general domain information sharing used a/o on the Internet.

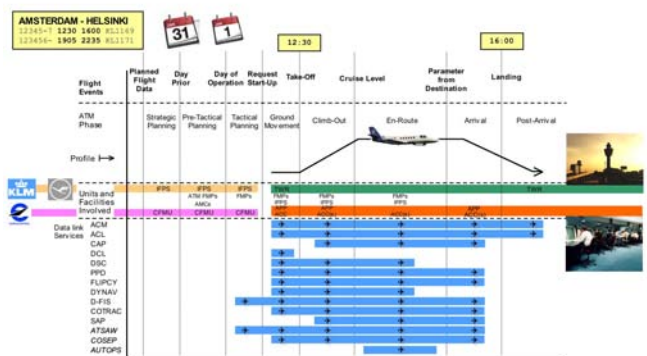


Figure 2: Overview of Eurocontrol's COOPATS concept.

Table 1 defines the network enabled services of the Co-operative Air Traffic Services concept depicted in Figure 2 above.

Service	Description
ACM	ATC Communications Management
ACL	ATC Clearance and Information
CAP	Controller Access Parameters
DCL	Departure Clearance
DSC	Downstream Clearances
PPD	Pilot Preferences Downlink
FLIPCY	Flight Plan Consistency
DYNNAV	Dynamic Route Availability
DFIS	Digital Flight Information Service
COTRAC	Common Trajectory Co-ordination
SAP	System Access Parameters
ATSAW	Air Traffic Situation(al) Awareness
COSEP	Co-operative Separation Assurance
AUTOPS	Autonomous Flight Operations Collaborative Decision Making Concepts

Table 1 Co-operative Air Traffic Services description (level 2 in italics).

B. Distributed Air-Ground Traffic Management

In [3] the Distributed Air Ground Traffic Management (DAG-TM) concept is defined as “a concept in which flight deck crews, air traffic service providers and aeronautical operational control personnel use distributed decision making to enable user preferences and increase system capacity, while meeting ATM constraints”. The centerpiece of the DAG-TM concept, depicted in Figure 3, is distributed decision making between the three parties involved:

- The flight deck, operated by the flight crew;

- The aeronautical operational control centre, operated by the flight planners and flight dispatchers. Each airline has an aeronautical operational control centre;
- The air traffic service provider, including air traffic controllers and traffic flow managers.

The DAG-TM concept defines 14 concept elements, which provide the services.

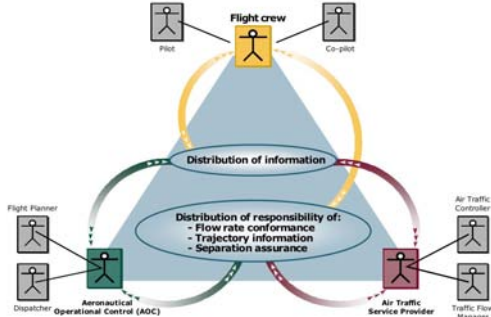


Figure 3: Overview of DAT-TM triad.

Table 2 provides an overview of the DAG-TM concept elements and the service provided by them.

Concept element	Provided services
Gate to gate	Information access / exchange for enhanced decision support
Pre flight planning	NAS (National Airspace System) constraint considerations for schedule / flight optimization
Surface departure	Intelligent routing for efficient pushback times and taxi
Terminal departure	Free maneuvering for user preferred departures
Terminal departure	Trajectory negotiation user preferred departures
En route (departure, cruise, arrival)	Free maneuvering for <ul style="list-style-type: none"> <li>• user preferred Separation assurance</li> <li>• user preferred local traffic flow</li> <li>• management conformance</li> </ul>
En route (departure, cruise, arrival)	Trajectory negotiation <ul style="list-style-type: none"> <li>• user preferred Separation assurance</li> <li>• user preferred local traffic flow management conformance</li> </ul>
En route (departure, cruise, arrival)	Collaboration for mitigating local traffic flow management restrictions due to weather, Special Use Airspace and complexity
En route / Terminal arrival	Collaboration for user preferred arrival metering
Terminal arrival	Free maneuvering for weather avoidance
Terminal arrival	Trajectory negotiation for weather avoidance
Terminal arrival	Self spacing for merging and in trail separation
Terminal arrival	Trajectory exchange for merging and in trail separation
Terminal arrival	Airborne conflict detection and resolution for closely spaced approaches
Surface arrival	Intelligent routing for efficient active runway crossing and taxi

Table 2 DAG TM concept elements and provided services.

Both COOPATS and DAG-TM comprise large systems-of-systems presenting a huge change with respect to current practice and supporting systems. Consequently, the required funding and transitional issues are significant. Within these Collaborative Decision Making concepts a much more agile concept has been developed, using the notion of services based information sharing but opting for an evolutionary realization instead. This Collaborative Decision Making

airports concept will be described below.

C. Collaborative Decision Making airport

Taking the flight profile, as depicted in Figure 2, the objective is to optimize the planning. As the en-route phase is becoming better coordinated, increasingly airports are becoming a bottleneck in air transport. At the airports usually the runway is the scarce resource. So during busy periods runway optimization is the objective, while during off-peak periods airline preferences, like on time departure, will prevail.

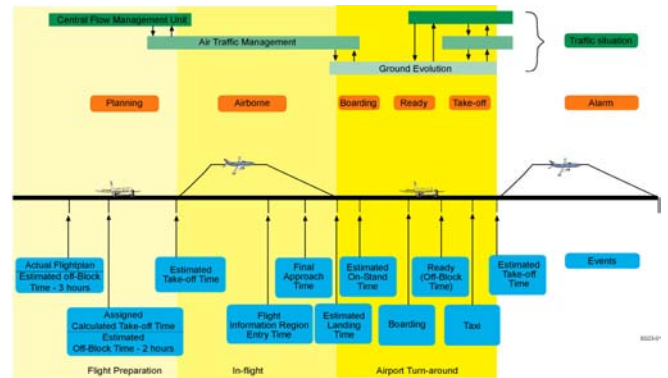


Figure 4: Overview of Collaborative Decision Making airports concept.

Figure 4 shows the main states of a flight, from an airport planning point of view. Currently every actor defines its own events which induce its state transitions and plans accordingly. Based on uniformly defined events, continuous monitoring of the on time performance can be done benefiting all actors. In case of deviations an alarm can be generated automatically. This alarm will initiate a re-planning of the traffic to maintain optimal runway usage. To maintain such a continuously optimized schedule, information sharing with all actors involved becomes necessary. Last minute rescheduling, e.g. due to late boarding by one passenger, may lead to a modified departure sequence, which may lead to a different taxing route for the aircraft having to depart earlier. This demonstrates the need for information sharing with all actors involved, including wireless communication with the mobile actors involved.

Due to the evolutionary realization, obtaining information from some actors will already improve the overall planning accuracy, allowing benefits to accrue. Also providing information to actors, e.g. baggage handling, will allow them to organize their activities to maximize overall capacity. Some changes may need not only data, but also software to be exchanged, e.g. new departure procedures. Such situations require software mobility. The next section will elaborate on the technical infrastructure to support this information sharing.

IV. INFORMATION SHARING INFRASTRUCTURE

An infrastructure for information sharing is a framework in which networked applications can be deployed as

distributed system components in an aeronautical network. The infrastructure comprises technology that will enable interoperability between networked applications, and common capabilities that can be reused by networked applications (e.g., system management, remote management, data encryption, data authentication, and security).

The goal of the information infrastructure is to provide an environment in which new aeronautical applications, like the ones mentioned by the collaborative decision making concepts, can easily be executed and tested. The key benefits of the information infrastructure are rapid response to user needs (i.e., swift deployment) and stimulation of technological innovations. This can be done without re-equipping aircraft or updating ground based systems.

A. System's Perspective

Figure 5 depicts an external system overview of the infrastructure comprising the networked applications, the Control and Display Units (CDU), and the aeronautical telecommunication network. Figure 6 depicts an internal system overview of the infrastructure in perspective to the networked applications, the CDUs, and the aeronautical network.

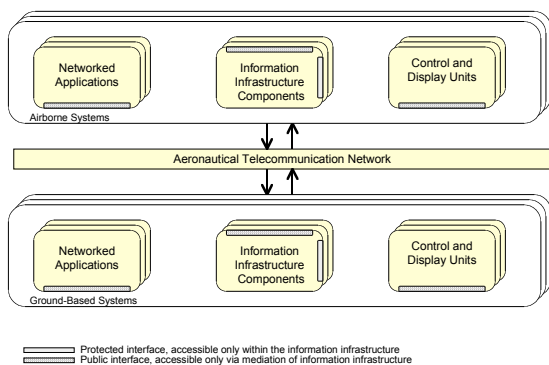


Figure 5: External system overview of the information infrastructure.

The infrastructure is chosen to be a component based middleware between information infrastructure components to enable a plug-and-play environment, comprising networked applications, CDUs, information infrastructure components, and aeronautical telecommunication networks. An information infrastructure component is an executable unit of independent deployment that can only be accessed through a published service interface. Examples of information infrastructure components are timer services, directory services, flight phase services, and data base services. Each information infrastructure component will be capable of being connected to other information infrastructure components to form a new aggregated information infrastructure component. In perspective of the infrastructure, two categories of information infrastructure components are distinguished: information infrastructure components that provide domain dependent capabilities and information infrastructure components that provide domain independent capabilities.

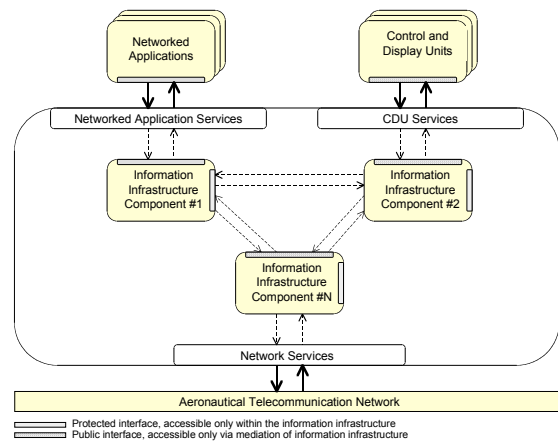


Figure 6: Internal system overview of the information infrastructure.

Networked applications and CDUs provide domain dependent capabilities. A networked application provides user oriented services and application oriented services. CDUs handle the actual communication between networked applications and their users (e.g., pilots, controllers, or operators). Information infrastructure components provide domain independent capabilities. They provide application-supporting services like registration, publication, location, and access services, data encryption and authentication services, and security services.

Each information infrastructure component has to register (part of) its services to the information infrastructure. These services will be published by the information infrastructure. Thereafter, they can be located and accessed by other information infrastructure components. This mechanism applies to networked applications, CDUs, as well as to the information infrastructure (including aeronautical telecommunication network components) itself.

B. System's Function And Purpose

The purpose of the information infrastructure is to provide software standards and technology that enable interoperability between various aeronautical applications. In other words, networked applications can coexist and co-operate with other networked applications regardless of their physical location. The information infrastructure technology will be an extensible and adaptable set of information infrastructure components that provide domain independent services. Commercial Off The Shelf (COTS) technologies and solutions can be used for this. For ground systems Do-278 applies, which, for the intended safety levels of information sharing infrastructure, allows the use of, carefully collected, service history. Consequently, COTS can also be feasible from a safety and certification perspective.

C. User Characteristics

The following categories of information infrastructure users are identified: pilots, controllers, and operators (e.g., system operators, airline operations controllers, airport service providers, and meteorological service providers).

Each category of users will use the information

infrastructure system via their specific CDUs: Multipurpose Control and Display Units (MCDU) and airborne printers for pilots, controller working positions and ground based printers for controllers, personal computers (PC), mobile devices, and workstations for operators.

#### D. Prototype System

A prototype system was developed comprising ground systems for simulating air traffic services, aeronautical telecommunication systems for communication between networked applications, and flight-deck systems (from the Airbus A380 simulator) for simulating flight-deck operations. This prototype system demonstrated from a technological perspective that information sharing, including software uploading (i.e., software mobility), identified as a fundamental asset [5] for information sharing, is feasible and that (partially) off-the-shelf products can be used. In addition, an Electronic Flight Bag (EFB) simulator was developed, in the Java programming language, for use in the cockpit and cabin for aircraft on-ground (e.g., at the gate) and in-flight operations. This development could be used to investigate software mobility mechanisms and to develop new networked EFB applications. The Java EFB (JEFB) is initially equipped with three EFB applications [6]:

- A meteorological application presenting now-cast and forecast meteorological information.
- An airport application for improved situational awareness on the ground.
- A video surveillance application for pilot security situational awareness via inside and outside video cameras of the cabin and fuselage.

Figure 7 depicts the user interface of the JEFB prototype.



Figure 7: Prototype of the Java Electronic Flight Bag.

## V. NEAR-FUTURE APPLICATIONS

In response to market developments, the European Commission has designed a road map for implementation of data link services in European Air Traffic Management [5]. These services will be implemented as information sharing applications. One of the near-future (2005 - 2010) key information sharing applications is a software loading application to be used in all flight phases. The concept of this application is software mobility to update existing functions and to add new functions in the cockpit. Such applications require adherence to strict security measures to prevent malicious attacks on the integrity of the overall air traffic system and of the aircraft systems in particular.

#### A. Software Mobility Application

Software mobility is an emerging technology used to share besides information also software. Some initial application domains for software mobility include distributed information retrieval (sharing), active documents (e.g., Postscript, HTML, and Javascript), advanced telecommunication services, remote device control and configuration, and workflow management and co-operation.

The exchange of information and code, so called software mobility is also emerging in avionics. Software mobility will ease installing and executing new applications and application patches in deployed and executing avionics systems. At the same time, if no measures are taken, this new development will make avionics systems highly vulnerable for malicious activities targeting the avionics system: threats in software mobility.

Each networked application (see Figure 5) can have its own security levels, implying an information architecture supporting various numbers of independent security levels. Traditionally, guards are used to meet the security levels. These guards operate at the boundary of a system, for example in a software loader. These guards are configured and managed by a security manager. Such security managers will check/verify the credentials of mobile software that is provided or requested by some entity. The credentials comprise information about the identity of the requestor, encryption keys, and reason for request, roundtrip information, traversed route information and predecessor credentials. The next section highlights leading threats in software mobility.

#### B. Threats In Software Mobility

As the air transport domain has no specific security requirements for information technology a threat analysis has to be performed to derive security design objectives for software mobility. A threat analysis for software mobility was performed using a proprietary method similar to the open Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE<sup>SM</sup>) method [7]. The OCTAVE<sup>SM</sup> method has three phases with eight processes.

In phase 1, threat profiles for each element that is valuable to an organization (i.e., an asset to an organization) are developed in four processes, namely identifying senior management knowledge, identifying operational area management knowledge, identifying staff knowledge, and creating threat profiles.

For each asset the following security issues are specified:

- Confidentiality, the need to keep proprietary, sensitive, or personal information private and inaccessible to anyone who is not authorized to see it,
- Integrity, the authenticity, accuracy, and completeness of an asset,
- Availability, when or how often an asset must be present or ready for use.

A threat profile consists of the following properties:

- Asset, e.g. information in electronic or physical form, information systems or people with unique expertise,
- Actor, who or what may violate the security requirements (confidentiality, integrity, availability) of an asset. Actors can be from inside or outside the organization,
- Motive (optional) indication of whether the actor's intentions are deliberate or accidental,
- Access (optional) how the actor (via network or physically) could access the asset,
- Outcome, the immediate result of violating the security requirements of an asset (disclosure, modification, destruction/loss, interruption).

In phase 2, infrastructure vulnerabilities are identified in two processes, namely identification of key components and evaluation of selected components. The vulnerabilities are grouped into the following categories [8]:

- Design vulnerability, a vulnerability that is inherent in the design or specification of the system's hardware or software. Even a perfect implementation of the design may result in the existence of a design vulnerability,
- Implementation vulnerability, a vulnerability that occurs from a flawed software or hardware implementation of a satisfactory design,
- Configuration vulnerability, a vulnerability stemming from system configuration or administration errors.

In phase 3, security strategies and plans are developed in two processes, namely conducting a risk analysis and developing a protection strategy. A risk is essentially a threat plus the resulting impact to the organization based on the threat outcome:

- disclosure of a critical asset (a violation of confidentiality)
- modification of a critical asset (a violation of integrity),
- loss or destruction of a critical asset (a violation of availability),
- interruption of a critical asset (a violation of availability).

Due to the difficulties of assessing a risk, OCTAVE<sup>SM</sup> uses a qualitative approach by developing a threat profile scheme for each threat, identified in phase 1. The security strategy of phase 3 determines which threats to address and to elaborate in security design objectives. Table 3 gives an overview, in alphabetic order, of the leading threats discerned in the threat/risk analysis for software mobility [9].

Threat	Description
Abuse	Gaining an advantage or causing disruption of service.
Analysis	Observing time, source and destination of code and information to locate or learn that some action is taking place.
Eavesdropping	Intercepting code and information without detection.
Exhaustion	Preventing authorized users from using a service by overloading the service.
Intervention	Preventing exchange of code and information traffic/protocols.
Leakage	Obtaining sensitive code or information by exploiting applications with legitimate access to code and information.
Manipulation	Modifying, inserting, or deleting code and information to frustrate safe and secure operation.
Repudiation	Denying that an action has taken place.

Table 3: Overview of threats.

To mitigate the risk impact exploited by these threats countermeasures are specified in the form of security design objectives.

### C. Security Design Objectives

Based on the listed threats and the risk analysis method the security design objectives of a software mobility architecture are derived. An architecture for software mobility shall:

- prevent intruders from obtaining unauthorized access to software and information by masquerading as authorized users.
- prevent intruders from hijacking of incoming and outgoing software and information by targeting their logical (e.g., memory, hard disk, databases) means.
- protect against unauthorized modification of software and information.
- protect confidentiality of user identity and information.
- protect against unwanted disclosure of locations of software and information for a user that is participating in a particular service.
- support various security levels since each networked application can have its own security levels.

### D. Software Mobility Architecture

The architecture for software mobility includes an execution environment that takes into account spatial and temporal partitioning requirements [10]. An architecture is envisaged that limits the vulnerabilities to malicious software and hosts. The architecture will support mechanisms for authentication, data integrity, access control, and verification of the semantics of a software component (code plus information). The architecture specifies the security environment for software mobility.

A security environment for software mobility comprises execution environments that are connected by air and ground networks. In an execution environment a resource layer, an application layer, and a communication layer are distinguished. The resource layer comprises internal and external resources like (air or ground based) databases, flight-deck systems, and other avionics. The application layer provides a capability to exchange and execute software components via mechanisms for location, migration, method

invocation and persistence. The communication layer consists of the particular protocols used e.g., IP (Internet Protocol), ATN (Aeronautical Telecommunication Network), and ACARS (Aircraft Communication Addressing and Reporting System) protocols. A COTS-based resource layer and a COTS-based communication layer can provide reliable, authenticated, and secure services. Figure 8 depicts a security environment for software mobility regardless of their physical location (i.e., airborne or ground-based).

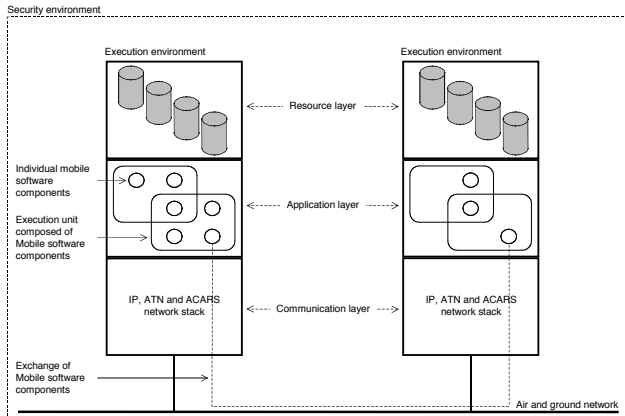


Figure 8: Security environment for software mobility.

A mobile software component is executed in the application layer of an execution unit. The application layer provides a restricted address space in which a mobile software component resides. Upon execution a mobile software component is assigned to a part of the restricted address space that is treated as local address space. A mobile software component can interface directly with resources in the local resource layer and, via de communication layer, with software components in the remote execution environment. Those software components can provide (controlled) access to remote resources.

A mobile software component comprises a code segment and data segment. The code segment contains the instructions that are executed in the local address space of the execution unit. The data segment contains the data and execution state of the concerning software component. Two classes of software component mobility are distinguished [11]: strong mobility in case a code segment plus a data segment (incl., execution state) are exchanged and weak mobility in case only a code segment is exchanged. The latter restarts execution from the beginning in its initial state ("out-of-the-box"), while the former resumes execution at the point where it was interrupted for transfer.

A security manager is installed to guard access to restricted resources. The security manager comprises security protocols to guarantee data integrity during exchange of mobile software between the server and clients (and visa versa), an architecture to implement the multiple independent levels of security, and policies to guard access to computational and information resources.

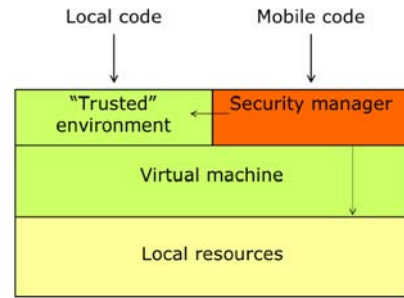


Figure 9: Security environment.

Figure 9 depicts the envisaged security environment. Local code (e.g., firmware such as the security manager and the operating system) and mobile code (e.g., networked applications) are treated independently. The local code is executed in a trusted environment with full access to all local resource. Software certification is applied according to the Do-178B [12] to the maximum certification level assigned to the mobile code. Mobile code is processed by a security manager that enforces security policies on the execution of the code and access to resources on the environment. Further research is in progress to develop a three-level security mechanism, namely on protocol level, byte-code level (i.e., verification and type checking) and run-time level (i.e., access-control and verification).

## VI. CONCLUSION

To improve the efficiency of operating aircraft in all flight phases collaborative decision making concepts are being developed. In these concepts the various actors and organizations are connected by an information sharing infrastructure to provide them with necessary information to take (collaborative) decisions. An information sharing infrastructure transforms aeronautical communication systems using wireless technology and mobile devices into a reliable, seamless, integrated solution.

Such information sharing infrastructure must adapt to the rapidly varying information needs of the actors and organizations involved to improve and support their collaboration processes. This will increase the efficiency of air transport. Reducing delays will also reduce the environmental impact. The European Union considers affordable air transport important for the single European market.

The requirements for an information sharing infrastructure were developed with help from the actual user organizations involved. Based on these real-world requirements a service driven network-centric solution was developed. As proof of concept a prototype system was developed to demonstrate, from a technical perspective, that information sharing including software mobility is feasible. Part of the information infrastructure can be realized using Commercial off the shelf (COTS) products.

Given the domain's justified security concerns, the security threats for software mobility are classified. Work on the security environment is in progress. A three-level

security mechanism is in development on top of existing hardware and data-link stack security measures.

- [10] ARINC, *Avionics Application Software Standard Interface*, ARINC 653, <http://www.arinc.com/cf/store/>, 2003.
- [11] Fariás, A., *A State Of The Art Of Security, Mobile Code And Aspect Oriented Programming*, <http://liang.peng.free.fr/thesisDescription.html>, 2000.
- [12] EuroCAE, *Software Considerations In Airborne Systems And Equipment Certification*, EuroCAE, Do-178B, 1992.

#### ACRONYMS

A380	Airbus 380
ACARS	Aircraft Communication Addressing and Reporting System
ACC	Area Control Center
ACL	ATC Clearance and Information
ACM	ATC Communication Management
AMC	Airspace Management Cell
ATM	Air Traffic Management
ATN	Aeronautical Telecommunication Network
APP	Approach Control
ATSAW	Air Traffic Situational Awareness
AUTOPS	Autonomous Flight Operations Collaborative Decision Making Concepts
CAP	Controller Access Parameters
CDM	Collaborative Decision Making
CDU	Control and Display Units
CFMU	Central Flow Management Unit
COOPATS	Co-operative Air Traffic Services
COSEP	Co-operative Separation Assurance
COTRAC	Common Trajectory Co-ordination
COTS	Commercial Off The Shelf
DAG-TM	Distributed Air Ground Traffic Management
DCL	Departure Clearance
DFIS	Digital Flight Information Service
DSC	Downstream Clearance
DYNAV	Dynamic Route Availability
EFB	Electronic Flight Bag
FLIPCY	Flight Plan Consistency
FMP	Flight Management Position
HTML	Hyper Text Markup Language
IFPS	Initial Flight Plan Processing System
IP	Internet Protocol
MCDU	Multi-purpose Control and Display Unit
NAS	(US) National Airspace System
PPD	Pilot Preference Down link
SAP	System Access Parameters
TWR	Tower control service

#### REFERENCES

(In order of appearance.)

- [1] Eurocontrol, *An Assessment of Air Traffic Management in Europe During the Calendar Year 2003*, <http://www.eurocontrol.int/prc/gallery/content/public/Docs/pr7.pdf7>, 2004.
- [2] Eurocontrol, *Towards Co operative ATS, The COOPATS Concept*, Eurocontrol DIS/ATD/AGC/MOD/DEL 01, 2000.
- [3] Bilimoria K.D., *Distributed air/ground traffic management, Air Traffic Control Quarterly*, volume 9, number 4, 2001, P.255 258, 2001.
- [4] ICAO, *Human Factors, Management and Organization*, Human Factors Digest No. 10, ICAO circular, n.249, 1994.
- [5] Shorthose, M., *Road Map For Implementation Of Data Link Services In European Air Traffic Management: Non-ATS Applications*, European Commission DG Energy and Transport, 2003.
- [6] TALIS Consortium, *TALIS Final Report*, TALIS Consortium, TALIS contract deliverable D.1.1.6, 2004.
- [7] Alberts, C. J., Dorofee, A. J., *OCTAVE<sup>SM</sup> Method implementation guide*, version 2.0, Carnegie Mellon University, 2001.
- [8] Howard J. D., Longstaff, T. A., *A Common Language for Computer Security Incidents (SAND98-8667)*, Sandia National Laboratories, 1998.
- [9] Grossmann, R.J.F., *Threat/Risk Analysis for Software Mobility*, To-Be-Published.