



# Integrated Security for Air Traffic Management IT Systems

How to achieve secure integration and administration  
of the IT systems involved in air traffic management



[www.objectsecurity.com](http://www.objectsecurity.com)

# Secure Air Traffic Management

## Highly Complex IT Infrastructure Requires Robust Security

In the past, Air Traffic Control was mainly concerned with safety, for example to ensure a sufficient separation between planes. Today this is not enough anymore, because during the last years the air traffic increased at very high rates. Instead of just keeping planes separated from each other, an efficient usage of the air space, avoidance of congestions or fuel economy play are more and more important role. This has a strong impact on ATC technology. In the past, ATC was mainly done locally, within a single sector and with coordination just between neighbouring sectors, and the ATC systems had a very low level of integration. Now, in order to deal with the enormous growth of traffic, ATC is more and more becoming a global scale optimization problem. Traffic management now has to be done at a larger scale, based on information from multiple sources and in a much larger time frame. This turns ATC in a problem of Collaborative Decision Making (CDM) with many stakeholders like control centres, airports or airlines. For example, from an overall perspective, it is not very efficient if a plane takes off in time, travels en route and then has to spend half an hour in a waiting stack, because there is no landing slot at the destination airport. It is much more economic and efficient to delay the departure, travel en route and land without delays. But things are not so easy, what are the impacts of this delayed flight? Does another plane need the plane's gate at the departure airport? Can the plane en route phase take place without congestion? What is the impact on the plane's further usage during the day? CDM now can help to improve the overall air traffic. The base of CDM is a Common Situational Awareness, much beyond the level of communication between neighbouring sectors. Common Situational Awareness is now achieved by an online data exchange between many stakeholders, like control centres, coordination centres, airlines, airports, providers of weather information, military, public authorities and many more. The improved situational awareness is then used for distributed planning and analysis.

CDM is a good idea, but is hard to implement in the real world because of the enormous complexity of the ATC systems. And it opens up vulnerabilities in the overall ATC system which was mainly ignored in the past.

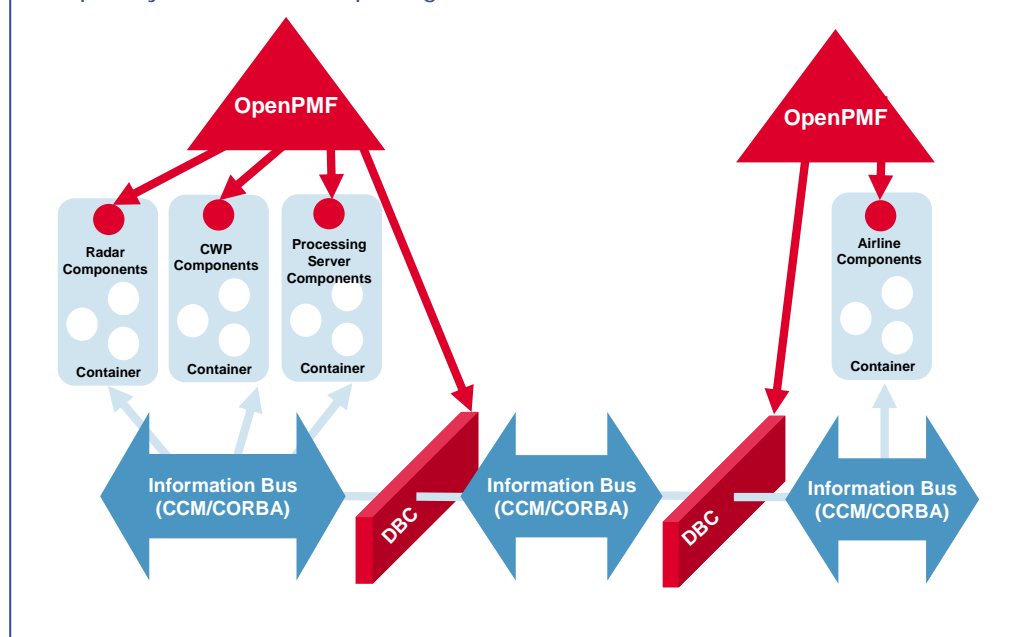
In the past, IT security of ATC systems was considered a minor concern. To a certain degree, this was acceptable, since these systems were really a difficult target for attackers, as they were mainly proprietary, often based on low tech communication means like fax or voice and not directly connected to public networks. In the future, the trend to collaborative ATC systems will dramatically increase the IT security requirements.

### Secure Air Traffic Management Case Study

This whitepaper illustrates how next-generation air traffic control systems can be built and protected using a middleware platform and a central security management framework. The project described in this whitepaper uses SecureMiddleware, a CORBA Component platform to integrate the involved systems.

As a central security management system, OpenPMF is used to protect the integrity and confidentiality of data (e.g. plane tracking data) and the system maintenance interfaces, as well as availability of the most safety-critical core functionality in near real time.

The diagram demonstrates how OpenPMF can be used to secure even very complex systems with multiple organizations.



# Information Security Issues

## Specific issues in security of collaborative ATM systems

What are the specific issues in security of collaborative ATC systems? The main issue is the very high level of integration of IT systems of different organisations. The first problem in the development of CDM systems is to achieve the requirement level of collaboration by integrating the systems. This is not simply done by just connecting them with each other, because the ATC systems are mainly proprietary. It is necessary to use a common middleware to achieve interoperability between the legacy ATC systems.

This common middleware has an enormous impact on IT security: First of all, it is much easier to communicate with the systems, over the boundaries of organizations. This is good from a functionality point of view, but it is very dangerous from a security point of view, because almost everybody in overall the system can do almost everything, for example inserting faked tracks of planes. The next problem is the wide spread knowledge of middleware, which is greatly increasing the number of people who have the necessary expertise to attack the system. Even if the ATC system would be completely disconnected from the outside world, it becomes so big that there would be a big threat of attacks from insiders. And finally, it is not possible to really keep the systems disconnected from the outside.

This makes integration without extensive IT security prone to disaster, esp. in the time of international terrorism. It is necessary to define and enforce an appropriate security policy. But this is easier said than done, because of the specific requirements in the ATC world. First of all, the overall system architecture is very complex, much more complex than for example in the financial domain. In the financial domain, most applications are based on a simple 3 tier architecture with client, business logic and a backend database. Security can easily be enforced using for example role based access control on the mid tier. In ATC, the architecture structure is much more complex, it is a fully distributed system with a high number of components exchanging data and a large number of human users, like the controllers, airline employees and administrators. There are many organisations with different with sometimes a high level of trust, but sometimes also distrust. And there are the technical requirements of the applications, for example fault tolerance or real time properties.

All this makes security in ATC a very challenging task.

→ [www.secure-airtrafficmanagement.com](http://www.secure-airtrafficmanagement.com)

# OpenPMF for Managing Security

## Consolidated Security Policy Management for Air Traffic Management

The complexity of IT security policy management in the previously described scenarios is a major challenge. This is to a large extent due to high complexity of the interactions, and the many different (also legacy) platforms and security technologies that need to be managed. This complex environment makes it hard to enforce and administer a uniform, coherent, organization-wide security policy across the many different systems used today by many agencies.

As a result, many insular security solutions are typically put in place and administered separately in incompatible ways by administrators who are only concerned with their part of the overall IT landscape. The result is often a mishmash of conflicting, redundant, and incoherent policies. Moreover, it is often unclear if and how the abstract organizational security policy has been enforced adequately by the infrastructure.



To solve this complex problem, we have developed OpenPMF, an innovative security policy management framework for distributed IT environments. OpenPMF makes security management in any large, complex, heterogeneous, networked IT environments more efficient and more accurate, and therefore less expensive. OpenPMF has been designed to secure the complex systems like air traffic management IT.

### Main Benefits of OpenPMF

- OpenPMF makes security administration of large, complex, networked IT environments manageable and more cost-effective.
- OpenPMF allows the definition of fine grained security policies. It supports a flexible enforcement of different security models like Role Based Access Control or Mandatory Access Control.
- It improves security by reducing policy complexity, policy redundancy, policy inconsistency, single sign-on and policy maintenance by consolidating security policies across many different technologies in one place and in a technology-neutral way.
- Thanks to its technology independence, the life-time of security policy information is increased dramatically, and software reuse and migration/upgrades become much easier. This also allows reusing already existing security infrastructure and policy information, for example by seamless integration of directory services

### OpenPMF Main Features

One of the main features of OpenPMF is that a model-based, technology-neutral security policy is specified and stored centrally, consistently, and in a flexible way, which allows easy administration, policy optimisation (i.e. avoid redundancy), and correctness validation. It also provides a central management of policies and logging of security events.

Using OpenPMF, this policy is then automatically enforced on the underlying technologies, and policy violations are detected. The concept that the policy is kept separate from the IT systems facilitates migration and code reuse. OpenPMF is completely independent of the underlying security infrastructure and therefore able to run on different military crypto systems.

OpenPMF's modular design allows tailor-made integration with almost any (also legacy and future) technology on the network (e.g. propriety applications, CORBA, CORBA Components, Enterprise Java Beans, XML Web Services and other messaging oriented systems, PKI, databases, LDAP directories, and firewalls). It also can be used for application specific security enforcement.

ObjectSecurity provides integration services as part of its OpenPMF services-and-software offering. The software is available in C++ and Java as a non-commercial GPL Open Source version and a commercial OpenPMF Enterprise Edition, which does

→ [www.openpmf.com](http://www.openpmf.com)

# OpenPMF for Managing Security

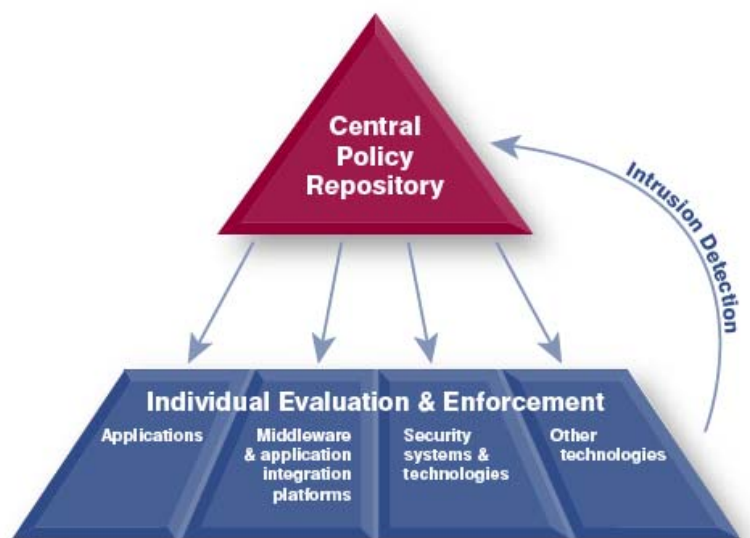
## Technology Overview

The diagram illustrates the OpenPMF architecture on a high level of abstraction. The policy is specified in an expressive, extensible, and technology-neutral language (optionally through a GUI), and stored centrally in a policy repository that is based on the flexible Meta-Object Facility (MOF) standard. OpenPMF is administered through its management GUI or integrated in other management consoles.

At system start-up, an efficient representation of the policy is fed into the technology-neutral policy evaluator, based on the information obtained from the policy repository. Within an organization, policies are centrally managed, and policy updates are automatically propagated to all concerned nodes.

Each incoming invocation on each system then triggers the evaluation process through the adapter agent, which also enforces the resulting decision. In the case of a policy violation, the agents notify the central management via the OpenPMF intrusion detection feedback system.

Currently, access control and audit policies are supported, but OpenPMF's very flexible policy model has been designed to allow fine grained information filtering policy as well at a later stage. OpenPMF also supports embedded systems which often do not have online access to the policy repository. In this case a static policy is loaded directly into the embedded device. In the near future, OpenPMF will also include improved support for the development of security policies in complex systems by close integration in with model based software engineering tools.

 OPEN pmf  
POLICY MANAGEMENT FRAMEWORK

### Infrastructure Integration with OpenPMF

OpenPMF is integrated with the underlying technologies through custom-made plug-ins per technology, which obtain security information and transform it into the technology-neutral form used by the evaluator. Transformers are currently available for CORBA and CCM (Java and C++), and Enterprise Java Beans.

As security infrastructure, the integration of public key and privilege management infrastructures, and directory services (LDAP) is supported.

For domain boundary protection, an integrated IIOP firewall is provided. Support for XML/SOAP based Web Services, web servers, .NET Remoting and other security infrastructures like Kerberos is under development.

Others can be ordered on-demand. It is esp. possible to add support for already existing crypto infrastructures, for example classified military crypto systems, or to directly add OpenPMF's policy evaluation and enforcement functionality to security aware applications.

→ [www.openpmf.com](http://www.openpmf.com)

# Secure Application Platform

## Open Source Platform for Secure Application Development and Integration

A middleware application development platform is the best option to integrate the various different systems of an air traffic management system, because it takes care of most issues related to network communications and deployment. Another benefit is that a lot of the IT security can be taken care of by the middleware platform without active involvement of the applications.

The AD4 project has developed SecureMiddleware, a standards-based middleware platform that is designed for building and integrating air traffic management systems.

SecureMiddleware is a robust, flexible and secure component platform based on a greatly enhanced version of the CORBA Components Model. SecureMiddleware can serve as a single platform for complex applications. But its real strength lies in the integration of different heterogeneous platforms and the fusion of different information sources.

SecureMiddleware supports the main middleware protocols and allows the effective integration of communications devices like low bandwidth radios. This provides a very high level of interoperability and makes SecureMiddleware an excellent information backbone, ranging from mobile devices to mainframes.

SecureMiddleware supports the main communications patterns and standard interfaces for the connection setup. Its very sophisticated deployment infrastructure allows the very quick setup of complex applications even in dynamic and heterogeneous settings.

SecureMiddleware separates functional aspects of the application from the non functional aspects. This greatly improves component reusability. To further facilitate fast and cost effective application development, SecureMiddleware is tightly integrated into a model driven development and software engineering process based on the OMG Model Driven Architecture (MDA). It supports the model driven development of both individual components and complete applications.

SecureMiddleware has been jointly developed by ObjectSecurity and Fraunhofer FOKUS.

### SecureMiddleware for complex environments

SecureMiddleware is particularly well-suited for very complex distributed applications scenarios where other platforms such as Enterprise Java Beans are not sufficient. For example, its automatic deployment mechanism for heterogeneous networks helps developers build large scale systems.

SecureMiddleware integrates with the OpenPMF security management framework to enable the centralised and consolidated definition and management of security policies. OpenPMF also provides clear separation of concerns (i.e. application logic and security). Two of the main benefits of SecureMiddleware are improved component reusability and high level of protection.

→ [www.securemiddleware.com](http://www.securemiddleware.com)

# Air Traffic Management Project

## Innovative Air Traffic Management R&D Project Produces Real-World Results

ObjectSecurity is part of a ten-partner European consortium set up to develop the AD4 Virtual Airspace Management System.

AD4 is a Specific Targeted Research Project (STREP) within the European Commission's Sixth Framework research programme. It is worth €3.5M, funded by the Commission's Directorate General H.3 Aeronautics to the tune of €1.9M.

The purpose of the project is to develop a visualization system for enhancing air traffic handling capacity while preserving safety. It integrates multi-sensor information, for example from radar and meteorology, in a secure, human-oriented 3D visualization platform for controlling air traffic. The project commenced on 18 January, 2005.

ObjectSecurity's contribution is the overall system security and in particular the security of the used application platform SecureMiddleware, which includes our OpenPMF Security Policy Management Framework. It demonstrates a large-scale deployment of OpenPMF in a mission-critical, highly complex environment.

The consortium consists of a national ATC organisation, leading vendors of ATC, visualisation, middleware and security systems, and of research organisations.

→ [www.ad4-project.com](http://www.ad4-project.com)



## Security Solutions for Air Traffic Management

ObjectSecurity provides expert information security solutions. Their particular offerings for air traffic management are in IT security for network-centric communications. The technical challenges of such communications are caused by the complex networked IT environments that comprise a multitude of incompatible systems and involve many parties with different policies and doctrines. In such environments, security policy information is currently stored and administered in many places in a proprietary and insular way. This is very time-consuming and error-prone, and security is not optimal because there is no complete picture of the enforced security.

We are the market leader in the area of security policy management in such IT environments. Our flagship open source technology for integrated security management is OpenPMF ([www.openpmf.com](http://www.openpmf.com)). It is part of the first model-driven, component-based distributed application platform in the world called SecureMiddleware ([www.securemiddleware.com](http://www.securemiddleware.com)).

ObjectSecurity has been in the market for secure distributed systems and middleware for many years, and has worked in R&D in a number of industry sectors, such as telecoms, defence, and air-traffic management. We have many R&D partners in the air traffic management sector.

### General Information Security Services

ObjectSecurity delivers a complete organization-wide approach to security, both from business imperatives through to technology solutions, and from policy creation to technologies.

The main benefits of our solutions are: adequate protection of your information assets, and reduced cost and administrative overhead of IT security.

We can offer you the following services:

- Risk analysis
- Security policy design
- Security architecture design
- Organization-wide security policy integration
- Security technology
- Security policy and technology effectiveness analysis
- Implementation of custom security solutions
- Integration of security technologies
- Technical support, R&D, and consulting for security technologies and distributed systems platforms

### Distributed Systems Security Services

Our main specialization is security of complex, heterogeneous networked applications. We are a leader in the area of distributed systems security, especially integration of security across heterogeneous IT landscapes. In particular, we deliver high-quality services in the following technologies:

- Organization-wide security technology integration
- XML Web Services security
- .NET security
- Enterprise Java Beans (EJB) security
- CORBA security and CORBA Component Model (CCM) security
- MDA modeling of security
- Secure mobile and embedded applications
- Firewalls for distributed applications
- Public key infrastructures (PKI) and privilege management (PMI)

[www.objectsecurity.com](http://www.objectsecurity.com)

[info@objectsecurity.com](mailto:info@objectsecurity.com)

ObjectSecurity Ltd.  
St John's Innovation Centre  
Cowley Road  
Cambridge CB4 0WS  
United Kingdom

Phone +44 1223 420252,  
Fax +44 1223 420844

ObjectSecurity LLC  
2910 Stevens Creek Boulevard  
Suite 109-764  
San Jose, CA 95128-2015  
USA

Phone 1-800-898-9148  
Fax 1-360-933-9591